University of Illinois at Chicago Information Technology Security Program

Version 1.0

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1: Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Section 2: UIC IT Security Policies Abstract</td>
<td>5</td>
</tr>
<tr>
<td>Section 3: UIC IT Security Program Implementation Schedule</td>
<td>6</td>
</tr>
<tr>
<td>Section 4: UIC Information Security Policy Primer</td>
<td>7</td>
</tr>
<tr>
<td>Section 5: Definitions</td>
<td>10</td>
</tr>
<tr>
<td>Section 6: UIC Information Security Program Overview</td>
<td>23</td>
</tr>
<tr>
<td>Section 7: UIC Information Security Policy Sections</td>
<td>38</td>
</tr>
<tr>
<td>Section 8: UIC Information Technology Security Program Procedures, Standards, Forms and Guidelines</td>
<td>67</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Security Program Policy</th>
<th>Section Abbrev.</th>
<th>If Present, corresponding: Procedure</th>
<th>Guideline</th>
<th>Standard</th>
<th>Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness Training</td>
<td>SA</td>
<td></td>
<td>SA.G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Classification and Security</td>
<td>DCS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.1 Data Classification</td>
<td></td>
<td></td>
<td>DCS.G.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.2.1 Identify Core Business Functions</td>
<td></td>
<td></td>
<td>DCS.G.2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.2.2 Identify Relevant Information Systems</td>
<td></td>
<td></td>
<td>DCS.G.2.2</td>
<td></td>
<td>DCS.W.2.2</td>
</tr>
<tr>
<td>Information Security Program Policy</td>
<td>Section Abbrev.</td>
<td>If Present, corresponding: Procedure</td>
<td>Guideline</td>
<td>Standard</td>
<td>Worksheet</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>DCS.2.3 Annually Classify Data</td>
<td></td>
<td></td>
<td>DCS.G.2.3</td>
<td></td>
<td>DCS.W.2.3</td>
</tr>
<tr>
<td>DCS.2.4 Risk Assessment</td>
<td></td>
<td></td>
<td>DCS.G.2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.2.5 Implement Risk Management Program</td>
<td></td>
<td></td>
<td>DCS.G.2.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.3 Access Authorization</td>
<td></td>
<td></td>
<td>DCS.G.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.4 Encryption and Decryption of Stored Data</td>
<td>DCS.P.4</td>
<td></td>
<td>DCS.S.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.5 Accountability for Hardware and Electronic Media Containing Unencrypted High Risk Data or Sensitive Data Collections</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.6 Cloud Services Storage</td>
<td></td>
<td></td>
<td>DCS.S.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.7 High Risk Data or Sensitive Data Collections Transmission Security</td>
<td></td>
<td></td>
<td>DCS.G.7.2</td>
<td>DCS.S.7.2</td>
<td></td>
</tr>
<tr>
<td>DCS.9 Develop and Implement Media Reuse Procedures</td>
<td></td>
<td></td>
<td>DCS.G.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.10 Methods Used for Disposal of All Storage Media</td>
<td></td>
<td></td>
<td>DCS.G.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCS.11 HIPAA Business Associate Agreement</td>
<td></td>
<td></td>
<td>DCS.G.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Program Policy</td>
<td>Section Abbrev.</td>
<td>If Present, corresponding: Procedure</td>
<td>Guideline</td>
<td>Standard</td>
<td>Worksheet</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Systems Security</td>
<td>SS</td>
<td></td>
<td>SS.G</td>
<td>SS.S</td>
<td>SS.S.13</td>
</tr>
<tr>
<td>SS.13 Cloud Computing Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>NS</td>
<td></td>
<td>NS.G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td>P</td>
<td></td>
<td>P.G</td>
<td>P.W.1.a</td>
<td>P.W.5</td>
</tr>
<tr>
<td>P.1 Facility Security Plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P.5 Maintenance Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Planning</td>
<td>DP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP.1 Data Backup Plan</td>
<td>DP.P.1</td>
<td></td>
<td>DP.G.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP.2 Disaster Recovery Plan</td>
<td></td>
<td></td>
<td>DP.G.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP.3 Contingency Operations</td>
<td></td>
<td></td>
<td>DP.G.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP.4 Emergency Mode Operation Plan</td>
<td></td>
<td></td>
<td>DP.G.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP.6 Applications and Data Criticality Analysis</td>
<td></td>
<td></td>
<td>DP.G.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel</td>
<td>PER</td>
<td></td>
<td>PER.P</td>
<td>PER.G</td>
<td></td>
</tr>
<tr>
<td>Policy Maintenance</td>
<td>PM</td>
<td></td>
<td>PM.P</td>
<td>PM.G</td>
<td></td>
</tr>
<tr>
<td>Reporting and Compliance</td>
<td>RC</td>
<td></td>
<td>RC.G</td>
<td>RC.S</td>
<td></td>
</tr>
<tr>
<td>RC.5 Reporting and Responding to IT Security Incidents</td>
<td></td>
<td></td>
<td>RC.P.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC.6 UISO Annual Report</td>
<td></td>
<td></td>
<td>RC.P.6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The goal of the UIC IT Security Policies & Program is to create a culture that respects and is respectful of the obligation we all have towards protecting University assets. In the case of the IT Security Policies, we are directing our efforts at protecting the digital assets of the campus and all of the respective stakeholders. We are unique in that in addition to academic, research, and financial data, we also a great amount of public health data to protect.

The purpose of the IT Security Policies and Program is to inform all campus stakeholders of their responsibilities to the safe access and securing of digital assets. One could consider these policies as being similar to the “Rules of the Road” for all drivers, cyclists, and pedestrians. Just as we all have responsibilities when we use the roads, we also all have responsibilities if we are accessing, storing, and transmitting data in the course of our jobs.

There are clear reasons we need to have an IT Security Program

- Protect student and academic data
- Protect research data
- Protect patient and health information data
- Protect HR data
- Protect financial data, including credit card information
- Protect ourselves from liability and potential loss of grant funding

To meet these goals, there will some actions that all of us will need to do. The basics of this include how computers are accessed, understanding the type of data we have, and who has access to that data. This will process is an on-going, typical part of the work we do and the mission of the University. The IT Security Program will take time to implement. It will also never be over in the sense that we will never stop being concerned with protecting the information that supports the mission of the University.
### Section 3: IT Security Program Implementation Schedule

From Policy Rollout Timeline 2014-06-04 prepared by Doug McCarthy
Full details are provided to UISOs at Orientation Meeting and Quarterly Meetings

<table>
<thead>
<tr>
<th>Action Item to be Completed</th>
<th>General Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness Training</td>
<td>Begins 1 month after Program Implementation</td>
</tr>
<tr>
<td></td>
<td>Finishes 6 months later</td>
</tr>
<tr>
<td>Data Classification</td>
<td>Begins at Program Implementation</td>
</tr>
<tr>
<td></td>
<td>DCS 2.1 through DCS 2.3 finishes 12 months later</td>
</tr>
<tr>
<td>Data Risk Management Program</td>
<td>Begins within 3 months of Program Implementation</td>
</tr>
<tr>
<td>Data Access Authorization</td>
<td>Begins 1 month after training</td>
</tr>
<tr>
<td></td>
<td>PER.3 completed in 3 months, PER.6 continues for 9 months</td>
</tr>
<tr>
<td>Data Backup Plan</td>
<td>Begins 6 months after Program Implementation</td>
</tr>
<tr>
<td></td>
<td>DP.1 completed in 6 months</td>
</tr>
<tr>
<td>Disaster Recovery Plan</td>
<td>Begins in third year of Program</td>
</tr>
<tr>
<td></td>
<td>(Unit should already have elements in Kuali Ready at start)</td>
</tr>
<tr>
<td>Contingency Operations Procedures</td>
<td>Begins in third year of Program</td>
</tr>
<tr>
<td></td>
<td>Completed 3 months later</td>
</tr>
<tr>
<td>Emergency Mode Operations Plan</td>
<td>Begins in third year of Program</td>
</tr>
<tr>
<td></td>
<td>Completed 6 months later</td>
</tr>
<tr>
<td>Systems Security</td>
<td>Begins at Program Implementation</td>
</tr>
<tr>
<td></td>
<td>SS.3, SS.8 and SS.10 completed in first year</td>
</tr>
<tr>
<td>Network Security</td>
<td>Begins in second year of Program</td>
</tr>
<tr>
<td></td>
<td>NS.1 completed then and NS.2 continues to 1st quarter Year 3</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Begins at Program Implementation</td>
</tr>
<tr>
<td></td>
<td>P.1 and P.2 completed 9 months later</td>
</tr>
<tr>
<td>Personnel</td>
<td>Starts at Program Implementation</td>
</tr>
<tr>
<td></td>
<td>PER.3 done in 3 months, PER.6 completed 9 months later</td>
</tr>
<tr>
<td>Reporting and Compliance</td>
<td>RC.4 and RC.5 begin at Program Implementation</td>
</tr>
<tr>
<td></td>
<td>RC.1 and RC.2 not begun until Year 3</td>
</tr>
<tr>
<td>Policy Maintenance</td>
<td>Ongoing and continuous</td>
</tr>
</tbody>
</table>
Section 4: UIC ITGC Information Security Program Primer / Quick Take

Purpose
The goal of the UIC ITGC Information Security Program and its constituent Policy is to provide a common framework that provides for the identification and protection of information assets at the University. The Program outlines the responsibilities of members of the Campus Community as well as the tools and procedures that are to be used to comply with the requirements.

IMPORTANT NOTE: This Primer is intended as an overview of the Security Program and is not intended as a guide to implementation of the policy. If you are required to implement any portion of this policy, you must read and follow the appropriate portion of the policy and its associated Standards, Procedures and Guidelines which are the authoritative source of information for the Program.

Program Organization
The program is broken into nine sections, each covering an aspect of operations necessary to create a secure computing environment:

1. Security Awareness
2. Data Classification and Security
3. Systems Security
4. Network Security
5. Physical Security
6. Disaster Planning
7. Personnel
8. Reporting and Compliance
9. Policy Maintenance

Security Awareness
Security awareness is discussed first as it’s recognized that the most important part of information security is making sure people are aware of the information that use on a daily basis and the requirements that exist to protect it. There are many state and federal laws and regulations that govern how different types of information need to be protected so it is important that members of the community are made aware of those laws and regulations as well as the steps they need to take to ensure the information remains secure.

Implementation tips: The bulk of the requirements of the Security Awareness section of the policy will be fulfilled by the campus-wide security awareness training program.

Data Classification and Security
Four classes of data are identified into which all data on campus can be grouped: High Risk, Sensitive, Internal and Public. In addition, as Sensitive Data is so pervasive throughout the university, a distinction is made regarding systems containing large amounts of Sensitive Data to ensure that more stringent protections are enabled on these devices.
This section of the policy requires that all units on campus determine what classes of data they possess, who has access to that data, where the data is used or stored and determine any potential risks of compromise to that information. In addition, policy is outlined to require the encryption of High Risk Data in certain circumstances as well as the appropriate methods to dispose of magnetic storage media. Implementation tips: Units will use procedure the DCS procedures to identify and classify data in their areas on an annual basis, identify relevant information systems and to conduct risk assessments. Encryption of High Risk Data can be accomplished using the UIC licensed PGP Whole Disk Encryption software available via the Software Web Store.

Systems Security
This section of the policy outlines basic policy requirements dealing with the appropriate measures and methods required to provide a secure working environment on all university owned computers. This section also outlines the requirements to remotely login to university systems and the requirements to maintain a record of their use. Implementation tips: Follow the Systems Security standards and guidelines. Be sure to implement at least the minimum requirements for your system. It is always acceptable to implement more stringent protections than the minimum requirements. Connecting your Unit’s Workstations to the campus Active Directory will greatly decrease the amount of effort required to secure your systems.

Network Security
The network security section of the policy outlines the requirements for wireless network deployment and access on campus as well as the need for firewalls on wired network segments. Specifically, all wireless networks must use encryption, require authentication and be installed or approved by ACCC. Implementation tips: If your Unit uses has their network services provided solely by ACCC, sorry, there’s nothing for you to do here.

Physical Security
The physical security of areas containing computing equipment and Workstations must be evaluated to ensure that people cannot gain access to data they should not have access to. It is also important to protect the integrity and availability of software programs for essential systems. Implementation tips: Units should use the Physical Security Guideline, P.G, for guidance on how to analyze the physical security of their locations.

Disaster Planning
Each Unit must establish and test data backup and disaster recovery plans to ensure that data can be recovered and operations can be resumed in the event of a system failure or disaster. Units that deal with electronic protected health information must also implement an Emergency Mode Operations plan. These plans must be tested on an annual basis. Implementation tips: ACCC provides a central backup service that can be used by units to fulfill all or part of the backup requirements in the disaster planning section.

Personnel
Units must identify the data access needs of all of their employees and ensure that they have access to that data but at the same time make sure they do not have access to data they don’t need. To do this, users must be uniquely identified on computing systems and all data access must be granted in a controlled, auditable manner. It is important that when an employee leaves, for whatever reason, that access is terminated.
Implementation tips: Units should connect to the campus Active Directory system and use the netid for identification and authentication. This will also simply the task of data access management.

Reporting and Compliance
It is important that logs of activity are created and that they are reviewed regularly to ensure the integrity of the systems and the data they process or store. An audit plan must be created and followed to achieve this goal. Units must follow Procedure RC.P.6 UISO Annual Report, to produce an annual compliance report.

Every member of the campus community must comply with the IT Security Policies of this Program. Failure to do so may result in disciplinary action, up to and including termination of employment.
All information security related incidents must be reported per Procedure RC.P.5 Security Incident Response and Reporting.

Implementation tips:
If the Unit does not already utilize the Request Tracker (RT) incident and service request ticketing system, they should inquire about having an RT queue set up for the Unit. Further information on RT is available at http://accc.uic.edu/service/rt

Policy Maintenance
This Program’s Policy and its associated Standards, Procedures and Guidelines will be reviewed on an annual basis and as needed modified to meet the evolving requirements of the campus. If a Unit has created any IT Security Policy, Procedures, or other associated documentation, it is required to review those documents on an annual basis as well.

Implementation tips: The Program defines communication channels and processes for anyone participating in the Program to submit reports of problems utilizing or implementing it, and to direct requests for additions or revisions to the Program. Timely critique, and response, will help in adapting the Program to evolving needs.
Section 5: Definitions

**Authentication** – A process to verify that someone is who they claim they are.

**Authorization** – A process to verify that a person, once authenticated, is able to do what they attempt to do.


**Best practice** - Ideas that represent the most efficient or prudent course of action based upon collective experience. Practices based on repeatable procedures that have proven themselves over time. Generally agreed upon processes and policies that should be undertaken when purchasing and deploying IT projects in order to decrease operational and financial risk. Strategies derived from experienced industry experts who have, through trial and error, discovered methods for design, development, and operation of computer systems which increase the chances of success and decrease risk. In information technology, to develop risk-based policies and procedures that cost-effectively reduce information security risks throughout the life cycle of each information system in information security Programs [http://www.gao.gov/key_issues/leading_practices_information_technology_management/issue_summary](http://www.gao.gov/key_issues/leading_practices_information_technology_management/issue_summary).

**Breach** – an executed threat in an **IT Security Incident** upon a **University Information System** or **University data** such that unauthorized changes to its configuration, programs, or data has caused the System or the data accessed by or stored on it to become insecure. An insecure system, also known as a breached or compromised system, can no longer be guaranteed to meet the intended University **confidentiality, integrity, or availability** needs and standards defined by this Program.

**Business process (Business function)** – a process or function carried out by a **Unit** and its **Workforce** in the course of executing its role assigned by the University, or which supports or facilitates such activity.

**Business Unit** – An administrative or operational entity within a **Unit** implementing or operating **University business processes**. These are typically directed by Business Administrators.

**Campus Community** – Participants in the University **business processes** including its **Workforce**, research partners, affiliates, Business Associates covered by [HIPAA Business Associate Agreements](http://www.gao.gov/key_issues/leading_practices_information_technology_management/issue_summary), and those who, through the University’s **business processes**, have access to non-**Public University Data** in performance of their responsibilities or obtaining information or services from **University Data** or University computational resources.

**Campus Information Technology Principals** – **Units** providing campus or University-wide information technology services: specifically including ACCC, AITS, and the University of Illinois Hospital and Health Sciences System.
Cloud Computing Services – NIST in “The NIST Definition of Cloud Computing” (2011) http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf states “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, Servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment model.”

The five essential characteristics are on-demand self-service provisioning of computing capabilities, broad network access to the service, resource pooling, rapid elasticity in provisioning capabilities, and automated and optimizing service measurement.

The three service models of cloud computing services are organized under a three tier architectural model: Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). This model can further be extended with tiers for desktop as a service (Daas), backend as a service (BaaS), and information technology management as a service (ITMaaS).

Cloud Storage – Cloud storage is a model of networked online storage in which data is stored on virtualized pools of storage which are generally hosted by third parties.

Compromise – see Breach

Confidential data – private organizational information not intended to be disclosed outside the context of the University or organization responsible for that information.


Contingency operations - the bare minimum services a Unit needs to operate its core business processes.

Control effectiveness - the ability of existing control measures implemented to measurably or estimably reduce risk.

Core business process (core business function) – an essential process or function carried out by a Unit and its Workforce in the course of executing its role assigned by the University, and tabulated by the Unit under the University’s UIReady (Kuali) Business Continuity Planning tool.

Covered Entity – The University of Illinois, as defined by the Board of Trustees of the University of Illinois in “Revise Criteria for Defining the “Covered Entity” Under Health Insurance Portability and Accountability Act” dated 7/24/2008.

http://www.uiillinois.edu/trustees/agenda/July%2024,%202008/016%20jul%20HIPAA-revised.pdf
Critical business process - Unit University core business processes identified by a Unit handling PHI to specifically meet the HIPAA Security Regulation requirements given in Policy DP.4 Emergency Mode Operations Plan.

Critical data – information which, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or recreation at considerable expense.

Critical Levels – There are four levels of criticality in a Disaster Recovery scenario and they have been defined for the University of Illinois enterprise-wide by the Kuali Ready Business Continuity System (https://us.ready.kuali.org). They are as follows:

- Critical 1: Cannot pause and must be continued at normal or increased service load. The Recovery Time Objective (RTO) or the maximum amount of time that activities must be recovered and operational is within 0 to 8 hours. (Examples: inpatient care, police services, network/IT, animal care)

- Critical 2: Must be continued if at all possible, perhaps in reduced mode. Pausing completely will have grave consequences. The RTO is within 8 to 24 hours. (Examples: provision of care to at risk outpatients, functioning of data networks, at risk research)

- Critical 3: May continue in reduced mode or pause if forced to do so, but must resume in 96 hours or sooner. The RTO is within 24 to 96 hours. (Examples: classroom instruction, research, payroll, student advising)

- Critical 4: May pause or be deferred, and resume when conditions permit. The RTO is > 1 week, but < 30 days. (Examples: elective surgery, routine building maintenance, HR-training)

Data Custodian - a person with a role responsible for providing and supporting elements of an infrastructure in support of access to University Data, its transmission and receipt, and storage, in a secure manner while providing for its availability according to diverse Unit business process needs, and ensuring its integrity. The Data Custodian may also provide and support secure access to computational resources utilized by Data Users, the Workforce, and the Campus Community, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by Data Stewards, and implementing and administering controls over that data.

Data Steward - the individual (or possibly, a group of individuals) who has a role with direct operational-level responsibility for management of University Data - usually Unit heads or directors. The Data Steward may be the person responsible for the original collection or aggregation of the data, for example, a Principal Investigator whose study collects ePHI from subjects. As another example, the Data Steward may be the assigned University business process owner, e.g. a department’s Director of Graduate Admissions who supervises the collection of departmental supplemental graduate applications.

Data User – an individual who uses University Data as part of their assigned duties or in fulfillment of their assigned roles or functions carrying out University business processes within the University community
DE-CENT Computing Environment - Units in which each Workforce member may store University Data on their own, or each subordinate Unit and its Workforce may individually choose how to store University Data. In this type of environment, Workforce awareness of what computing equipment exists in their Unit or what type of data is stored may be limited.

Delegate – Staff assuming Program responsibility or implementation duties.

Delegation Agreement – A written document stipulating the terms of the delegation of a duty under this Program, defining what duty is delegated, to whom it is delegated, and the duties still required of the delegating Unit.

Emergency Mode Operations Plan – a plan that enables the continuation of critical business processes as identified by the Unit under the requirements of Policy DP.4 Emergency Mode Operations Plan, developed under the Unit’s DP.G.4Emergency Mode Operations Plan.

Encryption - the process of encoding messages or information through a cryptographic algorithm so that only parties having authorized access to the encryption keys can decrypt and read the original data.

Endorsed campus solution (“endorsed”) – A product or service approved by Campus Information Technology Principals or the University Office of Business and Financial Services for purchase or use by the Campus Community, or a specific subset of those individuals.

EPHI (ePHI) – Electronically protected health information as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Title II Administrative Simplification, Subpart A: General Provisions, section 160.103. Quoting from it,

PHI (Protected health information) means individually identifiable health information.

EPHI is PHI transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or media. EPHI includes the following types of health information:

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census the geographic unit formed by combining all zip codes with the same three initial digits contains less than 20,000 people
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers  
10. Account numbers  
11. Certificate/license numbers  
12. Vehicle identifiers and serial numbers, including license plate numbers  
13. Device identifiers and serial numbers  
14. Web Universal Resource Locators (URLs)  
15. Internet Protocol (IP) address numbers  
16. Biometric identifiers, including finger and voice prints  
17. Full face photographic images and any comparable images; and  
18. Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual.

**Full backup** - A backup of all data and configurations including metadata on a system as well as installed programs and the operating system.

**HIGH-CENT Computing Environment** - Highly centralized and controlled computing environment in which a Unit knows exactly what computing equipment they have, what data they have, and in addition they maintain a high level of security in their environment so that may ensure that the Unit University Data cannot be stored places the system administrators are not aware of.

**High Risk Data** – Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as the federal Health Insurance Portability and Accountability Act (HIPAA) or the Illinois Personal Information Protection Act (IL PIPA), are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements. These Policies recognize that other data including Confidential Data may need to be treated as High Risk Data because it would cause severe damage to the University if its unauthorized disclosure or modification occurs through a breach. The Data Steward should make this determination. It is the Data Steward's responsibility to request the Data Custodian implement the necessary security requirements for High Risk Data under this Program.

For a fuller discussion, please see the University of Illinois Information Security Policy:  


**Impact (in a risk context)** - the financial or reputational harm that would be incurred by the University if an adverse event occurred.

**Impact level** - The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on University business processes, University assets including University Information Assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
The potential **impact** is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on **University business processes**, including **University Information Assets**, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential **impact** is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on **University business processes**, including **University Information Assets**, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Harm to individuals as described in these impact levels is easier to understand with examples. A **breach** of the confidentiality of PII at the low **impact** level would not cause harm greater than inconvenience, such as changing a telephone number. The types of harm that could be caused by a **breach** involving PII at the moderate **impact** level include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail. Harm at the high **impact** level involves serious physical, social, or financial harm, resulting in potential loss of life, loss of livelihood, or inappropriate physical detention.

**Incremental backup** - A backup of only files which have changed since the last full backup.

**Information Asset** - information, software, services, intangibles (e.g. reputation), and physical assets (devices or components) used to access, store, or process information assets.

**Insecure System** - When a **threat** has been executed upon a **University Information System** such that unauthorized changes have occurred or are possible to its configuration, programs, or data, the system is insecure. An Insecure System, also known as a **Breached** or **Compromised** system, can no longer be guaranteed to meet intended University confidentiality, integrity, or availability needs and standards. It is **prohibited** to connect an Insecure System to a University network, and to use the system for any **University business Process**.

http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf defines integrity as “(g)uarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.”

**Instructional Systems – Workstations** dedicated for the use of instructional software or to display presentations of educational material which do not have any High Risk Data, Sensitive Data Collections, or Sensitive Data stored on them or which are configured to have access to such data on file shares.
Internal Data - information that, if disclosed or modified without authorization, would have moderate adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

IT Security Incident – The NIST Federal Information Processing Standards (FIPS) Publication Series 200, “Minimum Security Requirements for Federal Information and Information Systems” http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf defines an information technology (IT) security incident as “(a)n occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”

Some of the ways an IT Security Incident at this University may affect:
   a. Confidentiality is by unauthorized disclosure of University Data;
   b. Integrity is by unauthorized change or deletion of University Data;
   c. Availability is by inhibition of access to or control of computer or network based resources used in University business processes.

An IT Security Incident may occur
   a. Intentionally, for example in the course of a malefactor’s violation of a statute or regulatory requirement, or
   b. Unintentionally, for example, in the course of a natural disaster.

IT Security Incident threats arise or have the potential to arise when vulnerabilities can be exploited.

Likelihood - the perceived likelihood of an adverse event occurring over a certain time range, typically one year.

Low strength encryption ("low strength") – encryption cipher strength less than Medium strength encryption.

Medium strength encryption ("Medium strength") - minimum 128 bit AES, IDEA or RC4 encryption level or 168 bit (effectively 112 bit) 3DES encryption ciphers.

MIXED Computing Environment - A mixture of varying levels of awareness of Unit University Data distribution, and of the effectiveness of administrative control of the systems and data storage.

Offsite backup - Backup media physically stored elsewhere besides a Unit’s assigned space or the campus building in which that space is located.

Originator Usage Period - applicable to the use of a unique Symmetric Data Encryption key in applying the original cryptographic protection to information (i.e., encrypting storage under DCS.4S.1.2). During the originator-usage period, information may be encrypted by the data-encryption key; the key shall not be used for performing an encryption operation on information beyond this period. However, the key may need to be available to decrypt the protected data beyond the originator-usage period (i.e., the recipient-usage period may need to extend beyond the originator-usage period).
Personally Identifiable Information (PII) – NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), defines PII Data as any information about an individual maintained by a Unit, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII Data include, but are not limited to:

a. Name, such as full name, maiden name, mother’s maiden name, or alias
b. Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number

c. Address information, such as street address or email address

d. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
e. Telephone numbers, including mobile, business, and personal numbers
f. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
g. Information identifying personally owned property, such as vehicle registration number or title number and related information
h. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

PHI (Protected health information) - individually identifiable health information. See ePHI

PIPA – Illinois Public Act 094-0036 “Personal Information Protection Act”, Illinois Compiled Statutes Chapter 815, Act 530

Portable media – utilized by magnetic or optical information data storage technologies on removable and thereby portable media: typically CDs, DVDs, or tapes

Portable data storage device – any physical data storage device designed to be readily picked up and transported by persons from workplace to workplace, as opposed to “desktop computers” or other bulkier and less transportable systems such as Servers generally meant to be utilized at a relatively permanent and single fixed physical location. Portable data storage devices include tablet, laptop, or notebook computers, handheld devices such as PDAs, USB interface storage devices including “thumb drives” and “flash drives”, and all types of removable data storage media.

Principals – see Campus Information Technology Security Principals
Private Data – Data that is to be observed only by the originator or sender(s) and a designated recipient or receiver(s).

Program – this Information Technology Security Program.

Program Components – this Information Technology Security Program’s Information Technology Security Policies, Procedures, Forms (Worksheets), Guidelines and Standards.

Public Access Systems – Systems identified and evaluated by the Guideline DCS.G.2.4 Conduct Risk Assessment and DCS.G.2.5 Implement Risk Management Program process which are designed to allow unauthenticated access. These systems are specifically exempted from the Policy SS.5 Automatic Locking requirements. As an example, a unit may define publicly accessible information kiosks and ACCC administered Pharos print stations as Public Access Systems if they are identified and evaluated in the above Procedures.

Public Data – Public Data is University Data intended for public use that, when used as intended, would have no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

Recipient Usage Period - applicable to the use of a unique Symmetric Data Encryption key in decrypting information (i.e., encrypted storage under DCS.4S.1.2). During the Recipient Usage Period, information may be decrypted by the data-encryption key. The Recipient Usage Period should not exceed the Originator Usage Period plus three years. Thus, a unique Symmetric Data Encryption key under the DCS.4S.1.2 Standard shall not be used for a period exceeding 5 years from the date the information has been encrypted.

Reporter – Any Unit staff member who identifies a potential or actual conflict in responsibility or implementation of any Program requirement.

RPO - Recovery Point Objective. The maximum tolerable period in which data might be lost from an information technology service due to a major incident.

RTO - Recovery Time Objective. The duration of time within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity.

Sensitive Data – Information that, if disclosed or modified without authorization, would have serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Sensitive Data includes information that is covered by FERPA, Non-Disclosure Agreements (NDAs), and other intellectual property are, as a minimum, in this class.

Note: Data described in Non-Disclosure Agreements may fall into the High Risk Data or Sensitive Data categories, and should be individually evaluated.

Sensitive Data Collection – a collection of Sensitive Data that results from compiling (i.e., collecting) the Sensitive Data from multiple sources. For example, an instructor’s compilation of grades for his/her own classes, held on their own computer, would not be a Sensitive Data Collection. However, a
department’s compilation of all the grades for all the classes in the department, held in storage, would be a Sensitive Data Collection.

Where a requirement is given in this Program for Sensitive Data, the same requirements apply to Sensitive Data Collections as a minimum threshold. Sensitive Data Collections are specifically identified in this program where a more restrictive or extensive requirement is applied to a Sensitive Data Collection than Sensitive Data.

Server – any system, application, or data storage device which is configured to allow access to it by a more than one user (excluding a single user per device and the system administrator, if separate from the user) concurrently.

Strong encryption ("Strong" or "High strength") - ciphers with an encryption level at least as strong as AES (192, and 256-bit key lengths), Blowfish (128 to 448-bit key lengths, in 8-bit increments), and ARCFOUR (2048-bit).

System – Any computer or networking resource such as a Workstation, Server, or router.

Threat – The NIST Federal Information Processing Standards (FIPS) Publication Series 200, “Minimum Security Requirements for Federal Information and Information Systems” http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf defines a threat as “(a)ny circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”

UISO – Unit Information Security Officer, typically at the college or upper administrative Unit level.

UISOO – Unit Information Systems Operations Officer. These are staff assigned system administration or operations duties, or managers of such staff (IT Directors for example).

Unit – an entity of administrative organization at the University of Illinois. The term is defined respectively by the University under its Statutes, and by its Office of Business and Financial Services:

1) The University of Illinois Statutes, as amended January 24, 2013 http://www.uillinois.edu/trustees/statutes.cfm describes Units at:

Article III. Campuses, Colleges, and Similar Units

Section 1. The Campus

a. The campus is the largest educational and administrative group. It is composed of colleges, schools, institutes, and other educational units in conjunction with administrative and service organizations.

Section 4. The School and Similar Campus Units
Article VIII. Changes in Academic Organization

Section 1. Definitions

a. Unit. For the purposes of Article VIII, a unit is a division of the University to which academic appointments can be made and to which resources can be allocated, including departments or similar units, centers, institutes, schools, and colleges.

2) The University of Illinois Office of Business and Financial Services (OBFS) defines a functional reporting Unit (such as a school, college, or department) with discrete financial activities as an organization, and utilizes a segment of the C-FOAPAL accounting string to identify Banner chart/org combinations that define university business units.

The OBFS Banner Alerts and Resources at http://www.obfs.uillinois.edu/banner-alerts/ give instructions on accessing the Banner FIFGRORGH (Organization Hierarchy) report of organizations (functional reporting Units with discrete financial activities) at the University.

University business process – see business process: a process or function carried out by a Unit and its Workforce in the course of executing its role assigned by the University, or which supports or facilitates such activity.

University Data – A type of University Information Asset, data created or acquired by the University and its Workforce in the course of planning or carrying out University business processes (Business functions).

University Information Asset – all Information Assets with value to the University as defined by one or more of the following criteria:

1) their usage in University business processes as identified in Policy DCS.2.1 Identify Core Business Functions,

2) by the reputational risk to the University if the availability, integrity, or confidentiality of the University Information Asset is compromised,

3) resources consistent with the definition of the University’s data in the University’s Office of Business and Financial Services’ Business and Financial Policies and Procedures, Section 19.5 “Information Security Policy - The University of Illinois” http://www.obfs.uillinois.edu/bfpp/section-19-business-systems-access-security/section_19_5/

defines a **vulnerability** as “(a) weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a **threat** source.”

**Whole/Full Disk Encryption (FDE)** - the process of encrypting all the data on a physical hard drive, or aggregation of physical hard drives through RAID technology.

**Workforce** – All University employees with appointments in a specific Unit, and also employees of external companies engaged in University contracts to carry out University **business processes** utilizing University Data for a Unit.

**Workstation** – any computer hardware which is implemented to provide user access to University systems, applications, or data regardless of the technology by which the data is stored, transmitted to, or accessed by that Workstation.

Workstations include traditional terminals and notebook, laptop, portable and desktop personal computers as well as tablet computers, personal digital assistants, and mobile / wireless / broadband telephone or other such network access devices.
# Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator/Approver</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Begin Overview and Policy assembly in October 2011 from UIC HSC IT Security Policies Version 3.0 source, and proceed with composing Version 0.1 Program to meet campus IT Security needs.</td>
<td>11/21/12</td>
</tr>
<tr>
<td>0.1</td>
<td>UIC Information Technology Governance Council - Infrasec Committee</td>
<td>Approved Version 0.1 of Overview and Policy and advanced to ITGC Council. Council approved development of Procedures, Guidelines and Standards by Committee necessary to implement Program</td>
<td>1/9/13</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Information Technology Governance Council - Infrasec Committee</td>
<td>Approved Version 1.0 of Program Procedures, Guidelines and Standards and advanced Program to Deans Council, and to Chancellor and Vice Chancellor Committees</td>
<td>2/12/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Deans Council</td>
<td>Reviewed Version 1.0 of Program and advanced to Chancellor and Vice Chancellor Committees</td>
<td>3/11/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Chancellor and Vice Chancellor Committee</td>
<td>Approved Version 1.0 of Program and the Implementation Plan prepared for it by the UIC IT Security Program Committee for the UIC campus</td>
<td>3/18/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Faculty Senate</td>
<td>UIC CIO presented Program</td>
<td>4/24/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>7/1/14</td>
</tr>
</tbody>
</table>
Section 6: SPO

University of Illinois at Chicago
Information Technology Security Program Overview
Version 1.0 7/1/14

SPO.1 Introduction
   SPO.1.1 Nondiscrimination Statement
   SPO.1.2 Minority Impact Statement
   SPO.1.3 Accessibility Impact Statement
   SPO.1.4 Group Impact or Special Concerns Statement

SPO.2 Mandatory Adoption and Compliance
   SPO.2.1 Individual Compliance
   SPO.2.2 Unit Compliance
   SPO.2.3 Key Words in this Program to Indicate Requirement Levels

SPO.3 Delegation

SPO.4 Information Security Program Goals

SPO.5 Information Security Program Components

SPO.6 Modification of the Information Security Program

SPO.7 Roles and Responsibilities
   SPO.7.1 The ITGC Infrastructure and Security Subcommittee (InfraSec)
   SPO.7.2 The UIC Information Technology Security Committee
   SPO.7.3 The Campus Chief Information Officer (CIO)
   SPO.7.4 The Campus Information Security and Privacy Officer (CISPO)
   SPO.7.5 Unit Heads
   SPO.7.6 Unit Information Security Officers (UISO)
   SPO.7.7 The Campus Community
   SPO.7.8 Information Technology Security Program Delegates

SPO.8 Reporting Inability to Implement Program

Table of Abbreviations
Change Log
Revision History
SPO.1 Introduction

The University of Illinois at Chicago (UIC) has adopted this Information Technology Security Program ("Program") to provide a unified structure for information technology security across its campus. The Program consists of Policy as well as its associated Standards, Procedures, Guidelines and Forms. This Program is a statement of the minimum requirements, responsibilities, and accepted behaviors within a Best practice\(^1\) framework required to establish and maintain a secure information technology environment within the University, as well as to achieve the Program’s SPO.4 Information Security Program Goals.

The Program emphasizes UIC’s commitment to strong information security; all individuals who use the information technology resources of the University are required to adhere to this Program. The University of Illinois at Chicago Information Technology Security Program Committee of the Information Technology Governance Council’s (“ITGC”) Infrastructure and Security Committee (“InfraSec”) is charged with providing oversight and maintenance of this Program for the University. As directed by its PM Policy Maintenance Policy, this Program will be reviewed for effectiveness and efficiency on an annual basis and modified as needed.

The University’s Combined Covered Entity\(^2\), including all Colleges and Units within UIC, is committed to securing and protecting High Risk Data\(^3\) (including electronic Protected Health Information (ePHI)\(^4\)),

\(^1\) See “Best practice” in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”


\(^3\) See High Risk Data in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

\(^4\) See ePHI in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
Sensitive Data Collections\(^5\) and Sensitive Data\(^6\) (including Family Educational Rights and Privacy Act (FERPA\(^7\)) data), in accordance with widely accepted information systems security Best Practices and standards, including those established by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC); the ISO/IEC 27000 series of Information Systems Security standards; the National Institute of Standards and Technology (NIST) Information Security Standards and Guides, and the Standards for Security and Privacy of individually identifiable health information established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) subject to later modification by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 as part of the American Recovery and Reinvestment Act (ARRA) of 2009.

SPO.1.1 Nondiscrimination Statement

This Program adheres to the University of Illinois Nondiscrimination Statement\(^8\) and is committed to the principles of academic freedom, equality of opportunity, and human dignity. Any questions or concerns on this Program’s impact on nondiscrimination should be addressed to the Program’s responsible officers at itsecpolicy@uic.edu.

SPO.1.2 Minority Impact Statement

The University of Illinois at Chicago adopted this Program to provide a unified structure for information technology security across its campus, and this Program is intended to be applied to all Units\(^9\), faculty and staff at UIC. It is further intended to provide the foundation to treat University Information Assets\(^10\) as strategic organizational assets, and in a manner consistent with that of other strategic assets of the University such as financial and facility assets.

The manner in which this Program is implemented is not intended or expected to have a capability to advance diversity on campus, and it is also not expected to have any differential or adverse impact on diversity at the campus\(^11\). Any questions or concerns on this Program’s minority impact should be addressed to the Program’s responsible officers at itsecpolicy@uic.edu.


\(^7\) See FERPA in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”


\(^9\) See Unit in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

\(^10\) See University Information Asset in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

SPO.1.3 Accessibility Impact Statement

After reviewing accessibility principles with the Disability Resource Center\(^{12}\) no impediments to accessibility were identified in the Security Program Overview or Policy. The review for potential accessibility issues will be done for each procedural element of the Program as it is developed, and addressed accordingly. Any questions or concerns on this Program’s impact on accessibility should be addressed to the Program’s responsible officers at itsecpolicy@uic.edu.

SPO.1.4 Group Impact or Special Concerns Statement

This Program from its initiation has sought representation from Units across the business enterprise of the campus in its own membership, including members from primarily educational and administrative Units, respectively. Further campus representation came by virtue of the Program being created within the control, oversight, review and approval of the campus Information Technology Governance Council\(^{13}\), which in turn has representative members from across the campus Units and also includes representation of the student body. The campus Office of Policy Development\(^ {14}\), Office of Diversity\(^ {11}\), and Disability Resource Center\(^ {12}\) were contacted to identify and review whether aspects of the Program would disproportionately or uniquely impact groups. No such concern was identified, but any questions or issues related to group impact should be addressed to the Program’s responsible officers at itsecpolicy@uic.edu for prompt assessment.

SPO.2 Mandatory Adoption and Compliance

SPO.2.1 Individual Compliance

Any individual who uses any University information technology resources including University Information Assets, whether with University or personally owned equipment, consents to all of the applicable portions of this Program and agrees to comply with all conditions and terms of use, as well as applicable state and federal laws and regulations. Workforce\(^ {15}\) members have a responsibility to use University resources in an ethical and lawful manner. Consequences of violations of this Program are stated in Policy RC.3 Sanctions for non-Compliance.

SPO.2.2 Unit Compliance

Each Unit must adopt all applicable elements of the UIC Information Technology Security Program.

\(^{12}\) Disability Resource Center www.uic.edu/depts/oaa/disability_resources

\(^{13}\) Information Technology Governance Council http://itgc.uic.edu/committees/itgc/

\(^{14}\) Office of Policy Development http://www.uic.edu/depts/oaa/policies

\(^{15}\) See Workforce in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
SPO.2.3 Key Words in this Program to Indicate Requirement Levels

The Program and all of its Information Security Program Components (defined at SPO.5) uses the following definitions derived from the Network Working Group’s RFC 2119\(^\text{16}\):

a. MUST, REQUIRED, or SHALL means that the definition is an absolute requirement of the specification.

b. MUST NOT or SHALL NOT means that the definition is an absolute prohibition of the specification.

c. SHOULD or RECOMMENDED means that while a particular specification is intended to be met by the Program, there may exist valid reasons in certain circumstances to consider an alternative to a particular specification. The full implications must be understood, carefully weighed, and the reasons for selecting the alternative must be documented and approved before choosing and implementing the alternative.

d. SHOULD NOT or NOT RECOMMENDED means that the Program does not approve a particular specification, but recognizes there may exist valid reasons in selected circumstances when the particular specification is acceptable or even useful. The full implications of proceeding with the specification must be understood, carefully weighed, and the reasons for selecting that specification must be documented and approved before implementing it.

SPO.3 Delegation

Because this Program requires Units to create certain roles and perform specified actions, it is recognized that Units may delegate duties herein to internal units, other campus units, or external vendors. If a duty is delegated outside the Unit, then the delegating Unit must create a Service Agreement defining what is delegated and to whom it is delegated. The Unit must remain responsible for monitoring and compliance of those delegated duties.

SPO.4 Information Security Program Goals

This Program provides and enforces Policy, Procedures, Standards, and Guidelines in order to meet the following University goals:

a. University Information Assets including University Data\(^\text{17}\) must be regarded as strategic organizational assets and be treated in a manner consistent with that of other strategic assets of the University such as financial and facility assets. University Information Assets must be protected from unauthorized disclosure, modification, use, disruption, or destruction, regardless of location. Prudent steps must be taken to ensure

---

\(^{16}\) https://www.ietf.org/rfc/rfc2119.txt

\(^{17}\) See University Data in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
that the appropriate confidentiality\textsuperscript{18}, integrity, and availability of the data are not compromised\textsuperscript{19}.

b. University Information System security must be addressed by integrating security safeguards into Unit University business processes\textsuperscript{20} and not as an isolated technical concern.

c. A comprehensive training program for all Workforce members should instill a culture of Information Security awareness across the entire University community.

d. In order to minimize the impact on resources, this Program will focus on those issues that represent the greatest risk to operations and University Information Assets.

e. Risk Management methods shall be used by the University business process identified risk owners to identify and manage risks including threats\textsuperscript{21} to University Information Assets and information technology resources.

f. Metrics will be used and data collected to evaluate effectiveness of and drive continuous improvements and efficiencies in the implementation of this overall Program.

g. Information Security incidents must be promptly detected and responded to in a manner that mitigates the impact\textsuperscript{22} to the security of University Information Assets and to the operations of the University.

h. Reporting and Auditing of compliance shall be achieved through a combination of reporting including UISO reports provided herein and routine University audits.

\textsuperscript{18} See confidentiality, integrity, and availability each in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

\textsuperscript{19} See breach (compromise directs to breach) in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

\textsuperscript{20} See University business process in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

\textsuperscript{21} See threat in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

\textsuperscript{22} See impact in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
SPO.5 Information Security Program Components

This Program consists of the Information Security Policy ("Policy") as well as its associated Standards, Guidelines, Procedures, and Worksheets or Forms ("Program Components").

a. The Policy broadly defines Program Information Security requirements.

b. The Standards list minimum specifications that must be maintained to be in compliance with the referring Program Policy or Procedure.

c. The Guidelines are Best practice processes and specifications that should be followed to meet Program requirements, but Units may develop alternate processes if they meet the overlying Policy and Standards requirements.

d. The Procedures are specific directives that must be followed where applicable to ensure consistent, repeatable, auditable, and reportable implementation of the Program’s Information Security practices.

e. The Worksheets or Forms ensure standard reporting of Program activities, events, and results.

SPO.6 Modification of the Information Security Program

Although Units may modify the components of the Program to meet the needs of their Units, their modifications cannot increase risk or exposure without compensating mitigation, and must meet the intended functionality of the applicable Program Components.

Modifications to specific Program Components must be addressed as follows:

a. While modifications may be proposed under the provisions as follows:

1. The modification proposal must include a cancellation date for the modification which cannot exceed a period of one year after the proposed date of implementation, and must identify the entity accepting risk for the modification,

2. Modification proposals must be submitted to the Unit Information Security Officer ("UISO") for review in advance of implementation,

3. The modifications can only be implemented if approved by the UISO, and

4. Any modification that needs to be extended beyond its cancellation date must be submitted for a new review under this section (SPO.6.a.1).

5. Upon discontinuation of modification, the UISO and CISPO must be informed.

b. The UISO must report any modifications approved or extended by the UISO to
InfraSec at least 30 days before implementation. (This feedback is necessary so InfraSec can assess the effectiveness of the Program Components.)

c. If InfraSec determines the risk is not correctly identified or not accepted by the correct party, InfraSec may recommend revision of the modification to the UISO.

d. Within this Program, Infrasec has the final authority to approve, modify, or disallow any modification to this Information Technology Security Program at any time.

SPO.7 Roles and Responsibilities

This Program shall be implemented collaboratively by the ITGC Infrastructure and Security Committee, its UIC Information Technology Security Committee, the Campus Chief Information Officer, the Campus Information Security and Privacy Officer, Unit Heads, Unit Information Security Officers, and the Campus Community.

There are Campus Information Technology Principals (“Principals”), external to the Units, which provide campus or University-wide information technology services: specifically ACCC, AITS, and University of Illinois Hospital and Health Sciences System. When the services and resources of those Principals are utilized, their Policies must also be complied with, in addition to those of this Program. The Program implementation responsibilities are as follows:

SPO.7.1 The ITGC Infrastructure and Security Committee (InfraSec)

The ITGC Infrastructure and Security Subcommittee (“InfraSec”) is charged with providing oversight for this Program. InfraSec shall:

a. Create and maintain the Program, delegating that to its UIC IT Security Committee.

b. Advise, inform, and coordinate with the Unit Information Security Officers as appropriate, to promote, facilitate in active practice, and support the Security Program.

c. Communicate with Principals as appropriate to ensure coordination of the Program with the Principals’ Information Technology Security Policies, Standards, Guidelines and Procedures.

d. Upon request of the University President, Chancellor, or Provost, and in collaboration with the UISOs, provide information on Security Program risk management decisions and direction to ensure alignment with University objectives.

e. Report to the UIC Information Technology Governance Council the effectiveness and status of the Program at least annually or as requested.
SPO.7.2 The UIC Information Technology Security Committee

InfraSec charged its UIC Information Technology Security Committee (“UIC IT Security Committee”) on 7/20/12 to continue its then ongoing work on creating this Program, directing:

a. The UIC IT Security Committee to create an IT Security Program to secure University data including across devices.

b. This IT security program will:
   1. align with industry Best practices,
   2. include a compliance reporting aspect,
   3. and consist of Policies, Procedures, Standards and Guidelines.

c. A primary goal while the UIC IT Security Committee develops the Program is to minimize unnecessary work while still protecting the data and devices within a risk management framework it establishes.

d. The UIC IT Security Committee shall prepare a report of:
   1. Recommendations on Program component implementation order, and
   2. Cost and resource estimates for Program implementation.

Operating under that charge, the UIC IT Security Committee completed this Program and submitted it to Infrasec for review and approval. Infrasec then forwarded the program to ITGC for review. Ultimately, the UIC Chancellor and Vice Chancellor Council approved the resulting Program on 3/18/14 for application to the UIC campus. Since that time the UIC IT Security Committee has maintained this Program as delegated to it by Infrasec at Policy SPO.7.1.a below.

SPO.7.3 The Campus Chief Information Officer (CIO)

The Campus Information Officer (CIO) guides the UIC ITGC Infrastructure and Security Subcommittee in setting program strategic goals and operational objectives that align with UIC’s mission.

SPO.7.4 The Campus Information Security and Privacy Officer (CISPO)

The Campus Information Security and Privacy Officer (CISPO) serves in a variety of technical and non-technical roles for the University campus and shall:

a. Provide day-to-day Information Technology Security Program management for the campus, advise Units on IT Security issues, and assist the UISOs with reviews and reporting.

b. Provide leadership by communicating the Security Program and its components to the campus community.
c. Assist Units with evaluating risks to University Information assets.

d. Assist with the preparation, approval, and maintenance of campus-specific and Unit-specific Information Technology Security policies, procedures, and guidelines as appropriate.

e. Establish and manage an IT Security awareness program.

f. When an IT Security incident affects the campus, lead investigations and coordinate with and/or report to the Provost, other Campus Principals, University Combined Covered Entity HIPAA Security and Privacy Officers, University Counsel, University Police, and others as appropriate.

g. Meet any other objectives defined by this program aimed at reducing risk to the University of possible IT Security incidents.

SPO.7.5 Unit Heads

a. Unit Heads must assign a person to fulfill the Unit’s Unit Information Security Officer (UISO) role.

b. Unit Heads are responsible for ensuring that all applicable Program requirements are implemented in their respective Units.

c. SPO.7.6 Unit Information Security Officers (UISO)

Unit Information Security Officers (UISOs) provide day-to-day management of the Security Program at the College or Vice Chancellor level and general advice on IT Security issues. Each Unit Information Security Officer shall:

a. Implement, manage, and maintain the Security Program within their Unit.

b. Review, report, and advise on the Security Program efficacy, including risk management, to their Unit Head and InfraSec as required.

c. Suggest improvements or additions to the Program’s Policies, Standards, Procedures, and Guidelines to InfraSec.

d. Submit reports to InfraSec on risk management decisions made by the Unit Head or referred by the Unit Head to a higher-level authority.

e. When a significant information security incident affects the Unit, lead investigations and coordinate with and/or report to the Unit Head, CISPO Office and other Principals, University Combined Covered Entity HIPAA Security and HIPAA Privacy Officers, University Counsel, University Police, and others as defined in Policy RC.5 Reporting and Responding to IT Security Incidents.
SPO.7.7 The Campus Community

The Campus Community are participants in the University business processes, and they include its Workforce, research partners, affiliates, Business Associates covered by Business Associate Agreements, and those individuals who, through their participation in the University’s business practices, have access to the University’s non-Public Data in the performance of their responsibilities, or in the course of obtaining information or services from the University.

Campus Community members who access University Information Assets categorized as non-Public under this Program (see Policy DCS.1 Data Classifications) are responsible for protecting the university information they access in any format; store on any media; or copy, reproduce, or transfer. As described at Policy PER.2 Job Descriptions, Responsibilities, and Training, as part of the hiring process, University employees must execute a User Acceptable Use Agreement as provided by this Program.

a. As so required by Policy SS.1.d Establish Workstation, Data Storage Device, and Server Access Controls, a Workstation or Server user must consent to a System Acceptable Use Agreement before utilizing a System allowing access to High Risk Data, or other Data classifications as determined by the Unit in the course of its execution of Policy DCS.2.5 Implement Risk Management Program.

b. As described in Policy SA.1 Security Training Program, Workforce training is provided. Furthermore a UIC Information Security Program Primer is available to assist Workforce members in meeting the requirements of this Program including its Policies.

SPO.7.8 Information Technology Security Program Delegates

Workforce members who have been assigned a Program responsibility or implementation duty by a UISO are referred to as “Delegates.”

The following support responsibilities are implicitly delegated by the UISOs:

a. Information Technology support and development personnel (such as application developers, database administrators, desktop support staff, network analysts, Server administrators, and webmasters) shall implement all applicable Program requirements within their areas of responsibility.

1. Policies DCS.2.4 Conduct Risk Assessment and DCS.2.5 Risk

---

23 “Campus Community” is defined in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
24 “Workforce” is defined at ibid.
25 See DCS.10, Business Associate Agreement and DCS.10G, Business Associate Agreement Guideline
26 See University Information Asset at “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
Management Program provide an operational framework for Units to perform a Risk Assessment and implement a Risk Management program in the Unit.

2. Additionally, as security concerns or breaches are recognized by the Unit IT support and development personnel, Policy RC.5 Reporting and Responding to IT Security Incidents provides a mechanism for them to report those emergent matters.

SPO.8 Reporting Inability to Implement Program

b. If any Unit staff member (“Reporter”) identifies a potential or actual conflict in their responsibilities under the Program, or in their implementation of any Program requirement, or is unable to implement a Program requirement when so required by the Program, then:

1. The Reporter must report the conflict or implementation inability on a timely manner to their UISO, who must address the matter.

2. This Policy recognizes that the Reporter, in addition to these provisions, may also seek guidance from the University Ethics Office, and may review the terms of the University Business and Financial Policies and Procedures, Section 9.6, Disclosure of Wrongful Conduct and Protection from Reprisal (Whistleblower Protection).

http://www.ethics.uillinois.edu/policies/whistle.cfm
Table of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARRA</td>
<td>American Recovery and Reinvestment Act of 2009</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td>CISPO</td>
<td>Campus Information Security and Privacy Officer</td>
</tr>
<tr>
<td>Delegates</td>
<td>Staff organizationally under a UISO assigned Program responsibility or implementation duties</td>
</tr>
<tr>
<td>ePHI</td>
<td>electronic Protected Health Information</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act of 1996</td>
</tr>
<tr>
<td>HITECH</td>
<td>Health Information Technology for Economic and Clinical Health Act of 2009</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>InfraSec</td>
<td>Infrastructure and Security Subcommittee</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITGC</td>
<td>Information Technology Governance Council</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-Disclosure Agreement</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PCI-DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>Principals</td>
<td>Campus Information Technology Principals</td>
</tr>
<tr>
<td>Program</td>
<td>Information Security Program</td>
</tr>
<tr>
<td>Program Components</td>
<td>Information Security Standards, Guidelines, Procedures, and Forms</td>
</tr>
<tr>
<td>UIC</td>
<td>The University of Illinois at Chicago</td>
</tr>
<tr>
<td>UISO</td>
<td>Unit Information Security Officer</td>
</tr>
</tbody>
</table>
Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>7/1/14</td>
<td>Completion of revisions to earlier 3/1/14 draft UIC IT Security Program Overview</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator/Approver</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Begin Overview and Policy assembly in October 2011 from UIC HSC IT Security Policies Version 3.0 source, and proceed with composing Version 0.1 Program to meet campus IT Security needs.</td>
<td>11/21/12</td>
</tr>
<tr>
<td>0.1</td>
<td>UIC Information Technology Governance Council - Infrasec Committee</td>
<td>Approved Version 0.1 of Overview and Policy and advanced to ITGC Council. Council approved development of Procedures, Guidelines and Standards by Committee necessary to implement Program</td>
<td>1/9/13</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Information Technology Governance Council - Infrasec Committee</td>
<td>Approved Version 1.0 of Program Procedures, Guidelines and Standards and advanced Program to Deans Council, and to Chancellor and Vice Chancellor Committees</td>
<td>2/12/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Deans Council</td>
<td>Reviewed Version 1.0 of Program and advanced to Chancellor and Vice Chancellor Committees</td>
<td>3/11/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Chancellor and Vice Chancellor Committee</td>
<td>Approved Version 1.0 of Program and the Implementation Plan prepared for it by the UIC IT Security Program Committee for the UIC campus</td>
<td>3/18/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Faculty Senate</td>
<td>UIC CIO presented Program</td>
<td>4/24/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>7/1/14</td>
</tr>
</tbody>
</table>
Section 7 Information Security Policy Sections

University of Illinois at Chicago
Information Technology Security Program
Policy Sections
Version 1.0 7/1/14

Summary

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Security Training Program</td>
<td>Data Classifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Data Classification and Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Systems Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Network Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Disaster Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Personnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Reporting and Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Policy Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Awareness

SA.1 Security Training Program
SA.2 Security Reminders
SA.3 Protection from Malicious Software
SA.4 User Password Compromise

Data Classification and Security

DCS.1 Data Classifications
DCS.1.1 High Risk Data
DCS.1.2 Sensitive Data
DCS.1.3 Sensitive Data Collection
DCS.1.4 Internal Data
DCS.1.5 Public Data

DCS.2 Data Risk Management
DCS.2.1 Identify Core Business Functions
DCS.2.2 Identify Relevant Information Systems
DCS.2.3 Annually Classify Data
DCS.2.4 Conduct Risk Assessment of Data
DCS.2.5 Implement Risk Management Program

DCS.3 Access Authorization
DCS.4 Encryption and Decryption of Stored Data
DCS.5 Accountability for Hardware and Electronic Media containing Unencrypted High Risk Data or Sensitive Data Collections

DCS.6 Cloud Computing Services Storage

DCS.7 High Risk Data or Sensitive Data Collections Transmission Security
   DCS.7.1 Data Transmission Integrity Controls
   DCS.7.2 Data Transmission Confidentiality Controls (Encryption)
   DCS.7.3 Messaging (Including but not limited to email) Security
   DCS.7.4 Transmission of High Risk Data or Sensitive Data to Entities External to the University of Illinois

DCS.8 Develop Data Backup and Storage Procedures
DCS.9 Develop and Implement Media Reuse Procedures
DCS.10 Methods Used for Disposal of All Storage Media
DCS.11 HIPAA Business Associate Agreement

Systems Security
   SS.1 Systems Monitoring
   SS.2 Establish Workstation and Server Access Controls
   SS.3 Identify Workstation Types and Functions or Uses
   SS.4 Establish Protection from Malicious Software
   SS.5 Automatic Locking
   SS.6 Workstation and Server Network Access Controls
   SS.7 Workstation and Server Intrusion Detection
   SS.8 Email Server Malware Protection
   SS.9 Remote Access
   SS.10 Audit Control Mechanisms
   SS.11 Non-secure Systems
   SS.12 Insecure (Breached or Compromised) Systems
   SS.13 Cloud Computing Services

Network Security
   NS.1 Wireless Access
   NS.2 Unit Network Perimeter Security

Physical
   P.1 Facility Security Plan
   P.2 Analyze Physical Attributes of Surroundings
   P.3 Access Control and Validation Procedures
   P.4 Access to Software Programs
   P.5 Maintenance Records

Disaster Planning
   DP.1 Data Backup Plan
   DP.2 Disaster Recovery Plan
   DP.3 Contingency Operations Procedures
   DP.4 Emergency Mode Operation Plan
DP.5 Testing and Revision Procedure
DP.6 Applications and Data Criticality Analysis

Personnel
PER.1 Identify Access Needs of All Users
PER.2 Job Descriptions, Responsibilities, and Training
PER.3 Ensure Unique Identifiers Have Been Assigned
PER.4 Access Establishment and Modification
PER.5 Access Authorization
PER.6 Termination of Access

Reporting and Compliance
RC.1 Audit Control and Review Plan
RC.2 Develop and Implement the Information Systems Activity process
RC.3 Sanctions for non-Compliance
RC.4 Common Incident Response and Reporting System
RC.5 Reporting and Responding to IT Security Incidents
RC.6 Unit Information Security Officer (UISO) Annual Report Policy
RC.7 Retention of the UISO Annual Report

Policy Maintenance
PM.1 Creating and Maintaining the Information Security Program

Table of Abbreviations
Revision History
Security Awareness

SA.1 Security Training Program

The Unit will ensure that its Workforce members have been given the appropriate level of High Risk Data and Sensitive Data security training so that all individuals who access, receive, transmit, or otherwise use High Risk Data and Sensitive Data are familiar with this Program and his or her responsibilities regarding that Program. Their appropriate training is required and may include the following:

- University Policies including this Information Systems Security Program
- Relevant State and Federal Regulations, including FERPA and PIPA
- Confidentiality, integrity, and availability
- Individual security responsibilities
- Common or well-known security threats and vulnerabilities
- Password management
- Server, desktop, and mobile system security procedures, including security patch and update procedures, and virus and malicious code protection
- Device and media physical control procedures
- Incident response and reporting procedures
- Federal HIPAA regulations and sanctions for non-compliance
- Business Associate agreements

SA.2 Security Reminders

The CISPO office shall send periodic security reminders to the University community to keep the community aware of current threats and Best practices\(^\text{27}\) as well as of any modifications to this Program.

SA.3 Protection from Malicious Software

The CISPO or UISO, as appropriate, will notify the Workforce of significant new and potential threats from malware, denial of service attacks, or any other computer program or code designed to interfere with the availability, integrity, or confidentiality of University Information Systems.

SA.4 User Password Compromise

If an individual believes the password for any account used by them to access a University Information System has been compromised, they must report it as a security incident to the entity that issued the account, and to their UISO.

\(^{27}\) See Best practice in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
Data Classification and Security

The underlying reason for this Information Security Program is to protect the University Information Assets at UIC. Data exists in many forms and on many types of media. In addition, data may have varying value and importance to the University depending on what it represents and the business functions it facilitates at various times.

The key to determining how data needs to be protected is to classify it. We must think about the importance of the data to the University and what would happen to the University if the data were altered without permission or exposed to people who should not have access to it.

DCS.1 Data Classifications

Four classes of data are defined globally for the University of Illinois: High Risk, Sensitive, Internal, and Public. This Program defines an additional fifth class, Sensitive Data Collection. The University classifications are repeated here for completeness.

DCS.1.1 High Risk Data

High Risk Data is information that, if disclosed or modified without authorization, would have severe adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information in this class includes, but is not limited to:

a. Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, such as credit card information (covered by the Payment Card Industry Data Security Standard (PCI DSS)).

b. Information covered by federal and state legislation, such as the federal Health Insurance Portability and Accountability Act (HIPAA) or the Illinois Personal Information Protection Act (IL PIPA).

c. Payroll, personnel, and financial information with special privacy requirements.

DCS.1.2 Sensitive Data

---

28 See University Information Asset in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

29 The four classes are defined at the “University Information Security Policy, approved as Interim by UTMT 9/8/2009 and subsequently provisionally revised 2012” http://www.uis.edu/campussenate/docs/agendas/documents/10-04-23UniversityInformationSecurityPolicy.pdf

Sensitive Data is information that, if disclosed or modified without authorization, would have serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information that is covered by FERPA, Non-Disclosure Agreements (NDAs), and other intellectual property are, as a minimum, in this class.

Note: Non-Disclosure Agreements may fall into the High Risk Data or Sensitive Data categories and should be individually evaluated.

DCS.1.3 Sensitive Data Collection

In addition to these University classifications, this policy creates a further distinction in the University Sensitive Data classification:

A Sensitive Data Collection is a collection of Sensitive Data that results from compiling (i.e., collecting) the Sensitive Data from multiple sources. For example, an instructor’s compilation of grades from courses they teach, held on their own computer, would not be a Sensitive Data Collection. However, a department’s compilation of all the grades for all the classes in the department would be a Sensitive Data Collection.

Where a requirement is given in this Program for Sensitive Data, the same requirements apply to Sensitive Data Collections as a minimum threshold. Sensitive Data Collections are specifically identified in this program where a more restrictive or extensive requirement is applied to a Sensitive Data Collection than Sensitive Data.

DCS.1.4 Internal Data

Internal Data is information that, if disclosed or modified without authorization, would have moderate adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

DCS.1.5 Public Data

Public Data is information intended for public use that, when used as intended, would have no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

DCS.2 Data Risk Management

In order to appraise and manage the risk associated with storing and using University Information Assets, a Data Risk Management program will be implemented through these five successive steps:

a. Identify Core Business Functions (DCS 2.1)
b. Identify Relevant Information Systems (DCS 2.2)
c. Annually Classify Data (DCS 2.3)
d. Conduct Risk Assessment (DCS 2.4)
e. Implement Risk Management Program (DCS 2.5)
DCS.2.1 Identify Core Business Functions

Each Unit must annually identify its Core Business Functions. Guideline DCS.G.2.1 describes how this should typically be done utilizing core business functions already defined by the Unit as part of its compliance with completing the University’s Kuali Ready Business Continuity Planning for the Unit.

DCS.2.2 Identify Relevant Information Systems

As directed by Guideline DCS.G.2.2, each Unit will annually prepare an inventory report of all systems it administers and then determine which systems are used to collect, store, process, or transmit High Risk Data, Sensitive Data Collections, or Sensitive Data.

DCS.2.3 Annually Classify Data

To ensure that all data that has a risk associated with it is protected properly, each Unit will perform an annual classification of data on the systems it administers. This assessment will highlight systems used to collect, store, process, or transmit High Risk Data, Sensitive Data Collections, Sensitive Data, Internal Data, or Public Data. Guideline DCS.G.2.3 provides Best practice guidance on meeting this requirement.

DCS.2.4 Conduct Risk Assessment of Data

As directed by Guideline DCS.G.2.4, each Unit accessing or storing High Risk Data, Sensitive Data, or Sensitive Data will conduct an annual assessment of the potential risks and vulnerabilities that may compromise the confidentiality, integrity, and availability of that High Risk Data, Sensitive Data Collections, and Sensitive Data. A report of the assessment will be provided as a supplement to the annual inventory. The Risk Assessment will:

a. Address the open items and mitigation efforts noted in previous assessments or audits.

b. Identify events that can potentially impact system security or operations.

c. Identify system vulnerabilities in and security threats to physical and technical safeguards.

d. Identify systems where additional data integrity solutions are required.

e. Assess the impact a security breach or prolonged disruption in service will cause.

33 See Core Business Function in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
DCS.2.5 Implement Risk Management Program

As directed in Guideline DCS.G.2.5 Risk Management Program Implementation, each Unit will implement a risk management program sufficient to reduce the risk and vulnerabilities to a reasonable and appropriate level.

The Risk Management Program will ensure the confidentiality, integrity, and availability of High Risk Data, Sensitive Data Collections, and Sensitive Data; protect against reasonably anticipated threats or hazards; and prevent any reasonably expected prohibited disclosures of information.

DCS.3 Access Authorization

Any individual requiring access to High Risk Data, Sensitive Data Collections, Sensitive Data, or Internal Data repositories must be approved by the Data Steward before being granted access. The Unit that grants the access must retain documentation supporting the approval and granting of the access per Guideline DCS.G.3 Access Authorization.

The documentation for this Access Management, if already regulated by Campus IT Principals and meeting Guideline DCS.G.3 documentation requirements, does not need to be replicated by Guideline DCS.G.3 as long as the Unit can obtain reports on that Access Management meeting the needs of this Program.

Personnel Procedure PER.P.5 Access Authorization, requires that the manager, supervisor, and/or department head or delegate must perform an annual review of the roles and individuals who have been granted access to High Risk Data, Sensitive Data, Sensitive Data Collections, or Internal Data.

DCS.4 Encryption of Stored Data

High Risk Data and Sensitive Data Collections must be encrypted when stored on portable data storage devices including flash drives, laptops, handheld devices, and removable media. Minimum data encryption storage specifications must meet or exceed the DCS.S.4 Data Encryption Storage Standard.

Encryption of High Risk Data or Sensitive Data on non-portable devices as an access control mechanism is not required unless the custodian of the High Risk Data or Sensitive Data has, by means of the physical security and risk assessment identified in Policy DCS.2.4 Conduct Risk Assessment of Data, deemed it a necessary control.

See “Portable data storage device” in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
DCS.5 Accountability for Hardware and Electronic Media Containing Unencrypted High Risk Data or Sensitive Data Collections

In any instance under which Policy DCS.4 is not complied with, and High Risk Data or Sensitive Data Collections present on portable storage devices and/or media are not stored encrypted, a procedure must be implemented to track the individual storage devices and/or media containing the High Risk Data or Sensitive Data Collections, their movement, and the parties in physical possession of and responsible for the devices and/or media.

Any backup media containing unencrypted High Risk Data or Sensitive Data Collections must be inventoried and tracked.

DCS.6 Cloud Computing Services Storage

Cloud Computing Services requirements are generally given at SS.13 Approved Cloud Services which defines the general University requirements for utilizing any Cloud Computing Services. The DCS.S.6 Cloud Computing Services Storage Standard will define any standards this Program defines for Cloud Computing Storage used for University Data.

Following the overarching requirement of the SS.S.13 Standard, the DCS.S.6 Standard will specify that Cloud Computing Services Storage of any High Risk Data or Sensitive Data Collections must meet the applicable requirements of this Program, and must be Endorsed by the UIC CIO or Campus Information Technology Principals.

DCS.7 High Risk Data or Sensitive Data Collections Transmission Security

All transmissions, including messaging transmissions, of High Risk Data or Sensitive Data Collections over insecure networks or any other insecure communications channel, must be secured in a fashion that protects the integrity and confidentiality of the data. Specifically:

a. The identities of the sender and the recipient must be authenticated. If the transmission is unidirectional from the sender to the recipient, then the identity of the recipient must be authenticated.

b. The recipient must agree to participate in the data transmission.

c. The data transmission must be encrypted. Either the data transmission channel must be encrypted, or the data must be encrypted prior to transmission according to the requirements of Policy DCS 7.2 Data Transmission Confidentiality Controls (Encryption) (see below).


d. The sender and receiver are aware of the risks involved respectively in sending and receiving the High Risk Data or Sensitive Data collections.

DCS.7.1 Data Transmission Integrity Controls

All High Risk Data transmissions over insecure networks must be digitally signed to ensure that modification without detection does not occur.

DCS.7.2 Data Transmission Confidentiality Controls (Encryption)

Data encryption transmission security settings must meet or exceed the minimum DCS.5.7.2 Data Transmission Confidentiality Controls Standard as specified by the Campus Information Security Officer.

DCS.7.3 Messaging (Including but not limited to email) Security

In addition to the preceding DCS.7 High Risk Data or Sensitive Data Collections Transmission Security requirements:

a. The Workforce, including select student employees as identified by a Unit in Policy PER.2 Job Descriptions, Responsibilities, and Training, must use university administered messaging systems (e.g. email, instant messaging, document sharing) to conduct university business.

b. Since Policy DCS.7 High Risk Data or Sensitive Data Transmission Security requires High Risk Data or Sensitive Data to be encrypted, High Risk Data or Sensitive Data is not permitted in the subject line or other unencrypted areas of any message.

DCS.7.4 Transmission of High Risk Data or Sensitive Data to Entities External to the University of Illinois

The transmission from a Unit or Workforce member to entities outside the University of Illinois of High Risk Data or Sensitive Data Collections, or High Risk Data or Sensitive Data via a messaging or data transfer system is permitted if the sender has ensured that Policy DCS.7 High Risk Data or Sensitive Data Transmission Security conditions are met, and furthermore:

a. Workforce members must use a University administered secure data transfer system to transmit High Risk Data or Sensitive Data Collections to external entities;

b. However, if the external entity requires use of its own data transfer system, the Workforce member must be able to verify the requirements of this Policy’s Section DCS.7 have been met prior to utilizing the external entity’s system.
DCS.8 Develop Data Backup and Storage Procedures

Data should be backed up in accordance with the Unit Data Backup Plan identified in Policy DP.1 Data Backup Plan.

DCS.9 Develop and Implement Media Reuse Procedures

Procedure DCS.8 must be implemented for the removal of High Risk Data, Sensitive Data Collections, Sensitive data, and Internal data from media before the media is made available to the Unit or to others outside the Unit for reuse.

DCS.10 Methods Used for Disposal of All Storage Media

Before relinquishing control or possession of storage media, all High Risk Data, Sensitive Data, or Internal Data on it must be rendered unrecoverable or the media the data is stored upon must be destroyed.

   a. The Unit shall follow the ACCC University Guideline on the Sale, Donation, or Transfer of Computer Hard Drives and Other Magnetic Media\(^{37}\). All data destruction should be done in accordance with data retention guidelines, if established.

   b. For storage devices not specifically identified in the Data Security on State Computers Act or in the University policy, High Risk Data, Sensitive Data Collections, Sensitive Data, and Internal Data must be rendered unrecoverable before disposal.

   c. If a process cannot be implemented to remove High Risk Data, Sensitive Data Collections, Sensitive Data, or Internal Data, then the UISO should be consulted for instructions.

DCS.11 HIPAA Business Associate Agreement

Any data collection, storage or processing activity that would disclose Protected Health Information (PHI) to a third party must be covered by an Agreement that documents satisfactory assurances by the third party that they will protect the data in a manner consistent with this Policy. This agreement may be in the form of a research agreement or contract approved through the Office for the Research Services for data sharing between institutions or a Business Associate agreement if dealing with an external entity (vendor) who performs or assists in the performance of University operations involving PHI. In accordance with University policy, all such documents are reviewed by University Counsel to obtain institutional endorsement.

\(^{37}\) [http://accc.uic.edu/policy/disk-scrubbing](http://accc.uic.edu/policy/disk-scrubbing)
Systems Security

SS.1 Systems Monitoring

Use of any system, authorized or unauthorized, constitutes to consent to monitoring of the system. Systems may be monitored by the CISPO, UIISO, or delegate to ensure their use is authorized, for management of the systems, to facilitate protection and assurance against unauthorized access to systems, and to verify security procedures, business continuity, disaster recovery, and operational security of systems. Monitoring may include active scans or attacks initiated by the security officer or the system’s administrator to test or verify the security of the system. During monitoring, information including user’s personal information placed upon or transmitted by the system to the network may be monitored.

SS.2 Establish Workstation and Server Access Controls

a. Any device meant to be accessed remotely by one or more users must meet the requirements of Procedure PER.1 Identify Access Needs of all Users.

b. Each user must consent to the System Security Standard SS.5.1.a System Acceptable Use Agreement before utilizing a Workstation or Server allowing access to High Risk Data or Sensitive Data Collections.

SS.3 Identify Workstation Types and Functions or Uses

Units that handle High Risk Data must utilize the listing of Workstations administered by the Unit from the inventory prepared under Policy DCS.2 Identify Relevant Information Systems, and then must ensure that the proper business functions can be performed at Workstations by:

a. Classifying Workstations into types based on the location, mobility, capabilities, connections, and allowable activities for each.

b. Developing policies and procedures for the allowed usage of each type of Workstation, identifying and accommodating their unique issues while securing them and permitting their correct utilization.

SS.4 Establish Protection from Malicious Software

To protect the confidentiality, integrity and access to data on university computers, all systems must have security software installed and enabled that protects the computer from malicious software.

SS.5 Automatic Locking

To prevent unauthorized access, all computers accessing University non-Public Data must be configured to automatically lock the device after a period of inactivity as specified in the Systems Security Standard SS.4 Automatic Locking.
Public Access Systems\textsuperscript{38} are specifically exempted from this Policy SS.4. As an example, a Unit may define publicly accessible information kiosks and ACCC administered Pharos print stations as Public Access Systems if they are identified and evaluated in the Policy DCS.2.4 Conduct Risk Assessment and DCS.2.5 Implement Risk Management Program processes.

**SS.6 Workstation and Server Network Access Controls**

Workstations and Servers may provide network services (services accessible via network connections). While Unit Network Perimeter Security may implement some access controls for the Workstation or Server network services, it is often advisable to implement complimentary, possibly broader scope, network access controls on the Workstations or Servers as well.

Access controls should be implemented for Workstation or Server network services:

a. All unnecessary network services should be disabled.

b. Access control lists should be configured and implemented for each active network service, defining the allowed, or denied, protocol, port and network connections.

c. The method with which any access control list is implemented should be documented. Examples include a host operating system packet filtering firewall (e.g. Microsoft Windows operating systems firewalls, or Linux iptables). When implemented, the current access control list must also be documented by the Unit.

**SS.7 Workstation and Server Intrusion Detection**

Intrusion detection facilitates regular appraisal of the effectiveness of network perimeter and host network access controls, and the forensic investigation of potential or actual intrusion activity.

a. Intrusion detection must be implemented following Standard SS.5.3.b.2.xii, System Standard for All Workstations, for all Workstations containing data classified as High Risk Data or Sensitive Data Collections.

b. Intrusion detection must be implemented following Standard SS.5.3.b.4.i, System Standard for All Servers, for all Servers containing data classified as High Risk Data or Sensitive Data Collections.

c. Per the above Standards, detected intrusion activity must be logged, and intrusion logs must be reviewed regularly.

\textsuperscript{38} See Public Access System definition in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
SS.8 Email Server Malware Protection

Any Unit implementing an email Server must implement malware protection, intercepting any incoming or outgoing malware including viruses.

a. All Units maintaining email Servers must scan incoming and outgoing email and attachments at those Servers for malware. The scan function may be offloaded to a separate Server or appliance.

b. Detected malware, or the messages or data transmissions they are contained in, must be disinfected or quarantined before the messages or data transmissions are further relayed or made accessible.

c. Logging of detected malware must be performed and the action taken must be recorded and reportable.

d. Logs of such activity must be reviewed regularly.

SS.9 Remote Access

All systems allowing remote login (or remote desktop) access must be configured to meet or exceed the Remote Access standards set forth in the Systems Security Standard SS.5.9 Remote Access Standard.

Note: Remote login/desktop access to Workstations should be disabled unless there is a business need that cannot be satisfied using less invasive technologies or methodologies.

SS.10 Audit Control Mechanisms

a. Each Unit will implement system-level logging mechanisms for all systems that contain High Risk Data or Sensitive Data Collections. The recorded log events must be stored on a separate event or log management system.

b. Where the system has the capability, for each user obtaining access to High Risk Data or Sensitive Data, each system’s audit log will include at least the User ID, User IP Address, Login Date and Time, and Logout Date and Time.

SS.11 Non-Secure Systems

a. Personal computers not administered and secured by Unit staff under Policy SS.2 Establish Workstation and Server Access Controls are non-secure systems, but still subject to regulation by this Program since:

Policy SPO.2.1 Individual Compliance establishes the foundation for Individual Compliance:

“Any individual who uses any University information technology resources including University Information Assets, whether with University or personally owned equipment, consents to all of the applicable portions of the Program and agrees to comply with all conditions and terms of use”.

52
Individuals who access Information Assets categorized as non-Public under this Program (see Policy DCS.1 Data Classifications) are responsible for protecting the university information they access in any format; store on any media; or copy, reproduce, or transfer.

b. Therefore, the reasonable steps Workforce members should take utilizing Non-Secure Systems:

1. to access University systems, or
2. on which to store non-public University data

to ensure those non-secure systems meet a minimum security baseline include:

As in Policy PER.3 Ensure Unique Identifiers Have Been Assigned,

1. Ensure that unique user identification and authentication is established for all individuals utilizing the non-secure system, even if some but not all of those individuals access non-public University data with the system. Do not share a login for use by more than one individual if activities accessing or storing non-public University data are done by one of the system users.

2. Each user's password must meet the ACCC Common Password Strong Password Policy given at http://www.uic.edu/depts/accc/accts/altpswd.html

As in Policy SS.6 Workstation and Server Network Access Controls:

3. Disable all unnecessary network services

4. Configure and implement Access control lists for each active network service, defining the allowed, or denied, protocol, port and network connections.

As in Policy SS.4 Establish Protection from Malicious Software

5. To protect the confidentiality, integrity and access to data security, install and enable campus site licensed security (antivirus/malware) software http://accc.uic.edu/tag/antivirus that protects the computer from malicious software.

As in Policy SS.7 Workstation and Server Intrusion Detection

6. Implement and log Intrusion detection.

c. Per Policy RC.5 Reporting and Responding to IT Security Incidents, a Non-Secure System experiencing an incident that may affect the confidentiality, integrity, or availability of High Risk Data or Sensitive Data Collections must be reported and responded to by following Procedure RC.P.5 Security Incident Response and Reporting. The UISO may request the Workforce member to provide intrusion logs and other configuration and forensic information from the system.
SS.12 Insecure (Breached or Compromised) Systems

When a Threat has been executed upon a University Information System such that unauthorized changes have occurred or are possible to its configuration, programs, or data, the system is **insecure**. An **Insecure System**\(^{39}\), also known as a **Breached or Compromised System**, can no longer be guaranteed to meet intended University confidentiality, integrity, or availability needs and standards. It is **prohibited** to connect an Insecure System to a University network, and to use the system for any University Business Process\(^{40}\). Insecure systems must be processed through the **RC.P.5 Reporting and Responding to IT Security Incidents Procedure**, section **RC.P.5.1.2 Breached Workstation or Portable Data Storage Device**.

SS.13 Cloud Computing Services

The development of cloud computing has virtualized the services which were once provided by physical computing devices or storage devices and physical infrastructure belonging to the service user’s Unit. Virtualized cloud services are typically leased, with lease terms commonly including specifications of capacity provided, capacity upgrades available, and service levels. As a Unit’s IT needs have moved to a virtual environment, the direct administration a Unit once over its equipment has been spliced onto or laid upon virtualized services administration, typically at an external Unit or service provider.

NIST defines cloud computing as NIST in “The NIST Definition of Cloud Computing” (2011) [http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf](http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf): “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, Servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.”\(^{41}\)

The five essential characteristics under the NIST definition are on-demand self-service provisioning of computing capabilities, broad network access to the service, resource pooling, rapid elasticity in provisioning capabilities, and automated and optimizing service measurement.

The three service models (three tier architectural model) of cloud computing services are: **Software as a Service** (SaaS), **Platform as a Service** (PaaS), and **Infrastructure as a Service** (IaaS)\(^{42}\). This model can further be extended with tiers for **Desktop as a Service** (DaaS), **Backend as a Service** (BaaS), and **Information Technology Management as a Service** (ITMaaS).

The four deployment models are **Private cloud**, **Community cloud**, **Public cloud**, and **Hybrid cloud**.

---

\(^{39}\) See Insecure System definition in “**UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions**”

\(^{40}\) See University business process in “**UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions**”

\(^{41}\) See Cloud Computing Services at “**UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions**”

\(^{42}\) Software Defined Networking (SDN) can be implemented as IaaS
The Program will be developing a **SS.S.13 Cloud Computing Services Standard**, and **DCS.S.5 Cloud Computing Storage Services Standard**.

SS.S.13 will advise that a Unit needs to carefully consider the relative security risks under each deployment model. In general, the Private Cloud deployment can be more readily secured than the other models. A Hybrid Cloud, guaranteeing “Private Cloud” security and configuration/control options at the service model level the Unit requires, E.g. SaaS or PaaS, but upon an underlying Community Cloud IaaS, may be a reasonable choice after the Unit performs a risk assessment and risk management plan for each type of deployment and determines the Hybrid Cloud deployment defined for them meets their needs.

The SS.S.13 Standard will specify that overall any Cloud Computing Services utilized for a University Business Process involving High Risk Data or Sensitive Data Collections must meet the applicable requirements of this Program, and must be Endorsed by the UIC CIO or Campus Information Technology Principals.

At this time, a Network Security section of the Program is not being prepared for IaaS.

---

Network Security

NS.1 Wireless Access

The University and the ACCC define access controls for wireless network implementation and access at UIC.

Unit wireless network access points providing access to the Unit and ACCC networks may be permitted when all of the following security measures have been implemented:

a. Encryption must be enabled.

b. Unique user identification/Password authentication must be enabled and all access must be logged.

c. All wireless access points must meet ACCC minimum requirements given in [http://accc.uic.edu/service/wireless/department](http://accc.uic.edu/service/wireless/department)

d. Wireless network access point activation must be approved in advance by ACCC.

NS.2 Unit Network Perimeter Security

Any Unit implementing or utilizing a network or networks will define the scope or extent of that Unit network as being any network administered by the Unit and which the Unit’s Workstations, data storage devices, or Servers have direct access to or the capability to directly access.

With respect to the Unit network, access points to other networks from that Unit network are defined as Unit network perimeter access points and define the perimeter of the Unit network.

a. Units will, in accordance with their risk management plan, implement network perimeter security and corresponding network access controls including the use of network firewalls, routers, or VLANs.

Units at UIC mostly utilize the ACCC as combined Ethernet and wireless network infrastructure provider, and internet service provider.

If the ACCC is the sole infrastructure and internet service provider, the ACCC network access controls should be used and, suitably configured at the network perimeter, can constitute a complete set of network perimeter security provisions.

b. The configuration of the firewalls, routers, VLANs, or other network access controls used to protect the Unit network environment must be documented and available to the Unit and the campus IT Principals.
Physical Security

P.1 Facility Security Plan

The Units will at least annually analyze and rank the existing physical security vulnerabilities of any location where its Workstations, data storage devices, and Servers are located according to the specifications of Guideline P.G.1 Facility Security Plan, and will develop a Facility Security Plan to protect that equipment from unauthorized physical access that could lead to theft, tampering, or unauthorized viewing, altering or erasing of data.

P.2 Analyze Physical Attributes of Surroundings

As part of the Facility Security Plan, Units will analyze the physical surroundings of each Workstation, data storage device and Server identified in the inventory under Policy DCS.2.2 Identify Relevant Information Systems in order to:

a. Determine which types of facility locations require physical access controls to safeguard data.

b. Determine whether changes in physical access controls or equipment location are required in order to reduce risk associated with the physical location to a level acceptable by the Unit. This evaluation is part of the DCS.2.4 Conduct Risk Assessment of Data process.

P.3 Access Control and Validation Procedures

Based upon the outcomes of the assessment of the preceding Policy P.2.b, Analyze Physical Attributes of Surroundings, the Unit may implement procedures to control and validate an individual’s access to facilities based on their role or function, including visitor control procedures. A facility with Servers containing High Risk Data or Sensitive Data Collections must have appropriate automated logging mechanisms for access to the facility.

P.4 Access to Software Programs

All Units that handle Protected Health Information must:

a. Create and maintain a list of software programs used by the Unit to access or manipulate ePHI.

b. Create and implement procedures to control access to these software programs for their use, testing, and revision.

P.5 Maintenance Records

Within the context of the Facility Security Plan, the Units will document repairs and modifications to the physical components of a facility that are related to physical security.


Disaster Planning

DP.1 Data Backup Plan

a. Each Unit will establish and implement a Data Backup Plan that will detail all backups to be performed, media used for the backups, security considerations, location used to store the backups, and procedure for recovery of the backup data.

b. The Data Backup Plan will be documented and available to key personnel.

c. All individuals with specific responsibilities in the Data Backup Plan must be trained in those responsibilities.

d. Data Backup Plans for Units that handle Protected Health Information must detail plans to create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

DP.2 Disaster Recovery Plan

a. The Units will maintain a Disaster Recovery Plan (DRP) with procedures to recover the Unit’s systems and data.

b. The Unit will periodically assess if the DRP meets the Unit’s business continuity plan requirements and report the results of their assessment to the UISO.

c. Where information technology or data is managed by a third party to the Unit or its primary technology support unit, the Unit will be responsible for ensuring the third party can meet or exceed its required DRP components.

d. The Unit will document procedures necessary for providing business continuity to contract partners, grant agencies, and business associates as documented within said grants, contracts, and business associate agreements.

e. The current Disaster Recovery Plan will be accessible off-site by key personnel in the event of a disaster.

f. All individuals with specific responsibilities in the Disaster Recovery Plan must be trained in those responsibilities.

DP.3 Contingency Operations Procedures

The HIPAA Security Regulation section 164.310(a)(2) (i) states “Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.”
Units that handle Protected Health Information must coordinate with the appropriate campus units to develop procedures to allow facility access in support of the restoration of lost data in the event of a disaster or an emergency.

**DP.4 Emergency Mode Operation Plan**

The HIPAA Security Regulation section 164.308(a)(7) (i) states “Standard: Contingency plan. Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.”

The HIPAA Security Regulation Section 164.308(a)(7) (i) (C) continues, “Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.”

An Emergency Mode Operation Plan must include provisions to meet HIPAA Security Regulation 164.312(a)(2) (ii), “Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.”

Units that handle Protected Health Information must:

a. Establish procedures to enable the continuation of University business processes in Critical Levels 1, 2 and 3 to ensure protection of the security of ePHI while operating in Emergency Mode. This is referred to as the Emergency Mode Operations (EMO) plan.

b. Train all individuals with specific responsibilities in the EMO plan.

c. Document the EMO plan and make it available to key personnel.

**DP.5 Testing and Revision Procedure**

a. Each Unit will establish a process to test their Data Backup Plan, Disaster Recovery Plan, and as appropriate, Emergency Mode Operations Plan. Individuals must be trained in their specific responsibilities, roles and duties prior to testing.

b. Each plan will be tested periodically and results/findings will be documented and shared with key personnel.

**DP.6 Applications and Data Criticality Analysis**

Each Unit subject to HIPAA regulations will assess the relative criticality of their specific applications and data in support of other Contingency Plan components. This list must be used when creating the Unit’s Disaster Recovery Plan, Data Backup Plan and Emergency Mode Operations Plan to ensure that the most critical applications are backed up and restored in the appropriate order.
Personnel

PER.1 Identify Access Needs of All Users

The Unit must develop and document procedures to determine the access needs of all Workforce in their Unit. The Units must maintain an inventory of all applications, systems, and data repositories housing High Risk Data or Sensitive Data Collections to determine who requires access and whether any use or access of High Risk Data or Sensitive Data Collections is available to unauthorized individuals.

PER.2 Job Descriptions, Responsibilities, and Training

a. The Unit must ensure that all Workforce accessing High Risk Data have been properly screened in accordance with UIC HR guidelines for Applicants selected for Security Sensitive Positions (UIC HR Policy Number 317) and Applicants Selected for Health Care Positions (UIC HR Policy Number 318).

b. The Unit must ensure that Workforce accessing High Risk Data, Sensitive Data Collections, or Sensitive Data are adequately trained, knowledgeable, and familiar with the policies and procedures for handling that data.

c. The Unit must ensure that all Workforce accessing FERPA data have been properly trained on the Student Records Policy, including completing the FERPA tutorial hosted by the Office of Admissions and Records.

d. An annual review of data access privileges of all Workforce within the Unit must be performed in conjunction with each Unit manager.

PER.3 Ensure Unique Identifiers Have Been Assigned

The Units must ensure that unique user identification and authentication is required for all individuals accessing High Risk Data or Sensitive Data Collections, and is established as noted below:

a. Each Workforce member must be provided with a unique user identification and authentication credentials to utilize when accessing Workstations, Portable data storage devices (including Laptops), Servers, and University Information Assets. A centrally administered University identity management system should be used to manage this identity information wherever possible.

b. Each user's password must meet the ACCC Common Password Strong Password Policy given at http://www.uic.edu/depts/accc/accts/altpswd.html

PER.4 Access Establishment and Modification

A Workforce member’s access to High Risk Data or a Sensitive Data Collections requires the following controls:
a. All individual access privilege assignments, changes, and deletions **must** be approved by the individual’s manager or supervisor, and/or department head.

b. Access privileges **must** be updated immediately when an individual’s job duties change such that their current access privileges are no longer appropriate, when the individual is no longer under the administrative control of the Unit granting the access privileges, or the individual is no longer employed by the University.

**PER.5 Access Authorization**

a. **Units** **must** create and implement a procedure to ensure that only authorized users are permitted access to High Risk Data, Sensitive Data Collections, or Sensitive Data.

b. **Any user requiring access to High Risk Data, Sensitive Data Collections, or Sensitive Data** **must** be approved through their manager, supervisor, and/or department head before being granted access to High Risk Data or Sensitive Risk Data.

c. When access to High Risk Data, Sensitive Data Collections, or Sensitive Data is granted, the Unit that grants the access **must** retain documentation supporting the approval and granting of user access to High Risk Data or Sensitive Data.

d. **Access Management** that is already regulated and reported by Campus IT Principals documentation requirements does not need to be replicated.

e. **Units** **must** ensure that the manager, supervisor, and/or department head or delegate **must** perform an annual review of the roles and individuals who have been granted access to High Risk Data, Sensitive Data Collections, or Sensitive Data.

**PER.6 Termination of Access**

As required by Policy **PER.4.b, Access Establishment and Modification**, each **Unit** **must** develop and implement a procedure for terminating access to High Risk Data, Sensitive Data Collections, and Sensitive Data including deactivation of computer access accounts; recovery of University computers, devices, and data; and recovery of access control articles such as identification badges, keys, access cards, etc.
Reporting and Compliance

RC.1 Audit Control and Review Plan

An Audit Control and Review Plan will be developed by the individual Units in conjunction with the CISPO office. On the basis of the previously completed Policy DCS 2.5 Risk Management Program, the plan will include:

a. A list of the systems and applications to be logged.
b. The information to be logged for each system or application.
c. The specifications for log reports for each system or application.
d. The procedures to review all audit logs and activity reports.
e. Details of how the UISO will confirm that the logs within their Unit are reviewed regularly by the Unit’s operational staff.

RC.2 Develop and Implement the Information Systems Activity process

a. The CISPO Office, in coordination with the ITGC InfraSec Committee, will establish and maintain Guidelines and Standards under this Program for regular review of information systems activity.

b. The Unit will issue procedures for their Unit compliant with the RC.2.a Standards, establishing information systems activity review responsibilities.

c. The UISO will monitor Unit compliance with the implementation of its Unit RC.2.b Procedures.

RC.3 Sanctions for non-Compliance

Any individual found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

a. The CISPO Office will establish a process to identify and report violations of this Policy and non-compliant disclosures of High Risk Data and Sensitive Data, including that covered by HIPAA, FERPA, and PIPA (Illinois Personal Information Protection Act).

b. Acceptable use, security awareness, and sanctions policies will be communicated to all staff.
RC.4 Common Incident Response and Reporting System

The campus Incident Response and Reporting System, as designated by the CISPO, will be used to report and document all IT Security Incidents including significant University Information Asset failures, outages, or data losses and their outcomes.

RC.5 Reporting and Responding to IT Security Incidents

Any IT Security Incident, defined as “an activity which may act as a threat to detrimentally affect or has affected the confidentiality, integrity, or availability of University data”, involving High Risk Data or Sensitive Data Collections must be reported and responded to by following Procedure RC.P.5 IT Security Incident Response and Reporting and using the following guidelines:

a. Incident Reporters must notify their U ISO of IT Security Incidents involving significant network or system-related attacks or unauthorized access attempts.

b. The U ISO will assign and manage an Incident Responder.

c. The U ISO will investigate and discuss possible remediation steps in response to IT Security Incidents and concerns. Incident Response will be coordinated by the Incident Responder with the U ISO and be based upon the Best practices guidelines of the NIST Computer Security Incident Handling Guide SP800-61.

d. When addressing and resolving HIPAA security and/or privacy related issues, the U ISO is responsible for initiating dialogue between their Unit and the University’s Combined Covered Entity HIPAA Security and/or HIPAA Privacy Officers.

e. The U ISO shall ensure that any initial contact need with any non-University parties regarding any IT Security Incident affecting University data or University Information Assets will be directed to the University’s Chief Information Security and Privacy Officer.

f. The University CISPO will direct any subsequent communication with any non-University party regarding such IT Security Incident.

---

44 See IT Security Incident definition in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”

45 See University Information Asset definition in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
RC.6 Unit Information Security Officer (UISO) Annual Report Policy

Each person defined under a Unit’s Procedure DCS 2.5 Risk Management Program, as responsible for a University Information Asset and acting within the scope of the risks managed by the Unit’s operational controls as implemented under Policy RC.2.c Develop and Implement the Information Systems Activity process, shall provide the UISO with the information requested by the USIO to evaluate the Unit’s Risk Management Program compliance with this Information Security Program. That information will provide the basis of the UISO Annual Report System.

RC.7 Retention of the UISO Annual Report

As described in the University of Illinois Records Management Program, the final versions of the UISO Annual report must be retained in compliance with the University Records Management Program. http://www.uic.edu/depts/lib/specialcoll/services/UA/UI_Rec_Mgt_2001.pdf
Policy Maintenance

PM.1 Creating and Maintaining the Information Security Program

An annual review of all Program Policies, Procedures, Guidelines, Standards and Forms by the IT Governance Council Infrastructure and Security committee is required.

*PM.P.1 Information Systems Security Policy Planning Procedure*, allows the creation and maintenance of this Program’s Information Technology Security Policies, Procedures, Guidelines, and Standards and Forms.

The procedure shall allow for Program Component Proposals, which are requests for additions to, modifications to, or removal of Program Policies, Procedures, Guidelines, or Standards and Forms. Program Component Proposals may be made by InfraSec or other participants in this Program.

The Procedure will also define necessary considerations for Program Component Proposal submissions, and a review and approval process.

The Procedure shall identify standard Policy, Procedure, Guideline, and Standards sections.

An annual review of all Program Policies, Procedures, Guidelines, and Standards and Forms by InfraSec is required.

Guideline *PM.G.1 Creating and Maintaining the Information Security Program*, directs that the Unit’s UISO must perform an annual review of all Unit created Program Policies, Procedures, Guidelines, Standards and Forms.
# Table of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARRA</td>
<td>American Recovery and Reinvestment Act of 2009</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning</td>
</tr>
<tr>
<td>CISPO</td>
<td>Campus Information Security and Privacy Officer</td>
</tr>
<tr>
<td>Delegates</td>
<td>Staff organizationally under a UISO assigned Program responsibility or implementation duties</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>EMO</td>
<td>Emergency Mode Operations</td>
</tr>
<tr>
<td>ePHI</td>
<td>electronic Protected Health Information</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act of 1996</td>
</tr>
<tr>
<td>HITECH</td>
<td>Health Information Technology for Economic and Clinical Health Act of 2009</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>InfraSec</td>
<td>Infrastructure and Security Subcommittee</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITGC</td>
<td>Information Technology Governance Council</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-Disclosure Agreement</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>Program</td>
<td>Information Security Program</td>
</tr>
<tr>
<td>Program Components</td>
<td>Information Security Policies, Procedures, Standards, Guidelines, and Forms</td>
</tr>
<tr>
<td>Principals</td>
<td>Campus Information Technology Principals</td>
</tr>
<tr>
<td>PCI-DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>UIC</td>
<td>The University of Illinois at Chicago</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator/Approver</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Begin Overview and Policy assembly in October 2011 from UIC HSC IT Security Policies Version 3.0 source, and proceed with composing Version 0.1 Program to meet campus IT Security needs.</td>
<td>11/21/12</td>
</tr>
<tr>
<td>0.1</td>
<td>UIC Information Technology Governance Council - Infrasec Committee</td>
<td>Approved Version 0.1 of Overview and Policy and advanced to ITGC Council. Council approved development of Procedures, Guidelines and Standards by Committee necessary to implement Program</td>
<td>1/9/13</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Information Technology Governance Council - Infrasec Committee</td>
<td>Approved Version 1.0 of Program Procedures, Guidelines and Standards and advanced Program to Deans Council, and to Chancellor and Vice Chancellor Committees</td>
<td>2/12/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Deans Council</td>
<td>Reviewed Version 1.0 of Program and advanced to Chancellor and Vice Chancellor Committees</td>
<td>3/11/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Chancellor and Vice Chancellor Committee</td>
<td>Approved Version 1.0 of Program and the Implementation Plan prepared for it by the UIC IT Security Program Committee for the UIC campus</td>
<td>3/18/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC Faculty Senate</td>
<td>UIC CIO presented Program</td>
<td>4/24/14</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>7/1/14</td>
</tr>
</tbody>
</table>
Section 8: Procedures, Standards, Guidelines and Worksheets
### SA.G Security Awareness Guidelines

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

### SA.G.0 Security Training Program Guidelines Purpose

Security awareness training is an essential part of any security program. It’s important that security awareness activities and training be initiated at the campus level to ensure that everyone is educated on their responsibilities to protect the information and equipment they use or maintain on a daily basis.

It is equally important, however, for Units to have a security training program as well. This not only helps ensure that all employees are aware of their responsibilities; it also allows the Unit to tailor the training for issues that are specific to the process that is used in that location.

### SA.G.1 Security Training Program Guidelines

a. What Training Should the Unit Supply?

As specified in [UIC Information Technology Security Program Policy SA.1 Security Training Program](#), the Unit must ensure that its Workforce members be trained on compliance with various laws and regulations, the proper handling of data based on its classification as well as other aspects of data security that may have an impact of protecting University data while performing their jobs.

Some of the topics outlined may be covered by training initiatives at the campus level and may not require any further training by the Unit while others may require the addition of Unit-specific training information. Other topics may not require the Unit to utilize documented resources to train their staff on the specific topics. For guidance on individual security training topics and resources available, please see [SA.G.1.a.4 Security Training Topics and Resources](#) below.
1. Compliance

The Unit should maintain records of training that can be used to demonstrate compliance with the Policy *SA.1 Security Training Program*. How these records are maintained is left up to the Unit, but they should contain at a minimum the name, date, UIN, training subject and the date of completion.

2. Renewal

The Unit should ensure that training is completed by each Workforce member *at least every two years*. Some topics may require more frequent training as documented below.

3. Updates

This document will be maintained with updated information regarding resources available for training. Units should check this document on a regular basis, and before performing new training activities.

4. Security Training Topics and Resources

As of this release of this Guideline, there are no individual security training topics and resources available

b. SA.G.1.b University Policies including this Information Systems Security Policy

All members of the Workforce should be made aware of the existence of this policy and be provided the URL where it can be accessed. All staff members should read the Program’s Policy Overview and Policy Sections, and understand that they are bound by its terms.

Staff members with specific duties that are covered in the policies should read the standards, procedures and guidelines that cover their specific areas of expertise. For example, members of the administrative arm of a Unit should most likely read and understand the sections of the policy, guidelines and procedures that deal with Security Awareness Training, Personnel and possibly Reporting and Compliance.

In general members of the IT staff for a Unit should read and understand the entire body of the Security Program.

c. Relevant State and Federal Regulations, including FERPA and PIPA

Information relating to the above external agency regulations may be placed here at a later date.
UIC Information Technology Security Program Procedures, Standards, Guidelines and Worksheets ver 1.0

**SA.G.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator</th>
<th>Description</th>
<th>Submission Date</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Mike Kirda</td>
<td>Initial composition</td>
<td>Sept. 17, 2013</td>
<td></td>
</tr>
<tr>
<td>0.9</td>
<td>UIC IT Security Program Committee</td>
<td></td>
<td></td>
<td>March 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.1.0 Introduction

Data in all its forms is one of the key assets of the University of Illinois at Chicago. The University and its employees are constantly in the process of generating, storing, using and sharing data in order to teach, conduct research, perform routine business, and accomplish a wide range of near- and long-term goals. In so many ways, data is the lifeblood of the UIC community, critical to the healthy, ongoing operation of the campus. Should a portion of that data become compromised or otherwise unusable, it could result in disruptions to teaching, research and other core services. It could also result in a negative financial impact, potential legal ramifications, and damage to the University’s reputation.

As with all valuable assets, University Data needs to be appropriately protected. As this data is collected and processed, it becomes the responsibility of the University, its employees, and all others who interact with this data to ensure the data is managed in an appropriate and secure fashion. What constitutes "appropriate" is mostly driven by legal, academic, financial and operational requirements and is based on the criticality and risk levels of the data. Some data can be freely shared with others, both internally and externally. Other data must be kept secure, following well documented policies and procedures and using appropriate data management controls to ensure that the integrity, availability, and confidentiality of that information are not jeopardized.

One of the most important steps in protecting data appropriately is to classify data into one of the defined data classification levels as defined in the UIC Information Technology Security DCS.1 Data Classifications Policy. The classification levels as defined are: High Risk Data, Sensitive Data, Internal Data, and Public Data46. In addition, this Program also defines a Sensitive Data Collection1, which is a stored aggregate of Sensitive Data.

---

46 See DCS.1, and also the in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
Who Should Classify?

It is common for people to assume that since IT manages the systems, they also own the data, but this is incorrect. IT is responsible for the systems that process and store the data and for maintaining the integrity of those systems, but not for deciding how data should be classified.

So who does decide how particular data should be classified? That generally falls to the Data Steward, the individual (or possibly, a group of individuals) who has a role with direct operational-level responsibility for management of University data – usually IT unit directors. When Data Stewards are trying to determine what classification some data should be, they are welcome to seek the help of the campus IT security group to assist them by providing some guidance, but the final determination for the classification is the data steward’s responsibility. The Data Steward is best qualified to make this decision because he or she has the most knowledge about the use of the data and its value to our organization. The Data Steward will also have to deal with the ramifications of any security breach of the data they are responsible for.

A Data Custodian is a person with a role responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by Data Stewards, and implementing and administering controls over the information. IT departments play an important part in serving as Data Custodians, but there may be other individuals or groups who serve in this role as well.

A Data User is an individual who uses University Data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to data have a position of trust, and as such are responsible for protecting the security and integrity of those data. They must follow appropriate procedures when they access the data, especially when the data they are using is not being housed on a managed Server (for example, when reports containing protected data are saved to a local computer, to a portable storage device, or transferred via e-mail). As Data Users, UIC employees and third-party contractors are obligated to handle all data in a manner appropriate with the data classification.

DCS.G.1.1 Data Classification Guidelines

In order to more easily manage data, it is important to understand the different types, or classes, of data and the policies, procedures, and guidelines to appropriately manage those sets of data.

Personally Identifiable Information (PII) is a specific classification of data that requires additional consideration, and constitutes data which in aggregate uniquely identifies an individual and can readily be used in conjunction with current publicly available data sources to compromise an individual’s credit, financial, medical identity or their choices in those areas. PII includes an individual’s first and last name, social security number, gender, date of birth, mother’s maiden name, driver’s license number, bank account information, and credit card information. Aggregated PII may be used to “steal” a person’s identity. Depending upon a Unit’s Policy DCS.2.4 Risk Assessment results, it may treat PII it aggregates or stores as Sensitive Data or High Risk Data.

See Personally Identifiable Information in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
Electronic protected health information (ePHI) is a subset of PII that includes health record information such as patient identification numbers, medical history, and treatments, as examples. Breach of this information may violate patient confidentiality, and be subject to strict fines and penalties as prescribed by HIPAA and the HITECH Act. Procedure RC.P.5 IT Security Incident Response and Reporting, requires that an information breach involving ePHI must be reported to the UIC HIPAA Privacy Officer and the campus CISPO. It may further require reporting to the US Department of Health and Human Services (HHS), amongst other state or federal agencies.

Directory information is a classification that contains limited personal information, but unlike PII, may be treated as Public data. Examples of directory information may include a portion of a personal record of a student generally available from published sources such as a telephone directory. The release of such information is not normally considered harmful or an invasion of privacy if disclosed. However, under the FERPA guidelines a student may declare directory information as confidential in which case it must be treated as Internal data.

It is interesting to note that sometimes data may be classified differently in different situations. For example, a person's name is considered PII when combined with other PII information, which puts it in the Sensitive Data or High Risk Data class. Yet the same name data may be considered directory information when in other situations, which puts it in the public classification. As you can see, sometimes the classification of data is not always clear cut. Data stewards will need to use their best judgment when choosing how to classify data depending on the situation.

**Data Classification Examples**

Recognizing that it can be difficult to determine the classification of pieces of data, we've provided the following table with some useful examples of how certain data items are typically classified. This is not an all-inclusive list, but it should demonstrate the range of information types typically handled at UIC along with typical classifications.

<table>
<thead>
<tr>
<th>Data Items</th>
<th>High Risk Data</th>
<th>Sensitive Data</th>
<th>Internal Data</th>
<th>Public Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN (including parent's and donor's)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protected health information (PHI)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Employee choice of wellness programs</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Education records</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Responses to faculty survey</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Driver's license number</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>State identification card number</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Data Items</td>
<td>High Risk Data</td>
<td>Sensitive Data</td>
<td>Internal Data</td>
<td>Public Data</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>University Identification Number (UIN)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Credit or debit card numbers</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit or debit card numbers security code</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit or debit card numbers password that permits access to account</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank account number</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic record</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates/license numbers</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer account information (i.e. payments, transactions or collections)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student loan agreements, loan balances, transactions, collection</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee counseling</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health of employee</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applicant interview results</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee benefit claim information</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Benefit enrollments, beneficiaries, workers comp/disabilities/family status change</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee retirement information</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Payroll deduction selections, registers, direct deposit, payroll reports, tax forms</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Tax ID number</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Donor personal information, credit cards, bank accounts, employment, family info, amount donated, medical history</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement Card numbers (P-Card)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Data Items</td>
<td>High Risk Data</td>
<td>Sensitive Data</td>
<td>Internal Data</td>
<td>Public Data</td>
</tr>
<tr>
<td>----------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Source files, license keys and installation documentation</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Student Date of birth (if student wants private)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Ethnicity</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Employee gender</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Religion</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Disability (physical, sight, or hearing)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Marital status</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Color or race</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Information on when/where people used building access cards</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Point of sale transactions</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ID cards</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Student cardholder accounts</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Information gathered on prospective applicant</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Convictions</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Resume</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Parent's financial records</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Veteran status</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Scholarship information</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Email communications on confidential matters</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Telephone number/fax number (could be public if part of student directory)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>University Course Catalog</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## Data Items

<table>
<thead>
<tr>
<th>Data Items</th>
<th>High Risk Data</th>
<th>Sensitive Data</th>
<th>Internal Data</th>
<th>Public Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>General web site information</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Information on classes, totals, demographics</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>General counseling services offered</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>General wellness program offerings</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Public job openings, duties, qualifications</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>General pay range for position opening</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Employee recruiting program</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>General employee benefits offered</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Payroll cycle/periods</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>General payroll deduction offerings</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Student Directory information (unless student wants private)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Employee compensation (can be found in gray book)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Email address (unless student invokes student confidentiality)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Age (unless student invokes student confidentiality)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Date and place of birth (unless student invokes student confidentiality)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Photographs (unless student invokes student confidentiality)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Student (unless student invokes student confidentiality)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Campus maps</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Bear in mind that Sensitive Data, if aggregated, may fall into the Data Classification of a Sensitive Data Collection, per DCS.1.3 Sensitive Data Collection: “A Sensitive Data Collection is a collection of Sensitive data that results from compiling (i.e., collecting) the Sensitive data from multiple sources”.

**DCS.G.1.2 Responsibility for Implementation**

The Unit head or delegate is responsible for the implementation of this Data Classification Guideline. The head of the IT unit, with review by the UISO, is typically responsible for making sure that the Guideline processes are performed annually.

**DCS.G.1.3 Definitions**

The definitions of Data Steward, Data Custodian, and Data user are given above in section DCS.G.1.0, Introduction.

**DCS.G.1.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Ed Zawacki</td>
<td>Initial document</td>
<td>Dec. 18, 2012</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

---

48 Data steward, Data custodian and Data user definitions are replicated in “UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions”
DCS.G.2.1 Identify Core Business Functions Guideline

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

DCS.G.2.1.0 Identify Core Business Functions Guideline Introduction

Information Technology at the University of Illinois at Chicago (UIC) exists, as in any institution, to support the University business processes and key critical functions within Units. Within a college or other administrative unit, Unit heads must identify Core Business Functions and their ‘criticality’ for the purposes of business continuity planning (BCP) and disaster recovery planning (DRP). Although this work may be delegated to Unit/departmental administrators, at UIC in BCP/DR planning the Unit head acknowledges the overall impact if a Core Business Function were not available during a disaster, or business could not function in full or in part due to a disaster.

DCS.G.2.1.1 Identify Core Business Functions Guideline Procedure

To facilitate this process, department and Unit heads enter their Core Business Functions into the UIReady (Kuali) tool, available at [https://us.ready.kuali.org/uic](https://us.ready.kuali.org/uic). To receive support and training on the application, UIC Ready Office contact information is available at [http://www.ready.uic.edu/](http://www.ready.uic.edu/)

Example Core Business Functions include instruction, research, patient care, meal services, pharmacy services, accounting, and many others. The screenshot below provides an example from the UIReady/Kuali system.
Generally Recommended Practice

A part of the University’s mandated Business Continuity planning by Units, Units must identify their Core Business Functions, even those that they believe would not be adversely affected during a disaster or crisis. Then, the Units choose how critical each Core Business Function is, and any service which supports the execution of each Core Business Function. More information on selecting criticality is found in DP.G.6 Applications and Data Criticality Analysis Guideline, and is part of the risk management process (as well as the BCP/DR process).

Once Units have identified and agreed to the critical processes supporting their Core Business Functions, Unit heads should meet together along with their dean, vice chancellor, or unit administrator, and key representatives from HR, IT, finance, and any other administrative area, to roll up mutual processes and prioritize those business functions.

This process will drive planning and form agreement for future work within IT systems and data for the next procedures the UISO will need to execute, especially those requiring identifying the relevant information systems that support Core Business Functions (DCS.G.2.2 Identify Relevant Information Systems Guideline), classifying the data needed to support University business processes (DCS.G.2.3 Annually Classify Data Guideline), and identifying and remediating risk to those processes through data management (DCS.G.2.4 Risk Assessment Guideline & DCS.G.2.5 Implement Risk Management Program Guideline).
DCS.G.2.1.2 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of this Identify Core Business Functions Guideline. The head of the Unit’s IT department, with review by the UISO, is typically responsible for making sure that the relationships and dependencies of IT System components in it are defined correctly and updated annually, or as significant system changes occur.

DCS.G.2.1.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial composition</td>
<td>Oct. 29, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.2.2 Identify Relevant Information Systems Guideline

Introduction

In order to more easily manage University Data, it is important to understand the different types, or classes, of data and the Program policies, procedures, and guidelines bearing upon them.

DCS.G.2.2.1 Information Systems Classification Guideline

Once a Unit has completed its data classification for information stored on its systems, and identified the Core Business Functions of the Unit, it is important that the Unit identify the computer systems on which the University Data its Data Stewards are responsible for resides, and where data is stored, accessed, and manipulated.

a. Step 1: Develop or use a template to collect and assess all potentially relevant information systems used in the Unit. A “Relevant Systems Inventory” ([DCS.W.2.2 Relevant Systems Inventory Worksheet](#)), is available to initiate this tabulation.

The Unit should use the data from its data classification survey to determine potentially relevant information systems used throughout it.

b. Step 2: Constrain the scope of the systems surveyed for data classification

At UIC, [DCS.2.1 Identify Core Business Functions](#) notes that a Unit’s existing need to comply with the University’s business continuity planning process allows it to identify its Core Business Functions. UIReady, which is the University of Illinois’ implementation of Kuali Ready

[https://us.ready.kuali.org/kcpt/plan/begin](https://us.ready.kuali.org/kcpt/plan/begin)
is an online database built by Units to list University Core Business Processes identified by them. Additionally, UIReady has an information technology section which can be used to list critical systems, as well as recovery time objectives (RTOs) and recovery point objectives (RPOs).

c. Additional Steps for Consideration:

1. The data available in Kuali Ready, or other sources, may only document part of a Unit’s overall Core Business Functions. For further consideration, bear in mind that historical data may quickly become out of date, or inaccurate. For this reason, a Unit needs to assess its relevant IT systems supporting the Unit’s Core Business Functions at least annually, and it is recommended the Unit uses a process driven by its business representatives or units, rather than have the identification of its IT systems solely driven by its IT unit.

2. IT systems that may support a Unit’s academic needs include ones utilized for exam scoring, grading, data entry, collaboration, research needs for generating and manipulating clinical or non-clinical research data, or other administrative needs (financial, decision making).

3. Finding the appropriate person who is accountable to accepting the risk for these systems (e.g. department/Unit heads, deans, vice chancellors, principle investigators (PIs)) is likely the best starting point on a first time or annual review of systems supporting University core business processes, as it provides that person insight into the process, the potential risk within the Unit, and opens communication for recommended best measures for future years.

Centralized IT/Smaller Unit/Dept:

If a Unit’s span of IT support is either highly centralized, directly supported, or includes a smaller set of systems, it may readily know the internal and external systems that are used to carry out University business processes in the Unit. In that case, for each system, it may consider designating an IT representative to work with the business unit designate who has responsibility for the system and its use.

Decentralized IT / Larger/Multiple Units Supported:

If a Unit’s span of IT support is broad or decentralized, it should consider assembling representatives from various groups in the Unit (business managers, financial officers, local IT representatives, research PIs) that may share or use similar systems, or potentially run their own local systems in the Unit.

DCS.G.2.2.2 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of this DCS.G.2.2 Identify Relevant Information Systems Guideline. The head of the Unit’s IT department, with review by the UISO, is typically responsible for making sure that the systems are identified periodically.
## DCS.G.2.2.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Phil Reiter</td>
<td>Initial document</td>
<td>Sept. 17, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
Placeholder for insertion of DCS.W.2.2 page 1 of 3 into PDF version of this document
DCS.G.2.3 Anually Classify Data Guideline

Purpose

UIC Information Technology Security Policy DCS 2.3 Anually Classify Data, requires that “each Unit will perform an annual classification of data on the systems it administers. This assessment will highlight systems used to collect, store, process, or transmit High Risk Data, Sensitive Data Collections, Sensitive Data, Internal Data, and Public Data.”

In order to protect your data, you first need to determine where your data lives and what the classification of that data is.

Although you may have a general sense of where different classes of data are stored, the process of data classification involves the data owners identifying and attesting to where their data is. Once completed, the data classification also drives later steps in reducing risk to data breach or exposure, such as conducting a risk assessment.

The University is a complex place and there’s usually a good chance that someone has data that you’re not aware of and it just might be stored in a location you’re not expecting.

Process

Who Should Perform this Classification?

Every Unit must perform this classification.

That being said, according to the role definition at UIC Information Technology Security Program section SPO.7.6.a, Unit Information Security Officers (UISO), each Unit Information Security Officer (UISO) shall “Implement, manage, and maintain the Security Program within their Unit.”
In other words, the UISO should coordinate the effort within their Unit to ensure that all sub-units are surveyed and accounted for. The UISO may coordinate the entire effort by his/her self or they may delegate part or all of the effort and simply act in a managerial role.

b. What Color is My Computing Environment?

In order to choose the best method to classify data for your Unit(s), it is important to first understand your computing environment.

In general, there is a wide spectrum of computing environments at the university.

Some units may have a highly centralized (spectrum: **HIGH-CENT**) and controlled computing environment in which they know exactly what equipment they have, what data they have and in addition they have a high level of security in their environment that may ensure that the data cannot be stored places they are not aware of.

On the other end of the spectrum, in some units everyone may host their own data or each Unit may do their own thing (spectrum: **DE-CENT**). In this type of environment, awareness of what computing equipment exists in their Unit or what type of data is stored may be limited.

The reality is that many units fall somewhere in the middle of the spectrum (spectrum: **MIXED**). They have a good idea where some of their data is, but not all of it.

![Diagram of computing environment spectrum](image)

The first step to finding and classifying the data in your Unit is to determine what type of environment you have.
c. My Unit is at the HIGH-CENT End of the Spectrum, What do We Need to Do?

If your Unit falls into the HIGH-CENT end of the spectrum, you may already know what data you have and where it resides. If so, the next step would be to complete the DCS2.3W, Data Classification Matrix Excel spreadsheet (or a similar worksheet) for each data resource that you have identified.

d. My Unit is in the middle of the Spectrum, with mixed significant HIGH-CENT and DE-CENT data, so how do We Start?

With varying degrees of data centralization within a Unit, falling into the MIXED part of the spectrum, you will basically need to follow the guidelines for both the HIGH-CENT and the DE-CENT spectrum units and combine the DCS.G.2.3.2.0.c HIGH-CENT and DCS.G.2.3.2.0.e DE-CENT guidelines to obtain the best coverage of the data to arrive at a clear idea of where the data is.

e. My Unit is at the DE-CENT End of the Spectrum, How do We Start?

If your Unit falls into the DE-CENT part of the spectrum, or you have not previously conducted a data classification, you will need to perform a survey to identify the systems and data that you are not currently aware of.

The recommended method is to use the Data Classification Survey that has been provided by the IT Governance InfraSec Committee for this purpose.

The survey was designed using the university-licensed Qualtrics system. Using the survey tool still requires work on your part in the form of determining who to send it to and analyzing the data when the survey is done, but the survey has been formatted to help you ask the right questions and record the responses in an organized fashion.

1. Steps to use the Qualtrics InfraSec Data Classification Survey:

   Obtain Access to the Survey

   i. Create a Qualtrics account. It is important that you create a Qualtrics account before proceeding to the next part as you will not be able to be granted access to the survey until you have created the account. See: http://accc.uic.edu/service/surveys

   ii. Send a request to security@uic.edu requesting access to the “InfraSec Data Classification Survey”
**Obtain Panel csv file**

iii. A PB Contact liaison can acquire a department email list from the PBUPDATE tool.

   A. Find your PB Contact liaison by visiting: http://tigger.uic.edu/htbin/cgiwrap/bin/webpbrw/liaison/data

   B. Ask your PB Contact liaison for the “Department - Email Only” Search/Report Type

      i. The PBUPDATE tool is located at: https://ness2.uic.edu/perl/pbupdate/pbupdate.cgi

      ii. Please note that this file should be saved as a .csv file

iv. **Create Panel and Import Panel Members**

   A. Login to Qualtrics at http://uic.qualtrics.com/

   B. From the Panels tab click the “Create New Panel” button

   C. This will progress you to the “Panel Members” section of the Panels tab

      Select “Add Panel Members” to individually add members, or select “Import From a File” to use your prepared csv file to import your Unit members

   **NOTE:** If you have not received confirmation that you have been granted access to the “InfraSec Data Classification Survey” please wait before proceeding.

v. **Edit, Activate and Distribute Survey**

   A. Login to Qualtrics at http://uic.qualtrics.com/

   B. You will see the “InfraSec Data Classification Survey” listed under the “My Surveys” tab

   C. You may wish to create a copy before making any changes to the original survey. If so, in the Tasks column, click the “Copy” link. Next, click the “Edit” link to review the survey and if necessary customize it to your Unit’s environment.

   D. In edit mode you may edit the text of a question or block of questions, delete a question or block of questions or rearrange the order of a question or block of questions

   E. **NOTE:** The survey has been designed to be launched as-is so most units will not require any modifications.

   F. Information about editing questions can be found on the Qualtrics website at http://www.qualtrics.com/university/researchsuite/
G. Once you are satisfied with the survey click the “Launch Survey” link in the menu bar

H. You will be prompted to activate the survey

I. Once you have activated the survey you will continue to the “Distribute Survey” tab.

J. In the “Distribute Survey” tab click the “Email Survey” link

K. At the To field navigate to the “My Library” selection and choose the previously created panel

L. Select “Entire panel”

M. At the “When” field you may select to send the message now or schedule it for the future
   Update the “When” field you may select to send the message now or schedule it for the future
   Update the From name, Reply-To Email and Subject as appropriate
   Be sure to enter a Subject as the default value is blank

NOTE: You may use the “Sample Qualtrics Survey E-mail” provided below or customize your own.

N. To access variables click the {a} in the format menu

O. Panel Field variables from your csv file are available to personalize the email message

P. After editing your message, click save to save your message to your library

Q. Depending on when you chose to schedule your mailing, in the bottom right will be a “Send Now” or “Schedule Mailing” button to distribute your survey

R. Your survey is now Active and awaiting responses

f. I think I know where my data is now, now what?

After you have completed the survey or used some other method to determine where your data is, you should use the provided Excel spreadsheet DCS.W.2.2 Relevant Systems Inventory Worksheet, to collect details about each Server, database, application, etc. that was identified in your data discovery process.
Note that this portion of the process is closely related to DCS.G.2.2 Identify Relevant Information Systems Guideline. As a result, the provided spreadsheet is intended to be used to fulfill both DCS2.2 and DCS2.3 requirements.

Sample Qualtrics Survey E-mail

Subject: IMPORTANT: Annual Data Classification Survey must be completed

Hi ${m://FirstName},

As part of ACCC’s effort to comply with the UIC Information Security Program, it is important that we identify and classify all data that our Unit handles.

To achieve that goal, we need you to complete the survey at the link below to the best of your ability.

NOTE: This is a test but I want you to complete the survey. It's okay to make up responses for the test. -- edz

Please respond to the survey by July 23, 2013.

Copy and Paste this link to take the Survey:
${l://SurveyURL}

Security is important! If you would like to verify the validity of this email, please send your question in email to security@uic.edu

DCS.G.2.3.2 Responsibility for Implementation

The Unit’s UISO is responsible for ensuring the Unit annually performs data classification.
DCS.G.2.3.3 Definitions

<table>
<thead>
<tr>
<th>Highly Centralized and Controlled Computing Environment</th>
<th>Highly centralized and controlled computing environment in which a Unit knows exactly what computing equipment they have, what data they have, and in addition they maintain a high level of security in their environment so that may ensure that the Unit data cannot be stored places the system administrators are not aware of.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE-CENT Computing Environment</td>
<td>Units in which each workforce member may host their own data or each subordinate Unit may do their own thing. In this type of environment, awareness of what computing equipment exists in their Unit or what type of data is stored may be limited.</td>
</tr>
<tr>
<td>MIXED Computing Environment</td>
<td>A mixture of varying levels of awareness of Unit University data distribution, and of the effectiveness of administrative control of the systems and data storage.</td>
</tr>
</tbody>
</table>

DCS.G.2.3.4 Resources

The DCS.W.2.2 Relevant Systems Inventory Worksheet and DCS.W.2.3 Data Classification Matrix for Guideline are provided in the Tools area of the UIC Information Technology Security Program website.

DCS.G.2.3.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Edward Zawacki</td>
<td></td>
<td>Oct. 29, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

49 HIGH-CENT, DE-CENT, and MIXED Computing Environment definitions are replicated in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
Placeholder for insertion of DCS.W.2.3 page 1 of 2 into PDF version of this document
DCS.G.2.4.0 Conduct Risk Assessment of Data Introduction

Once a Data Classification has been performed, the groundwork is laid for performing a risk assessment of data.

In general, a risk assessment begins with an understanding of the priorities of your Unit, the core functions that support those priorities, and as an outcome, determining the relative risk of being unable to perform those University core business functions. That concept is supported in the UIC Information Technology Security Program in its Policy DCS.2.1 Identify Core Business Functions by initiating risk assessment by identifying these functions.
DCS.G.2.4.1 Data Classification Guidelines

a. Risk Assessment Cycle
The University of Illinois has an established process for assessing risk through its Enterprise Risk Assessment office. As illustrated in the diagram below, this process establishes the four phases of the risk assessment cycle as discovery, evaluation, communication, and response.

Discovery – goals, risk environment & emerging risks
Evaluation – risk information & analysis
Communication – report to leadership & ROI
Response – influence decisions & planning

Discuss strategic risk
Gather data from risk owners & analyze
Report results
Discuss risk mitigation strategies
In the Discovery phase, the Unit should identify the current goals of the Unit and identify its goals for future delivery on its core mission, such as teaching, research, or clinical services, as examples. The conversation, in the context of IT support, should involve IT representatives hearing from leaders and representatives so IT has an understanding of the organization's goals as well as its willingness to accept risk to meet those goals. This is commonly referred to as risk appetite.

In the Evaluation phase, information is gathered on the state of the environment and their assessment of areas that pose the greatest risk or areas they may wish to minimize risk. This is an opportunity for the IT representative and Unit representatives to match potential IT risks to units capability to deliver on their mission, goals, or directly on services they provide. During this phase, a spreadsheet should be used to identify risks for scoring (see below) and ranking in partnership with local Unit representatives, and an agreement on relative ranking of risk should be formed. This should be driven by the business unit leaders, not IT. IT can advise on its perception of how technology factors into risk profiles and include its own ranking and scoring of risk for IT services in the sheet. Since this is an IT process rather than a general risk assessment, each risk area should have a component for IT risk associated with it.

In the Communication phase, IT and Unit leadership take the results as presented on the spreadsheet and present the completed spreadsheet and risk scores (See “Risk Scores”) to Unit leadership and present highest risk for discussion and awareness.

Finally, in the Response phase, methods of risk remediation (acceptance, transfer of risk, et al) are discussed. Unit leadership accepts the risk and chooses a course of action. IT leaders and teams may have to respond through implementation of some remediation method, and clearly communicate the resources and timeline necessary to meet those obligations.

It is recommended that this lifecycle be followed or adapted to meet your business unit’s needs to conduct an annualized risk assessment process.

Additionally, in general, a number of other Risk assessment models and control recommendations exist that are worth review. These models include, but are not limited to:

1. RiskIT – Standards and Controls for Risk Management established by ISACA, an IT Governance organization

http://www.isaca.org/riskit
https://www.isaca.org/
b. Risk Scoring

A key first step in conducting a basic risk assessment is to identify risks and score those relative risks. At the University of Illinois, this process is done using a risk score card which can rank relative ‘perceived risks’ in the organization.

It is recommended that key business unit/ organizational unit decision makers be assembled at least annually to perform the risk scoring exercise. Since these executive leaders are those which ultimately accept risk on behalf of the organization, it is important that they participate in the exercise as a team.

The ultimate goal is not necessarily to create precise qualitative numbers, but generalized risk rankings so all participants understand the relative risks to the business unit and agree on the rankings of those risks.

Clear communication is critical in this process, especially the promotion of awareness, understanding, and agreement, in this phase, as within identifying IT Systems that support the business practices, and mitigation strategies.

The University, like many other institutions conducting risk scoring, uses this simple formula to score risk:

\[
\text{Risk Score} = \text{Impact} \times \text{Control Effectiveness} \times \text{Likelihood}^{56} \text{ (of risk event occurring)}
\]

---

53 http://www.isaca.org/COBIT/Pages/default.aspx
54 http://www.iso.org/iso/home.htm
55 http://www.iso.org/iso/home/standards/iso31000.htm
56 See likelihood in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
Impact\textsuperscript{57} refers to the financial or reputational harm that would be incurred by the University if an adverse event occurred.

Control effectiveness is the ability of existing control measures implemented to measurably or estimably reduce risk.

Likelihood simply refers to the perceived likelihood of an adverse event occurring. For example, it may be ‘almost certain’ that a computer within a business unit would be infected with a virus at some time in a given year, that likelihood would be scored as a ‘5.’ However, it may only be ‘unlikely’ or ‘unlikely’ that a flood would damage the computer (a score of 2 or 1 respectively).


\begin{center}
\begin{tabular}{|c|c|}
\hline
\textbf{Score} & \textbf{Definition (Financial / Non-Financial)} \\
\hline
5 & Greater than $50 million \textbf{Or} Extreme reputational impact \\
4 & $25 million to $50 million \textbf{Or} High reputational impact \\
3 & $5 million to $25 million \textbf{Or} Medium to low reputational impact \\
2 & $100,000 to $5 million \textbf{Or} Low to no reputational impact \\
1 & Less than $100,000 \textbf{Or} No reputational impact \\
\hline
\end{tabular}
\end{center}

\begin{center}
\begin{tabular}{|c|c|}
\hline
\textbf{Score} & \textbf{Definition} \\
\hline
5 & Little or no effectiveness \\
4 & Effective some of the time \\
3 & Generally effective \\
2 & Effective most of the time \\
1 & Maximum effectiveness \\
\hline
\end{tabular}
\end{center}

\begin{center}
\begin{tabular}{|c|c|}
\hline
\textbf{Score} & \textbf{Definition} \\
\hline
5 & Almost certain; expected to occur \\
4 & Likely; probably will occur \\
3 & Possible; might occur at some time \\
2 & Unlikely; could occur at some time \\
1 & Rare; may occur \\
\hline
\end{tabular}
\end{center}

\textbf{Risk Score} = \text{Impact} \times \text{Control Effectiveness} \times \text{Likelihood}

A conversation about risk assessment involves reviewing the core business functions identified in Policy \textit{DCS 2.1 Identify Core Business Functions} and in \textit{DCS.G.2.1 Identify Core Business Functions Guideline}, and assigning risks that might threaten conducting those functions. As an example, in the University, conducting classes, research, or clinical operations are core business functions. Through your business area’s teams, apply and further break down those functions into your business unit. For example, an academic unit may not be able to conduct...
classes if the technology supporting it is unusable or the network is not operational. Similarly, it cannot conduct classes if the facility is unusable.

To illustrate the use of the risk scorecard, let’s examine the example above of the network being down. If the impact of the network being down is that classes are unable to be taught, we need to examine the problem. Are all classes in the Unit affected? Several? Or only one? Let’s assume that several classes are affected. Chances are that there is no discernible financial impact and if the classes were unable to be taught for a short period of time, there also wouldn’t be any impact on the Unit’s reputation so we assign the impact a score of one (1).

Next, for the control effectiveness, we assign a value of two (2) since we have plans to use backup slides and handouts to teach the class, and can post additional content following class. Those controls limit the risk of being unable to teach many of the classes or teach most of the class....

For the likelihood, we assign a value of two (2) since it is unlikely a network outage would occur during a given class, but possible.

Finally we can calculate the Risk Score as:

\[
\text{Risk Score} = 1 \text{ (Impact)} \times 2 \text{ (Control Effectiveness)} \times 2 \text{ (Likelihood)} = 4
\]

The list of these functions (as in DCS 2.1) and possible risks should be created and the team should assign relative risks based on discussion of impact (cost or reputational), what controls are in place, and likelihood of occurrence. The process is iterative.

Once calculated, these risk scores will provide the Unit with a roadmap identifying the areas of greatest risk that need attention before those of lower risk.

For those items that are supported by information systems/technology, IT should participate in the risk scoring exercise.

**DCS.G.2.4.2 Responsibility for Implementation**

The Unit head or delegate is responsible for the implementation of this Risk Assessment Guideline. The UISO is typically responsible for making sure that the IT system related Risk Assessments are performed annually.

**DCS.G.2.4.3 Definitions**

a. **Control effectiveness** - the ability of existing control measures implemented to reduce risk.
b. **Impact** - the financial or reputational harm that would be incurred by the University if an adverse event occurred.

c. **Likelihood** - the perceived likelihood of an adverse event occurring over a certain time range, typically one year.

**DCS.G.2.4.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Ed Zawacki</td>
<td>Initial document</td>
<td>Dec. 18, 2012</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.2.5 Implement Risk Management Program Guideline

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

DCS.G.2.5.0 Implement Risk Management Program Introduction

In general, the University of Illinois facilitates risk management awareness and processes through its Enterprise Risk Management Office and at UIC, through the IT Governance Council’s InfraSec Committee, and the Risk Management Advisory Group.


Each Unit needs to adapt this generic University of Illinois risk framework along with the University processes the Unit participates in to meet its local organizational structure. Effectively, risk management at its most basic level involves *continuous* identification of risks and subsequent response to those risks identified in the risk assessment. This is done through implementation of mitigation strategies to address those risks.
a. **Response**

The University defines the objective of Risk Response to provide support to the risk owner. However, it is the risk owner (dean, director, department head), that ultimately accepts risk. The University Risk Management Office offers four general categories for risk response; avoid, share, reduce, and accept risk. These categories are listed here relative to the level of risk, from “Very High Risk” to “Very Low Risk,” respectively. That is, it is recommended to avoid ‘Very High Risk’ when possible. That is not to say that units should not engage in activities which carry risk, as some risk is usually necessary to conduct business.

<table>
<thead>
<tr>
<th>Risk Score</th>
<th>Consequences</th>
<th>Immediate Actions</th>
<th>Response Choices** (Individual or Combinations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High Risk (101-125)</td>
<td>Extreme financial loss; extreme reputational impact</td>
<td>Requires essential and immediate allocation and organization of resources to manage/mitigate the risk; establish plans and countermeasures.</td>
<td>Avoid</td>
</tr>
<tr>
<td>High Risk (76-100)</td>
<td>High financial loss; high reputational impact</td>
<td>Requires priority allocation of resources for management and/or mitigation; establish plans and countermeasures.</td>
<td>Share</td>
</tr>
<tr>
<td>Moderate Risk (51-75)</td>
<td>Moderate financial loss; medium to low reputational impact</td>
<td>Allocation of resources for study is desirable; risk should be monitored for increases in impact or likelihood.</td>
<td>Reduce</td>
</tr>
<tr>
<td>Low Risk (26-50)</td>
<td>Low financial loss; low to no reputational impact</td>
<td>Generally does not require action, but should be reviewed periodically.</td>
<td>Accept</td>
</tr>
<tr>
<td>Very Low Risk (1-25)</td>
<td>Negligible financial loss; no reputational impact</td>
<td>No action required.</td>
<td></td>
</tr>
</tbody>
</table>

* Risk Score = Impact x Likelihood x Control Effectiveness
** No implication is made that a Very High Risk should be Avoided or a Very Low Risk should be Accepted

It is recommended that ‘shared risks’ which have common drivers be considered for shared risk mitigation strategies. For example, if multiple units under an organization have identified risks that are dependent on the network being available, it may make the most sense to aggregate those risks into a single response strategy in coping with network outages. As another example, if several units in proximity to each other require secure offsite storage of backup media, they may agree to a single common secure location for collection and temporary storage of the
media pending its pickup/return by an external vendor who provides secure offsite storage services.

Considerations on the appropriate response to risk involve the urgency of the risk response, budget, the Unit and University’s risk appetite, whether the risk can be mitigated directly or is external, impact to other units, lead time to implement a risk response, and relative priority, along with the likelihood for successful mitigate given a strategy.

b. IT/Data Security Take-Away

Although the risk model can be used broadly for any type of risk, it is important for the UISO as well as the Data Stewards and Data Custodian(s) to participate in this process and advocate for its performance in order to have appropriate awareness of the University core business processes, location of High Risk Data and IT/IS assets, potential risks the organization identifies, and to be allowed to weigh in on the relative controls in place or advocate for controls to be put in place to address risk.

DCS.G.2.5.2 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of this Implement Risk Management Program Guideline. The UISO is typically responsible for making sure that the duties of the Guideline are carried out, and that the Implement Risk Management Program Guideline is updated on an annual basis.

DCS.G.2.5.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Ed Zawacki</td>
<td>Initial document</td>
<td>Oct. 29, 2012</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.3.0 Access Authorization Guideline Introduction

The goal of access authority is to ensure that the individual requiring access to High Risk Data, Sensitive Data Collections, Sensitive Data, or Internal Data is:

a. Currently serving in a role requiring them to have access to such data

b. There is organizational awareness and agreement that the individual’s access is appropriate, and that the Unit has responsibility to provide the training and work knowledge for the individual to securely access, modify, and store the data without compromising its confidentiality, integrity, or availability.

c. To ensure that access to data sets is removed immediately or as soon as reasonably possibly upon change of role.

d. Providing a logged, auditable, and visible method to determine what individuals, roles, or groups had access to a data set or system granting access to a data set at a particular point in time.

DCS.G.3.1 Access Authorization Guideline Procedure

In general and where possible, we encourage business units to consider a role-based access control (RBAC) model. In this model, individual ‘user’ accounts are placed into groups that have a particular functional role, such as HR, finance, academic, et al, and potentially into subgroups or supergroups. Those groups align with the organization of data in data repositories or in simple computer systems, files or folders. For example, a College’s HR director and business managers may have access to a shared ‘HR’ folder based on their role, however, local department heads or business managers not handling
centralized hiring processes would not be granted access, as their role does not require access. The practice or restricting or limiting such access is called the principle of least privilege.

At UIC, several systems follow such a model, such as the University’s enterprise applications, as well as UIC’s implementation of Microsoft (MS) Active Directory (AD).

When possible, this Program encourages the use of AD, LDAP, and other directory services to facilitate organization of file shares and authentication. These services allow the use of an organizational structure (organized into units, or ‘OU’s) to group users and allow them to authenticate based on their access privileges and roles. In combination with appropriate logging of access to files, folders, or repositories, this provides the most robust and scalable method, and manageable method to properly manage user accounts, particularly those with files containing High Risk Data or Sensitive Data.

UIC is currently implementing a logging service which can provide an audit trail of access to files/records. Contact security@uic.edu to learn more about connecting your system to this share.

**DCS.G.3.2 Responsibility for Implementation**

The Unit head or delegate is responsible for the implementation of this *DCS.G.3 Access Authorization Guideline*. If the Unit adopts the *PER.G Personnel Guideline* then the Business Unit IT Systems Risk Assessment Committee is responsible for the implementation of this *DCS.G.3 Access Authorization Guideline*.

**DCS.G.3.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial composition</td>
<td>Oct. 29, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.S.4.0 Data Encryption Storage Standards Purpose

UIC Information Technology Security Policy DCS.4 Encryption of Stored Data, requires “High Risk Data and Sensitive Data Collections must be encrypted when stored on portable data storage devices”, including flash drives, laptops, handheld devices and removable media.” Additionally, High Risk Data and Sensitive Data Collections stored on non-portable devices must be encrypted when deemed necessary by its Data Custodian(s) as part of the risk assessment(s) conducted per Policy DCS.2.4 Conduct Risk Assessment. This Standard is intended to meet regulatory requirements for encryption of High Risk Data as data-at-rest including those of HIPAA, and/or for the encryption to be a compensating control for broader aspects of the same regulatory requirements.

DCS.S.4.1 Data Encryption Storage Standards - General Requirements

a. Required symmetric block cipher encryption algorithms and strengths have been specified in this DCS.4S after review and selection by the UIC Information Technology Security Committee from the “NIST Cryptographic Toolkit - Block Ciphers - Approved Algorithms”.

---

58 See “Portable data storage device” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”

59 See “High Risk Data” definition including at See “Portable data storage device” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”

Only Advanced Encryption Standard (AES) and Triple DES (3-DES) encryption algorithm ciphers are permitted. Furthermore, encryption strength under those ciphers must be:

1. Medium Strength\(^{61}\) 128-bit AES (AES-128), or Strong\(^{62}\) 192-bit AES (AES-192) or 256-bit (AES-256) key size symmetric block ciphers in CBC or GCM mode\(^{63}\), or

2. Alternatively, the Medium Strength 3-DES symmetric block cipher, also known as Triple Data Encryption Algorithm (TDEA) or Triple DEA, with keying option 1 (3x56 bit independent keys, 168 bit equivalent) or keying option 2 (2 independent 56 bit keys, 112 bit equivalent) is allowed\(^{64}\), but Strong 256 bit AES encryption is preferred over 3-DES keying options 1 and 2 since AES-256 tends to encrypt and decrypt significantly faster than 3-DES.

3. Low strength\(^{65}\) cipher Triple DES with keying option 3 (56 bit equivalent) is prohibited for encrypting stored data under this DCS.4S Standard.

b. This Standard follows the NIST Special Publication 800-57, “Recommendation for Key Management – Part 1: General (Revision 3)”\(^{3}\) suggestions in section 5.3.6, Cryptoperiod Recommendations for Specific Key Types, that the Originator Usage Period (applicable to the use of a unique Symmetric Data Encryption key in applying the original cryptographic protection to information [i.e., encrypting storage under DCS.4S.1.2]) should be less than or equal to 2 years. The section states “(d)uring the Originator Usage Period, information may be encrypted by the data-encryption key; the key shall not be used for performing an encryption operation on information beyond this period. However, the key may need to be available to decrypt the protected data beyond the Originator Usage Period (i.e., the recipient-usage period may need to extend beyond the Originator Usage Period)”.

c. The same NIST SP 800-57 section 5.3.6 defines the Recipient Usage Period to permit all information that has been protected by the originator to be processed by the recipient before the processing key is deactivated. It advises the recipient-usage period should not exceed the Originator Usage Period plus three years. Thus, a unique

---

\(^{61}\) See “Medium Strength” cipher in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”

\(^{62}\) See “Strong” cipher in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”


\(^{65}\) See “Low Strength” cipher in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
Symmetric Data Encryption key under this Standard shall not be used for a period exceeding 5 years from the date the information has been encrypted.

**DCS.S.4.3 Resources**

A Unit may use cryptographic algorithms for applications outside of the ones in the scope of this Standard. Cisco Systems, Inc. advises that “over the years, numerous cryptographic algorithms have been developed and used in many different protocols and functions. Cryptography is by no means static. Steady advances in computing and in the science of cryptanalysis have made it necessary to adopt newer, stronger algorithms and larger key sizes. Some older algorithms and key sizes no longer provide adequate protection from modern threats and should be replaced.”

If the Unit is utilizing an algorithm with a **Recommendation Status of Avoid** in the table below, the algorithm **must** be replaced with the one designated in the **Alternative** field.

### Recommendations for Cryptographic Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Operation supported by algorithm</th>
<th>Recommendation Status</th>
<th>Alternative</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>Encryption</td>
<td>Avoid</td>
<td>AES</td>
<td></td>
</tr>
<tr>
<td>3DES</td>
<td>Encryption</td>
<td>Legacy</td>
<td>AES</td>
<td>Short key lifetime</td>
</tr>
<tr>
<td>RC4</td>
<td>Encryption</td>
<td>Avoid</td>
<td>AES</td>
<td></td>
</tr>
<tr>
<td>AES-CBC mode</td>
<td>Encryption</td>
<td>Acceptable</td>
<td>AES-GCM</td>
<td></td>
</tr>
<tr>
<td>AES-GCM mode</td>
<td>Authenticated encryption</td>
<td>NGE¹</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DH-768, -1024</td>
<td>Key exchange</td>
<td>Avoid</td>
<td>DH-2048 (Group 14)</td>
<td></td>
</tr>
<tr>
<td>RSA-768, -1024</td>
<td>Encryption</td>
<td></td>
<td>RSA-2048</td>
<td></td>
</tr>
<tr>
<td>DSA-768, -1024</td>
<td>Authentication</td>
<td></td>
<td>DSA-2048</td>
<td></td>
</tr>
<tr>
<td>DH-2048</td>
<td>Key exchange</td>
<td>Acceptable</td>
<td>ECDH-256</td>
<td></td>
</tr>
<tr>
<td>RSA-2048</td>
<td>Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSA-2048</td>
<td>Authentication</td>
<td></td>
<td>ECDSA-256</td>
<td></td>
</tr>
<tr>
<td>MD5</td>
<td>Integrity</td>
<td>Avoid</td>
<td>SHA-256</td>
<td></td>
</tr>
<tr>
<td>SHA-1</td>
<td>Integrity</td>
<td>Legacy</td>
<td>SHA-256</td>
<td></td>
</tr>
<tr>
<td>SHA-256</td>
<td>Integrity</td>
<td>NGE</td>
<td>SHA-384</td>
<td></td>
</tr>
<tr>
<td>SHA-384</td>
<td>Integrity</td>
<td>NGE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-512</td>
<td>Integrity</td>
<td>NGE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMAC-MD5</td>
<td>Integrity</td>
<td>Legacy</td>
<td>HMAC-SHA-1</td>
<td>Short key lifetime</td>
</tr>
<tr>
<td>HMAC-SHA-1</td>
<td>Integrity</td>
<td>Acceptable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDH-256</td>
<td>Key exchange</td>
<td>Authentication</td>
<td>ECDH-384</td>
<td></td>
</tr>
<tr>
<td>ECDSA-256</td>
<td>Authentication</td>
<td></td>
<td>ECDSA-384</td>
<td></td>
</tr>
<tr>
<td>ECDH-384</td>
<td>Key exchange</td>
<td>Authentication</td>
<td>NGE</td>
<td></td>
</tr>
<tr>
<td>ECDSA-384</td>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹. NGE = next generation encryption

[66](http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html)
## DCS.S.4.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9</td>
<td>Richard Chua</td>
<td></td>
<td>November 4, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.P.4.0 Data Encryption Storage Procedure Purpose

UIC Information Technology Security Policy DCS.4 Encryption of Stored Data, requires “High Risk Data and Sensitive Data Collections must be encrypted when stored on portable data storage devices,” including flash drives, laptops, handheld devices and removable media.” Additionally, High Risk Data and Sensitive Data Collections stored on non-portable devices must be encrypted when deemed necessary by its Data Custodian(s) as part of the risk assessment(s) conducted per Policy DCS.2.4 Conduct Risk Assessment. The DCS.4 Policy, Procedure and Standard for Encryption of Stored Data are intended to meet regulatory requirements including those of HIPAA for encryption of High Risk Data as data-at-rest, and/or for the encryption to be a compensating control for broader aspects of the same regulatory requirements.

DCS.P.4.1.1 Data Encryption Storage Procedure - General Requirements

High Risk Data or Sensitive Data Collections, as data-at-rest on portable data storage devices or deemed needing encryption by the Data Custodian, must be encrypted by one of the following storage encryption technologies depending upon the type of device the data is stored upon: whole/full disk encryption (DCS.P.4.1.2.a), portable device encryption (DCS.P.4.1.2.b), external device encryption (DCS.P.4.1.2.c), file / folder encryption (DCS.P.4.1.2.d), or virtual disk encryption (DCS.P.4.1.2.e). Implementers are encouraged to utilize and leverage implementations supported by the ACCC, but may also implement methods that meet the encryption requirements given in this section DCS.P.4.1.1.

---

67 See “Portable data storage device” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”.

Specifically:

a. The Unit **must** document its encryption procedures including those for cryptographic key generation, use, storage, recovery and destruction\(^\text{69}\). Compromise recovery planning procedures are set forth in the earlier cited NIST Special Publication 800-57, section 5.5, *Compromise of Keys and other Keying Material*.

b. Special attention needs to be paid to the method of storage of the encryption keys, as it may be feasible for a malicious party to circumvent the high security of the encryption storage by compromising ineffective encryption key storage security through:

   1. computationally brute forcing an insecurely encrypted file containing encryption keys on an unencrypted device (e.g. a 7-Zip file encrypted as a zip filetype archive format with the default ZipCrypto encryption algorithm which is subject to plaintext attacks rather than the more secure AES128, AES192, or AES256 algorithms), or
   2. computationally brute forcing a file consisting of hashes of encryption keys (e.g. in an unencrypted file), or
   3. otherwise compromising an insecure key storage mechanism, or an insecure disposal mechanism for the physical or logical records of the encryption keys.

c. Policy **PER.4b, Access Establishment and Modification**, details the conditions under which an individual’s access privileges **must** be updated, and both Policy **PER.6 Termination of Access** and **DCS.G.3.0 Access Authorization Guideline**, detail consequent removal of data access privileges. To facilitate those processes on systems under this Standard, the Unit’s encryption procedures **must** include provisioning of an administrative account, with documentation including the account credentials to allow authorized IT administrators to gain access to devices that are no longer assigned to individuals.

   The initial encryption, and any subsequent decryption, of any storage device utilized under this Standard **must** be documented.

d. Any unauthorized attempt to disable, remove, or otherwise tamper with encryption implemented under this **DCS.P.4** is **prohibited** and is a violation of Policy **DCS.4 Encryption of Stored Data**.

e. Any encrypted system known to contain High Risk Data, Sensitive Data Collections, or other data deemed necessitating encryption under **DCS.P.4.0**, **must** undergo a secure data-wipe process prior to release or reassignment as specified by **DCS.G.8 Develop and Implement Media Reuse Procedures**.

f. Required symmetric block cipher encryption algorithms and strengths have been specified in DCS.S.4.1.a after review and selection by the UIC Information Technology Security Committee from the “NIST Cryptographic Toolkit - Block Ciphers - Approved Algorithms”\(^\text{70}\).

Only Advanced Encryption Standard (AES) and Triple DES (3-DES) encryption algorithm ciphers are permitted. Furthermore, encryption strength under those ciphers must be:

1. Medium Strength\(^\text{71}\) 128-bit AES (AES-128), or Strong\(^\text{72}\) 192-bit AES (AES-192), or 256-bit (AES-256) key size symmetric block ciphers in CBC or GCM mode\(^\text{73}\), or

2. Alternatively, Medium Strength 3-DES symmetric block cipher, also known as Triple Data Encryption Algorithm (TDEA) or Triple DEA, with keying option 1 (3\times56 bit independent keys, 168 bit equivalent) or keying option 2 (2 independent 56 bit keys, 112 bit equivalent) is allowed\(^\text{74}\), but 256 bit AES encryption is preferred over 3-DES keying options 1 and 2 since AES-256 tends to encrypt and decrypt significantly faster than 3-DES.

3. Triple DES with keying option 3 (56 bit equivalent) is prohibited for encrypting stored data under the DCS.4S Standard.

g. Standard DCS.S.4.1.b Data Encryption Storage Standards - General Requirements advises that the Originator Usage Period (applicable to the use of a unique Symmetric Data Encryption key in applying the original cryptographic protection to information [i.e., encrypting storage under DCS.P.4.1.2]) should be less than or equal to 2 years. The key may need to be available to decrypt the protected data beyond the Originator Usage Period (i.e., the recipient-usage period may need to extend beyond the Originator Usage Period).


\(^\text{71}\) See “Medium Strength” cipher in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”

\(^\text{72}\) See “Strong” cipher in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”


h. Standard DCS.S.4.1.c defines the Recipient Usage Period to permit all information that has been protected by the originator to be processed by the recipient before the processing key is deactivated. The recipient-usage period should not exceed the Originator Usage Period plus three years. Thus, a unique Symmetric Data Encryption key under Standard DCS.4.S.1.c shall not be used for a period exceeding 5 years from the date the information has been encrypted.

i. In accordance with the above DCS.P.4.1.1h, when data storage is encrypted under this Standard and the data is expected to have modification life span exceeding the Originator Usage Period, the Data Custodian must develop a plan to replace the encryption key so the Originator Usage Period is not exceeded, and execute that plan with the approval of the Data Steward.

j. Similarly to DCS.P.4.1.1j, the Data Custodian must develop a plan to replace the encryption key so the Recipient Usage Period is not exceeded, and execute that plan with the approval of the Data Steward.

**DCS.P.4.1.2 Data Encryption Storage Standards - Specific Storage Encryption Technology Requirements**

DCS.P.4.1.2 hereunder applies to the Policy DCS.4 Encryption of Stored Data required encryption of High Risk Data and Sensitive Data Collections. Rather than repeating those data classes in each of the DCS.P.4.1.2a through DCS.P.4.1.2e sections below, it is presumed that the following requirements are being applied because the devices contain or are intended to contain High Risk Data and/or Sensitive Data Collections.

**DCS.P.4.1.2.a Whole/Full Disk Encryption**

Whole/Full Disk Encryption is the process of encrypting all the data on a physical hard drive, or aggregation of physical hard drives through RAID technology. The implementation of whole disk encryption ensures that any and all data contained within the physical or virtual (RAID) device is encrypted. Whole/Full Disk Encryption implementation must require the manual or automatic input of an encryption key prior to the device OS boot sequence.

Recommended application(s): Microsoft Bitlocker Drive Encryption (available through Microsoft Vista Enterprise or later), PGP Desktop, or FileVault 2 (available through OSX 10.7 Lion or later; the predecessor FileVault only encrypted the user home folder, and was vulnerable to decryption attacks).

1. If Microsoft BitLocker is used, note that it defaults to 128 bit AES encryption with the Elephant Diffuser algorithm enhancement. Its encryption level can optionally be elevated to AES-256, methods include:

i. Windows 7 and Windows Server 2008 R2:
A. Group Policy Editor: Computer Configuration --> Administrative Templates --> Windows Components --> BitLocker Drive Encryption

B. Choose drive encryption method and cipher strength (Windows 7 and Windows Server 2008 R2), or

C. Configure encryption method (Windows Vista and Windows Server 2008)
   Select AES 256-bit

D. Alternatively, you may familiarize yourself with the Elephant Diffuser\(^{75}\), and select AES 256-bit with Diffuser.

ii. Windows 8 and 8.1:

A. Press the Windows + R keys to open the Run dialog, type `gpedit.msc`, and press Enter.

B. If prompted by UAC, then click on Yes

C. In the left hand pane of Group Policy, successively click on to expand `Computer Configuration, Administrative Templates, Windows Components`, and then open `BitLocker Drive Encryption`.

D. In the right hand pane of the `BitLocker Drive Encryption` folder, double click on `Choose drive encryption method and cipher strength` to edit it.

E. Follow either step F. or G. below according to the encryption level you intend:

F. To use the Default AES 128-bit Method and Cipher, in the Choose Drive encryption method and cipher strength window, select either `Not Configured` or `Disabled`, and go to step H. below.

   **NOTE:** Disabled or Not Configured is the Microsoft gedit “reverse logic” method of enabling / not changing the default setting.

G. To choose a different Drive Encryption Method and Cipher Strength, Select `Enabled`, then under the Options section below the `Not Configured/Disabled/Enabled` selections, select the AES 256-bit encryption method (you can also select AES 128-bit (default) here if you want to prove to yourself you are really and truly selecting it as enabled). Go to step H. below.

H. Click on OK. You can now close Group Policy.


DCS.P.4.1.2.a Whole/Full Disk Encryption, cont.

2. FileVault 2

FileVault 2 utilizes the 128 bit symmetric XTS-AES encryption cipher. The algorithm was approved by NIST under its Special Publication 800-38E, “Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices” five years after Apple Inc. began its deployment under FileVault with OSX 10.3 Panther. FileVault could only encrypt files or folders, and did not provide for Whole/Full Disk Encryption.

FileVault 2 only protects the system drive, and cannot be used on additional partitions on the system drive, and cannot be used on RAID volumes. If the Macintosh computer has multiple internal or external hard drives after the system drive, the data on those drives cannot encrypted by FileVault.

i. If you are initially setting up the MacOS 10.7 or higher release system, or reformating the system volume, you should take the opportunity to segregate the system file partition from the partition containing the user(s) home folder(s). The first and system file partition should contain the MacOS installation, all of the software planned to be installed on the computer, and the admin user account. The second partition should have the user account(s) home folder(s). As you create a new user account, you can use the Advanced feature in the Accounts preference to set the home folder for a user.

ii. Before enabling FileVault 2, make a full backup of the data on the system drive.

iii. Log in to OS X with an account that has administrative privileges and go to System Preferences > Security & Privacy > FileVault. Click the padlock in the lower left of the

iv. FileVault 2 utilizes the existing admin account password to decrypt the drive at boot so there is no need to set and remember a separate password to decrypt your drive at each boot. To allow for recovery in the event that the admin account password is lost, a separate FileVault 2 recovery key is generated and displayed on the screen as part of the process of enabling FileVault 2 as a backup access method. It allows an alternate method to unlock the system drive. The recovery key window will be displayed only once in this process, it states “The recovery key is a safety net...”. Copy the recovery key string and store it according to the Unit’s cryptographic key generation, use, storage procedure under DCS.P.4.1.1.a, Data Encryption Storage Standards - General Requirements.

v. The FileVault 2 enablement process also offers the option to store the recovery key in escrow with Apple Inc. If this is allowed under the Unit’s cryptographic key generation, use, storage procedure at DCS.P.4.1.1.a, then at the prompt, select from the choices available for each of the three security questions and enter their corresponding answers. Record the questions, and the answers. That information serves as the credentials needed if the recovery key must be obtained from Apple Inc.

vi. Optional note: The FileVault 2 recovery key can be used to gain access to a system if the password is not available for a FileVault-authorized account on the system.

A. In the initial gray boot screen, select an account and then click the question-mark (?) icon in the password field. A message is displayed, “If you forgot your password, you can reset it using your recovery key.” Click on the right-pointing triangle, and enter the recovery key.

B. If you do not have credentials to log into the system and need to obtain the recovery key information stored in escrow at Apple Inc., proceed as in step v. to the ? prompt. At the bottom of the screen you should note two pieces of information, the serial number of the computer, and a “Record Number” used to track the recovery request at AppleCare. Call AppleCare in your country, and be prepared to provide those two pieces of information and also the answers to the three security questions defined when FileVault 2 was configured on the system. The answers to the three questions are used to authenticate you access to the FileVault recovery key, Apple Inc. does not utilize any Apple ID or iCloud account to permit or validate access to an escrowed FileVault 2 recovery key.

vii. Next, the Macintosh will reboot and prompt for the user account password at the EFI boot screen.

viii. After booting, FileVault will proceed to encrypt the system drive. You can follow the progress of this process at System Preferences > Security & Privacy > FileVault. It should state FileVault is enabled, and show a progress bar for the encryption process, and an estimated time to completion. This process will take between tens of minutes
and a number of hours depending on the size of your system drive and the speed of your Macintosh computer. Five hours for every 250GB of storage is typical. You can continue to use your Macintosh during this process, and reboot it if needed. You should confirm the drive encryption process is complete at the System Preferences.

ix. If you want to grant additional (existing or newly created) users the ability to unlock the drive utilizing their own account rather than the account you used to enable FileVault, “open the Security & Privacy pane of System Preferences. Select the FileVault tab and click the lock icon in the lower left corner of the window. Enter your admin privileges when prompted. Click the “Enable Users...” button to add existing users to the list of accounts that can unlock the disk”.

x. In addition to selecting FileVault 2 encryption, the protection of the system drive backups must be considered. While the system drive may be encrypted, the backups may not be encrypted by default. If you are using Apple’s Time Machine, you can configure backup encryption by going to System Preferences > Time Machine > Select Disk and selecting the box Encrypt Backups. Once you select the backup destination disk, if it is not already encrypted, Time Machine will allow you to encrypt it. The disk encryption password must match the FileVault 2 encryption password.

A. Under Lion 10.7.x, you can encrypt backups made to an internal or directly connected (not network accessed) external hard drive, the backup destination drive must have a GUID partition table, and the backup destination partition must be encrypted (MacOS Extended Case Sensitive, Journalled, Encrypted). If the disk does not have the GUID partition table, you must completely erase and reformat it under MacOS with the necessary encryption setting. The backup destination partition will be encrypted with the AES 128 bit cipher.

B. Effective with Mountain Lion 10.8.x, you can also encrypt backups to network storage, such as on a Time Capsule or a shared drive on another Macintosh computer. If you’re using a third party backup solution, you will need to verify if the software or cloud based backup service offers an option for encrypted backups.

DCS.P.4.1.2.b Portable Media Encryption:

Portable media must be encrypted using file/folder encryption (DCS.P.4.1.d) or virtual disk/volume encryption (DCS.P.4.1.a).

---

82 “With File Vault ON are time machine backups encrypted?”
http://apple.stackexchange.com/questions/46833/with-file-vault-on-are-time-machine-backups-encrypted
83 Further details at “OS X Mountain Lion: Choose a backup disk and set encryption options”
http://support.apple.com/kb/PH11102
84 See “portable media” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
DCS.P.4.1.2.c External Device Encryption:

External devices that do not have built in hardware encryption must be secured by the implementation of file/folder encryption or virtual disk/drive encryption.

Recommended software application(s): PGP Desktop (via PGP Disk), Bitlocker-to-Go.

1. BitLocker To Go (Windows 7)

   For a removable drive to be BitLocker-protected, it must be formatted by using the exFAT, FAT16, FAT32, or NTFS file system. The drive, volume, or partition must be at least 64 MB in size.

   If the drive is NTFS formatted, it can only be unlocked on a computer running Windows Server 2008 R2, Windows 7, Windows Server 2012, or Windows 8. Prior versions of the Windows operating system will not recognize the drive and will prompt you to format the drive.

   i. To encrypt a USB drive under BitLocker To Go, insert the USB drive, right-click on it in Windows Explorer, and select the Turn on BitLocker command. A message will be displayed, “Please wait while BitLocker initializes the device”.

   ii. After the initialization completes, BitLocker Drive Encryption will prompt you to enter a password to subsequently unlock the USB drive.

   iii. Next, you will be prompted to either store the recovery key to a file, or to print it out.

   iv. The password assigned and recovery key generated, you will be prompted to begin the encryption process. As it proceeds, a standard progress monitor will report the percentage of the process completed, but not provide a time estimate. There is a Pause button that will allow you to temporarily halt the process should you need to perform another task.

   v. BitLocker To Go reports when the encryption is complete, and changes the icon under Windows Explorer associated with the encrypted drive to a drive with a padlock.

   vi. When you later insert the BitLocker To Go encrypted drive into a Windows 7 system, you will immediately be prompted to enter the password. After you type the password, you can select the Automatically Unlock on This Computer from Now On check box to store the password in the Windows 7 password cache.

2. BitLocker To Go (Windows 8)

   i. The AES encryption level should be set by the process described at DCS.P.4.1.2.a.ii

   ii. Connect the USB drive to the system, then either:

       A. Open the Control Panel (icons view), and click on the BitLocker Drive Encryption icon. Under the Removable data drives - BitLocker To Go section, click on the arrow
to expand the drive letter you want to encrypt, then click on the Turn on BitLocker link, or

B. In File Explorer, open Computer, select the drive letter of the unencrypted removable data you want to encrypt, right click and hold it, then click on Turn on BitLocker, or

C. In File Explorer, open Computer, select the drive letter of the unencrypted removable data you want to encrypt, click on the Manage (Drive Tools) tab, click on the BitLocker icon in the ribbon, click on Turn on BitLocker

iii. At the prompt, “Choose how you want to unlock this drive”, enter the password which will be used to unlock the drive. Next, select how you want to back up your BitLocker recovery key: either stored in a file, or printed out.

A. The Save to your Microsoft account option is additionally available on non-domain-joined PCs. It permits you to you save the BitLocker recovery key to your Microsoft account. All your saved recovery keys can then be recovered at

http://windows.microsoft.com/recoverykey

iv. With the recovery key stored, select encrypt entire drive, and click on Next.

3. BitLocker To Go Reader (bitlockertogo.exe) allows Windows XP or Windows Vista systems to open and view the content of removable drives that have been encrypted with BitLocker To Go. When a drive is encrypted with BitLocker To Go, the BitLocker To Go Reader installer is automatically placed upon it.

i. When you insert the BitLocker To Go encrypted drive in a Windows XP or Vista system, you will see an AutoPlay dialog box that prompts you to install the BitLocker To Go Reader.

ii. After the Reader installs, the BitLocker To Go Reader will prompt you to enter the password assigned to the BitLocker encrypted drive. The Automatically Unlock on This Computer from Now On check box is not available with the BitLocker To Go Reader.

iii. Upon successfully providing the USB drive password, a BitLocker To Go Reader window opens. Although it looks like a Windows Explorer window, it doesn’t work like Windows Explorer. The BitLocker To Go Reader window displays the encrypted drive contents, but if you attempt to open any file by double-clicking on it, you’ll immediately be prompted to copy the file to the desktop - you won’t be able to open the file on the USB drive. You cannot simply copy files from the BitLocker To Go Reader window.

Recommended hardware encrypted device(s): LOK-IT Secure Flash Drive, Aegis Apricorn Padlock, Corsair Padlock 2.

DCS.P.4.1.2.d File / Folder (Directory) Encryption:

Files or folders (directories) must be encrypted when their containing physical hard drive or external device is not encrypted. Multiple file systems, referenced as partitions, may exist on a single physical hard drive, or on virtual hard drives presented through RAID technology. Such complete file systems, also known as individual hard drive partitions, or RAID partitions, must be encrypted, providing encryption to any files or folders (directories) contained thereunder.

Recommended application(s): PGP Desktop (via PGP Zip), FileVault 1 (only available with Mac OSX 10.3 Panther to 10.6 Snow Leopard. More recent releases of OSX only utilize the Full/Whole Disk Encryption for Filevault 2)

Alternative(s): 7-Zip, WinZip, Microsoft EFS.

DCS.P.4.1.2.e Virtual Disk/Volume Encryption:

The term “virtual disk/volume” is defined in the previously cited NIST Special Publication 800-111. It refers to the “process of encrypting a file called a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided, at which point the container is typically mounted as a virtual disk”. A virtual disk/volume is a type of logical disk partition (file system). In lieu of hardware encrypted devices, encrypted virtual disk(s)/volume(s) can be created within storage devices which lack hardware encryption capabilities. If encryption is not provided for High Risk Data or Sensitive Data Collections at the file or folder (directory) level, it can be provisioned at the higher and inclusive virtual disk/volume level.

Recommended application(s): PGP Desktop (via PGP Disk)

DCS.P.4.2 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of this DCS.4P Data Encryption Storage Procedure.

Data Custodians and Data Stewards, with review by the UISO, are responsible for ensuring that any and all data encryption requirements of this Standard are met including establishment and documentation of encryption procedures followed, and that encrypted data storage is monitored and maintained.

86 See Data Custodian and Data Steward definitions in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
### DCS.P.4.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9</td>
<td>Richard Chua</td>
<td>Initial composition</td>
<td>November 4, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.S.7.2 High Risk Data or Sensitive Data Collections Transmission Security Standard

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

DCS.S.7.2.0 High Risk Data or Sensitive Data Collections Transmission Security Standard Purpose

The following individual standards list minimum specifications that must be maintained to be in compliance with the DCS.7 High Risk Data or Sensitive Data Collections Transmission Security Policy and which must be maintained under its DCS.G.7 Guideline.

DCS.S.7.2.1 High Risk Data or Sensitive Data Collections Transmission Security Standards

The individual Standard numbers map to the corresponding Guideline requirement, for example, DCS.S.7.2.1.c.1 maps to DCS.G.7.2.1.c and its first requirement for a Standard. Similarly, DCS.S.7.2.1.3.d maps to DCS.G.7.2.1.3 and its fourth requirement for a standard.

DCS.S.7.2.1.c.1 128 bit or higher encryption required for SSL or TLS "SSL" High Risk Data or Sensitive Data Collections data transmissions

Many current implementations of the TLS (Transport Layer Security) protocol are informally referred to as utilizing the predecessor protocol to TLS, the SSL (Secure Sockets Layer) protocol. In a similar manner, the data transmissions under this TLS protocol are often informally referred to as "SSL transmissions" even though the actual protocol being used on the transmission is the TLS protocol.

Digital signatures of High Risk Data or Sensitive Data Collections Data SSL or TLS "SSL" transmissions must be signed by the DH or RSA protocol at a minimum 128 bit AES, IDEA or RC4 encryption level or
168 bit (effectively 112 bit) 3DES encryption ("Medium strength")\textsuperscript{87} and with SHA1, SHA2 or MDS message authentication. Lower encryption levels ("Low strength")\textsuperscript{88} including SSL or TLS "SSL" transmissions with null cipher encoding encryption or null authentication are prohibited. Default \textbf{Low Strength ciphers must explicitly be removed} from the permitted negotiated cipher suites for an application providing remote access to High Risk Data or Sensitive Data Collections data including the Apache http Server and Apache Tomcat Server, and also Microsoft Internet Information Services (IIS) and SharePoint Server, otherwise a client application requesting use of the low strength ciphers will be permitted by the application Server to utilize them.

Strong Encryption\textsuperscript{89} ciphers such as AES (192, and 256-bit key lengths), Blowfish (128 to 448-bit key lengths, in 8-bit increments), and ARCCFOUR (2048-bit) provide an additional level of security over Medium Strength ciphers.

\textsuperscript{87} See “Medium strength” in \textit{UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions}

\textsuperscript{88} See “Low strength” in \textit{UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions}

\textsuperscript{89} See “Strong encryption” in \textit{UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions}
**DCS.S.7.2.1.c.2 Prohibited High Risk Data or Sensitive Data Collections SSL or TLS/ "SSL" Transmission Protocols**

<table>
<thead>
<tr>
<th>Encryption type and strength</th>
<th>Key Exchange</th>
<th>Authentication</th>
<th>Cipher Encoding Encryption</th>
<th>Message Authentication Code / Message Digest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>RSA</td>
<td>RSA</td>
<td>None</td>
<td>SHA1</td>
</tr>
<tr>
<td>Null</td>
<td>RSA</td>
<td>RSA</td>
<td>None</td>
<td>MD5</td>
</tr>
<tr>
<td>Low &quot;40 bit&quot; export grade</td>
<td>512 bit RSA</td>
<td>RSA</td>
<td>40 bit RC2 or 40 bit RC4</td>
<td>MDS</td>
</tr>
<tr>
<td>Low &quot;40 bit&quot;</td>
<td>512 bit DH</td>
<td>RSA or DSS</td>
<td>40 bit DES</td>
<td>SHA1 export</td>
</tr>
<tr>
<td>Low &quot;40 bit&quot;</td>
<td>512 bit RSA</td>
<td>RSA</td>
<td>40 bit DES</td>
<td>SHA1</td>
</tr>
<tr>
<td>Low &quot;40 bit&quot;</td>
<td>512 bit RSA</td>
<td>RSA</td>
<td>40 bit</td>
<td>MD5</td>
</tr>
<tr>
<td>Low &quot;56 bit&quot;</td>
<td>RSA</td>
<td>RSA</td>
<td>56 bit DES</td>
<td>MD5</td>
</tr>
<tr>
<td>Low &quot;56 bit&quot;</td>
<td>DH</td>
<td>RSA or DSS</td>
<td>56 bit DES</td>
<td>SHA1</td>
</tr>
<tr>
<td>Low &quot;56 bit&quot;</td>
<td>RSA</td>
<td>RSA</td>
<td>56 bit DES</td>
<td>SHA1</td>
</tr>
<tr>
<td>Low &quot;64 bit&quot;</td>
<td>RSA</td>
<td>RSA</td>
<td>64 bit RC4</td>
<td>MD5</td>
</tr>
</tbody>
</table>

**DCS.S.7.2.1.c.3 TLS 1.2 Preferred for High Risk Data or Sensitive Data Collections data transmissions**

Due to known vulnerabilities in the SSL 1.0, 2.0 and 3.0 protocols, their use in High Risk Data or Sensitive Data Collections Data transmissions is strongly discouraged. Where possible, depending upon the capabilities of the client and Server respectively in the TLS communication, “The Transport Layer Security (TLS) Protocol Version 1.2” [http://tools.ietf.org/html/rfc5246](http://tools.ietf.org/html/rfc5246) should be used in preference to TLS 1.0 or 1.1.

As noted in the above Standard DCS.S.7.2.1.c.2, “Prohibited High Risk Data or Sensitive Data Collections SSL or TLS/ "SSL" Transmission Protocols”, the insecure 40 or 56 bit DES, RC2 and RC4 cipher suites are prohibited in any SSL or TLS transmission.
DCS.S.7.2.1.c.4 128 bit or higher encryption required for SSH "SSL" High Risk Data or Sensitive Data Collections data transmissions

Following the specifications of "The Secure Shell (SSH) Transport Layer Protocol" http://tools.ietf.org/html/rfc4253 ciphers for use in SSH or SFTP High Risk Data or Sensitive Data Collections data transmissions must use keys with an effective key length of 128 bits or more (Medium strength), and Message Authentication Code / Message Digest digital signature must be enabled. Null encryption and/or null digital signature are prohibited for these transmissions. Other applications utilizing the SSH protocol for secure file transfer services such as SCP or PuTTY must meet this same specification.

DCS.S.7.2.1.c.5 SSH version 2.0 required for SSH "SSL" High Risk Data or Sensitive Data Collections data transmissions

Due to known vulnerabilities in the SSH 1.0 protocol its use in High Risk or Sensitive Data Collections Data transmissions is prohibited.

More information on SSH client applications which support this DCS.S.7.2.1.c.5 Standard is available at http://www.uic.edu/depts/accc/software/ssh/index.html

DCS.S.7.2.1.3.a 128 bit RC4 encryption required for Microsoft Remote Desktop Protocol High Risk Data or Sensitive Data Collections data transmissions

The Microsoft Remote Desktop Protocol, utilized by the Microsoft Remote Desktop application and Terminal Services, is capable of being used with Low Strength 56 or Medium Strength 128 bit RC4 cipher stream cipher keys. Only 128 bit RC4 encryption Microsoft Remote Desktop Protocol is allowed for High Risk Data or Sensitive Data Collections data transmissions.

The RD RemoteApp Manager should be used to configure Windows Server 2008, or the Remote Desktop Management Server (RDMS) interface to configure Windows Server 2012, to utilize digital signatures issued with a digital certificate which must be provided by a certificate authority.

The UIC Information Technology Security Program Committee recognizes that some devices only permit the use of self-signed certificates. In such cases, compensating, mitigating controls such as network, operating system, or application access controls must be implemented. If self-signed certificates are used, the RDP client must not be configured to never warn about the self-signed certificate for a host again because if it is, that insecure configuration will effectively enable Man-in-the-Middle attacks.

Transmission security should be set to TLS 1.0, not the native RDP encryption, in the Microsoft Remote Desktop application and Terminal Services.
DCS.S.7.2.1.3.b Prohibited Remote Desktop access applications for High Risk Data or Sensitive Data Collections data transmissions

Only properly configured Microsoft Remote Desktop, or SSH Server with or without X Server, applications along with the ACCC provided OpenVPN are the permitted methods of remote desktop access. Installation and usage of any other remote access application such as GoToMyPC or LogMeIn are prohibited on University systems because they do not require adherence to or allow administrative verification of the requirements of Policy PER.3 Ensure Unique Identifiers Have Been Assigned, section PER.3b referencing the ACCC Common Password Strong Password Policy.

DCS.S.7.2.1.3.c Microsoft PPTP VPN Prohibited for High Risk Data or Sensitive Data Collections data transmissions

The Microsoft PPTP VPN is prohibited for use in High Risk Data or Sensitive Data Collections data transmissions.

The OSI Layer 2 (datalink) RFC2637 Point-to-Point Tunneling Protocol (PPTP) allows RFC 1661 Point to Point Protocol (PPP) traffic to be tunneled through a call-control and management tunnel it establishes, and then in conjunction with a simultaneous second RFC 2784 “Generic Routing Encapsulation (GRE)” tunnel it encapsulates and transports many types of protocols including AppleTalk, IP and Netbeui. The underlying PPP protocol in a PPTP VPN permits transport across many types of differing Layer 2 physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET encompassing differing sets of protocol characteristics including physical addressing, network topology, error notification, frame sequencing, and flow control.

As described in “VPN Tunneling Protocols” Microsoft PPTP uses the PPP encryption and PPP compression schemes. The CCP (Compression Control Protocol) used by PPP is used to negotiate encryption. “Understanding PPTP (Windows NT 4.0)” further explains PPTP defaults to a RSA RC4 40 bit cipher using encryption keys generated from the Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) or Extensible Authentication Protocol-Transport Level Security (EAP-TLS) authentication process. Those keys are readily crackable. PPTP can be configured to utilize a symmetric 56 or 128 bit stream cipher, but those ciphers are crackable as well.

The commercial CloudCracker.com service will provide a “restored” decrypted MS-CHAP v2 PPTP key from a short segment of captured Microsoft PPTP VPN traffic in under a day. Microsoft has issued PEAP as a patch to replace MS-CHAP, but notes in that patch notice direct that L2TP/IPsec or SSTP should be used instead of PPTP. Low Strength 40 and 56-bit RC4 support was removed starting with Windows Vista and Windows Server 2008, but can be added (not recommended) by changing a registry key. EDAP-TLS authentication requires server-side “computer certificates” and client side “user certificates”, but these are only used to establish user, not machine, authentication.

Furthermore, although PPTP encrypts data, it does not have the capability to verify the integrity of data.
DCS.S.7.2.1.3.d 128 bit or higher encryption required for Microsoft L2TP/IPsec VPN High Risk Data or Sensitive Data Collections data transmissions

RFC2661 Layer Two Tunneling Protocol (L2TP) [http://www.rfc-editor.org/pdfrfc/rfc2661.txt.pdf](http://www.rfc-editor.org/pdfrfc/rfc2661.txt.pdf) in itself does not provide any encryption or confidentiality to traffic that passes through it, and thus it is usually implemented with IPsec encryption via the RFC 2406 Encapsulating Security Payload (ESP) protocol [http://www.rfc-editor.org/rfc/rfc2406.txt](http://www.rfc-editor.org/rfc/rfc2406.txt) component of IPsec: this then provides end to end encryption for data passing through an integrated L2TP/IPsec OSI layer 3 (network) VPN tunnel. “Securing L2TP using IPsec” is described in [http://www.rfc-editor.org/pdfrfc/rfc3193.txt.pdf](http://www.rfc-editor.org/pdfrfc/rfc3193.txt.pdf). Since L2TP can tunnel PPP traffic, it can support transport across non-IP layer 2 protocols such as Frame Relay and ATM.


High Risk Data or Sensitive Data Collections data transmissions must use keys with an effective key length of 128 bits or more (Medium Strength), and thus **use of the 56 bit DES encryption key is prohibited**.

The RFC 2409 IKE (Internet Key Exchange) [http://www.rfc-editor.org/rfc/rfc2409.txt](http://www.rfc-editor.org/rfc/rfc2409.txt) phase of IPsec negotiation can be performed with X.509 public key digital certificates or Kerberos authentication (MS Active Directory) – both being the more secure methods, or with a preshared secret - the less secure method. The more secure methods readily meet the requirements of Policy DCS7.a, "The identities of the sender and the recipient must be authenticated" and the protocol negotiation process incorporates the requirement of Policy DCS.7.b, “The recipient must agree to participate in the data transmission”.

OSI Layer 4 (session) User authentication in L2TP is performed by the same MS-CHAP v2 EAP-TLS authentication process as PPTP, but L2TP adds computer (machine) authentication.

As of Windows Server 2008, 3DES encryption algorithm with Message Digest 5 (MD5) integrity check support has been removed, but can be added (not recommended) by changing a registry key. The Microsoft VPN Client removed support for L2TP VPN connections as of Windows 7 in favor of SSTP.

DCS.S.7.2.1.3.e Microsoft SSTP VPN permitted for High Risk Data or Sensitive Data Collections data transmissions

Secure Socket Tunneling Protocol (SSTP) is a Microsoft proprietary tunneling protocol encapsulating PPP or L2TP traffic over the version 3.0 Secure Sockets Layer (SSL) channel of the HTTPS protocol (TCP port 443).

Data encryption for PPTP or SSTP connections is available only if MS-CHAP v2 or EAP-TLS is used as the authentication protocol; CHAP should not be selected (CHAP utilizes insecure reversibly encrypted format passwords). Data Encryption should be set to Maximum strength encryption to enable 2048-bit encryption. SSTP uses 2048 bit certificates for authentication. Microsoft SSTP is available for Windows Vista Service Pack 1 (SP1), Windows Server 2008, and later versions. A SSTP Client has also been developed under the Ubuntu Linux distribution.

DCS.S.7.2.1.3.f Microsoft IKEv2 VPN permitted for High Risk Data or Sensitive Data Collections data transmissions

The Microsoft IKEv2 VPN is described at “Configure IKEv2-based Remote Access” http://technet.microsoft.com/en-us/library/ff687731(v=WS.10).aspx. IKEv2, a tunneling protocol that uses the IPsec Tunnel Mode protocol to encapsulates datagrams by using IPsec ESP or AH headers for transmission over UDP port 500, is described in “Internet Key Exchange (IKEv2) Protocol” http://www.rfc-editor.org/pdfrfc/rfc4306.txt.pdf. Strong 192 bit AES or 256 bit AES encryption keys or Medium Strength 128 bit AES or 168 bit 3DES (effectively 112 bits) encryption keys can be generated during the IKEv2 negotiation process.

Microsoft VPN clients only support IKEv2 on Windows 7 and Windows Server 2008 R2 systems and later versions, and are permitted for High Risk Data or Sensitive Data Collections data transmissions.

DCS.S.7.2.1.3.g Microsoft PAP Prohibited for authentication of High Risk Data or Sensitive Data Collections data transmissions

Authentication via the Microsoft Password Authentication Protocol (PAP) Unauthenticated Access for any application or service allowing High Risk Data or Sensitive Data Collections data transmissions is prohibited. Enabling PAP as an authentication protocol means that user passwords are sent from a client to the application or service in plain text.
## DCS.S.7.2.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>ITGC Policies and Procedures Committee (creator)</td>
<td>Initial document</td>
<td>Nov. 11, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.7.0 High Risk Data or Sensitive Data Collections Transmission Security
Introduction

These guidelines establish mechanisms to guarantee the integrity and confidentiality of data transmitted over insecure networks or any other insecure communications channel.

DCS.G.7.1 High Risk Data or Sensitive Data Collections Transmission Security Guidelines

Policy DCS.7.a High Risk Data or Sensitive Data Collections Transmission Security requires that the identities of the sender and the recipient of a transmission of High Risk Data, or of Sensitive Data Collections, must be authenticated.

The same Policy section also requires that in the case that the transmission is unidirectional from the sender to the recipient, then the identity of the recipient must be authenticated.

In both cases above, typically this authentication is carried out as part of the process establishing, and then periodically renewing, the transmission channel. The identities may be authenticated through a shared secret, through interface with other identity directory services, or through a PKI infrastructure which provides authentication services to the application establishing the transmission channel.

See High Risk Data and Sensitive Data Collections definitions in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
a. The data transmission **must** be encrypted according to the minimum specifications of the UIC Information Technology Security Standard **DCS.S.7.1.c.1 “128 bit or higher encryption required for SSL or TLS "SSL" High Risk Data or Sensitive Data Collections Data transmissions”**. Standard **DCS.S.7.1.c.2** lists “**Prohibited High Risk Data or Sensitive Data Collections SSL or TLS/ "SSL" Transmission Protocols**”. Standard **DCS.S.7.2.1.c.3** advises “**TLS 1.2 Preferred for High Risk Data or Sensitive Data Collections Data transmissions**”. Standard **DCS.S.7.1.c.4** holds “**128 bit or higher encryption required for SSH "SSL" High Risk Data or Sensitive Data Collections Data transmissions**", and Standard **DCS.S.7.1.c.5** holds “**SSH version 2.0 required for SSH "SSL" High Risk Data or Sensitive Data Collections Data transmissions**”.

Either the data transmission channel **must** be encrypted, or the data **must** be encrypted prior to transmission. Typically the application establishing the transmission channel permits configuration of the type and strength of encryption. In cases where a secure transmission channel cannot be established, and alternate mechanism to protect the High Risk Data or Sensitive Data Collections during transmission is to encrypt their data prior to transmitting the data as a file.

**DCS.G.7.1.1 High Risk Data or Sensitive Data Collections Data Transmission Integrity Controls Guidelines**

Digital signatures of High Risk Data or Sensitive Data Collections data transmissions **are required** in order to ensure a recipient of the authenticity of the transmitted digital data and to guarantee the integrity of the data in transmission and must be implemented through Message Authentication Code / Message Digest as a component of the encryption requirements collectively meeting the minimum specifications of the **DCS.S.7.2.1.c.1 High Risk Data or Sensitive Data Collections Data Transmission Integrity Controls Standard**.

**DCS.G.7.1.2 Data Transmission Confidentiality Controls (Encryption) Guidelines**

Data encryption security settings **must** meet or exceed the Standard **DCS.S.7.2.1.c.4 “128 bit or higher encryption required for SSL or TLS "SSL" High Risk Data or Sensitive Data Collections Data transmissions”**, Standard **DCS.S.7.2.1.c.5** holds “**SSH version 2.0 required for SSH "SSL" High Risk Data or Sensitive Data Collections Data transmissions**, Standard **DCS.S.7.2.1.3.a “128 bit RC4 encryption required for Microsoft Remote Desktop Protocol High Risk Data or Sensitive Data Collections Data transmissions”**, or Standard **DCS.S.7.2.1.3.d “128 bit or higher encryption required for Microsoft L2TP/IPsec VPN High Risk Data or Sensitive Data Collections Data transmissions”**.

Any other protocols utilized in transmissions of High Risk Data or Sensitive Data Collections Data **must** also effectively meet a minimum encryption 128 bit encryption level, and null encryption is **prohibited** for such transmissions.
A Virtual Private Network (VPN) allows a private network (in most plausible use cases) to be extended across a potentially shared network infrastructure and non-private networks to a remote private network or remote network device. VPNs provide a logical path (“VPN tunnel”) for encapsulated private data packets, allowing them to securely traverse a public network.

Examples of VPNs include 1) a Workforce member’s off-campus computer’s transmissions encrypted by a VPN client when then establishes a VPN tunnel through their ISP’s network and across the internet to the campus intranet, terminating upon the local department network, 2) a campus offsite branch office network’s traffic being collectively gathered into a site-to-site VPN tunnel, and traversing through their ISP’s network and across the internet to the campus intranet, terminating upon the local department network.

With appropriate VPN encryption ciphers and “authentication” (Message Authentication Code / Message Digest) digital signature (see the individual standards under the DCS.S.7 High Risk Data or Sensitive Data Collections Transmission Security Standard) the confidentiality and integrity of the transmissions can be ensured, and utilization of the VPN is capable of being restricted to a defined set of network devices or networks and routed between them according to a separate and discrete routing table from the commodity internet traffic routing of the networks participating in the VPN tunnel.

At this date, ACCC is transitioning from the OpenVPN VPN client to the Viscosity VPN client. Legacy (already installed) VPN clients might still use the OpenVPN VPN client, but beginning September 3rd, 2014 the Software Webstore only distributes the Viscosity VPN client. Further information on the VPN client is available at http://accc.uic.edu/tag/vpn

The ability to access a desktop computing and file storage environment from a remote location with respect to the UIC campus can be highly useful, and in some cases, essential to University core business processes, but it can simultaneously can pose serious security risks, particularly for High Risk Data and Sensitive Data Collections data transmissions if they are not secured using appropriately configured encryption and authentication.

Workforce members should contact their Unit’s IT services office to inquire about this VPN client capability. The PER.4 Access Establishment and Modification, and PER.5 Access Authorization Policies have generic provisions for workforce member requests for such services to be reviewed and processed. If the Unit does not provide assistance with VPN client services, the ACCC Client Services Office should be contacted for further assistance.
DCS.G.7.1.4 Secure File Transfer

Several mechanisms are available to permit secure transfer of files under these Policies. The SFTP and SCP applications, both of which utilize the SSH protocol suite, suffice as long as the SFTP or SCP client is configured to meet the same standards as for a SSH client given at Standard DCS.S.7.2.1.c.4 “128 bit or higher encryption required for SSH "SSL" High Risk Data or Sensitive Data Collections data transmissions” and Standard DCS.S.7.2.1.c.5 “SSH version 2.0 required for SSH "SSL" High Risk Data or Sensitive Data Collections data transmissions”. A remote desktop client configured to meet Standard DCS.S.7.2.1.3.a, “128 bit RC4 encryption required for Microsoft Remote Desktop Protocol High Risk Data or Sensitive Data Collections data transmissions”, also suffices secure transfer of files under these Policies.

DCS.G.7.1.5 Other remote desktop access methods prohibited

Per Standard DCS.S.7.2.1.3.b, “Prohibited Remote Desktop access applications”, only properly configured Microsoft Remote Desktop, or SSH Server with or without X Server, applications along with the ACCC provided OpenVPN are the permitted methods of remote desktop access. Installation and usage of any other remote access application such as GoToMyPC or LogMeIn is prohibited on University systems because those applications do not require adherenceto the UIC Information Technology Security PER.3b ACCC Common Password Strong Password Policy, or allow administrative verification of adherence to that Policy.

In some UIC units secure remote desktop access is provided by Citrix products, and may meet the provision of this Policy to allow users to remotely login, access, and manipulate data.

DCS.G.7.1.6 Non OpenVPN VPN solutions

The ACCC provided Viscosity VPN client is the Endorsed campus solution\(^{100}\) to potentially permit the workforce to access their UIC desktop environment remotely. Some workforce members may utilize other solutions to arrive at the same level of functionality while remaining compliant with this Program. Standard DCS.S.7.2.1.3.c directs “Microsoft PPTP VPN Prohibited for High Risk Data or Sensitive Data Collections data transmissions”.

Approved non-OpenVPN VPN solutions include those meeting the specifications contained in Standard DCS.S.7.2.1.3.d “128 bit or higher encryption required for Microsoft L2TP/IPsec VPN High Risk Data or Sensitive Data Collections data transmissions”, Standard DCS.S.7.2.1.3.e “Microsoft SSTP VPN permitted for High Risk Data or Sensitive Data Collections data transmissions”, and Standard DCS.S.7.2.1.3.f “Microsoft IKEv2 VPN permitted for High Risk Data or Sensitive Data Collections data transmissions”.

\(^{100}\) See “Endorsed campus solution” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
DCS.G.7.2 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of this High Risk Data or Sensitive Data Collections Transmission Security Guideline.

The head of the IT unit, with review by the UISO, is typically responsible for making sure that any Unit University business process requiring transmission of High Risk Data or Sensitive Data Collections Data meets the requirements of this Guideline.

DCS.G.7.4 Resources


“Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in NIST Special Publications 800-52, Revision 1, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations (September 2013) [http://csrc.nist.gov/publications/drafts/800-52-rev1/draft_sp800_52_r1.pdf]; NIST 800-77, Guide to IPsec VPNs (December 2005) [http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf]; or NIST 800-113, Guide to SSL VPNs (July 2008) [http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf], and may include others which are FIPS 140-2 validated.”

DCS.G.7.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>ITGC Policies and Procedures Committee (creator)</td>
<td>Initial document</td>
<td>Nov. 11, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.9.0 Develop and Implement Media Reuse Procedures Guideline

Introduction

Various classes of University Data may be stored upon Portable media, and Policy DCS.4 Encryption and Decryption of Stored Data specifies how High Risk Data and Sensitive Data Collections must be stored. When the storage media is no longer needed to store the DCS.4 controlled data, the data must be securely removed from the storage media before it is reused. This Guideline describes processes which accomplish that goal.

DCS.G.9.1 Develop and Implement Media Reuse Procedures Guidelines

In order to more easily manage data, it is important to understand the different types, or classes, of data and the policies, procedures, and guidelines. The procedure for data sanitization depends on the type of media and its destination.

a. Media destruction is only permissible in the case of optical disks (such as CDs or DVDs), floppy disks, and magnetic tapes. Do not destroy University equipment such as hard drives yourself. It is illegal and a job for University Surplus. Detailed information on surplus procedures can be found in the Office of Business and Financial Services disposal manual.

b. Magnetic tapes should be overwritten.

c. Floppy disks should be degaussed, overwritten, or destroyed.

d. Optical disks (CDs/DVDs) should be shredded in a CD-capable shredder.

e. Hard drives should be overwritten or encrypted with key deletion (see below).
f. *Memory* (flash drives) should be overwritten or destroyed.

g. *Portable devices* (PDAs, cell phones, etc.) should be hard reset as specified by the device manufacturer.

<table>
<thead>
<tr>
<th>Destination for Media</th>
<th>Media Overwrite Required/Recommended</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Surplus</td>
<td>Single pass, such as the DBAN software's “quick erase” mode</td>
<td>Department of Defense (DoD) Short or equivalent</td>
</tr>
<tr>
<td>Transfer between units</td>
<td>Single pass</td>
<td>DoD Short or equivalent</td>
</tr>
<tr>
<td>Transfer between individuals</td>
<td>Single pass</td>
<td>DoD Short or equivalent</td>
</tr>
<tr>
<td>Transfer between individuals within a workgroup</td>
<td>None: If media is transferred between individuals within the same workgroup (i.e., between researchers within the same research group), media does not need to be overwritten, provided that the recipient is authorized to access all data stored on the media in question.</td>
<td></td>
</tr>
<tr>
<td>Transfer outside of University</td>
<td>DoD Short</td>
<td>DoD Short or equivalent</td>
</tr>
<tr>
<td>Return of non-functional drive to vendor</td>
<td>Disk should be degaussed before sending back.</td>
<td>A degausser is available through ACCC.</td>
</tr>
</tbody>
</table>

h. Media overwrite software

1. UIC has site licenses for special software is available to perform the data overwriting. The software is Active Eraser for Windows (or any DOS/Bootable personal computer such as a Linux PC) The software is available through the University of Illinois [WebStore](#), free of charge to all faculty and staff. For more information on this software, see Secure Data Erasers for Windows and Macs.

2. DBAN (Darik’s Boot And Nuke) is also an industry-standard program for overwriting hard drives, and WeibeTech Drive Eraser is considered by University Audits as an acceptable overwriting program as well.
**DCS.G.9.2 Responsibility for Implementation**

The Unit head or delegate is responsible for the implementation of the Media Reuse Procedures Guideline. The head of the IT unit, with review by the UISO, is typically responsible for making sure that processes are performed as needed.

**DCS.G.9.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Phil Reiter</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.10 Methods Used for Disposal of All Storage Media Guideline

Purpose
Access to High Risk Data, Sensitive Data Collections, Sensitive Data or Internal Data must be controlled at the end of the life cycle of the storage media it may be placed upon by specifying a secure disposal process for that media.

Process
The ACCC University Guideline on the Sale, Donation, or Transfer of Computer Hard Drives and Other Magnetic Media can be found at http://accc.uic.edu/policy/disk-scrubbing.

Responsibility for Implementation
The Unit head or delegate is responsible for the implementation of this Methods Used for Disposal of All Storage Media Guideline. The head of the IT unit, with review by the UISO, is typically responsible for making sure that processes are performed as needed.

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Phil Reiter</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DCS.G.11 HIPAA Business Associate Guideline

DCS.G.11.0 HIPAA Business Associate Guideline Introduction

The University of Illinois at Chicago, Office of Business and Financial Services (OBFS), provides standard Business Associate Contracts for Units.

DCS.G.11.1 HIPAA Business Associate Guidelines

The OBFS provided contract for Professional and Artistic Services under $5000 Requiring HIPAA (created 1/19/12, last modified 1/29/14) must be used when the University is required to provide access to its protected health information in order for a contractor to perform services, and is located under the OBFS Policies and Procedures Section 2.3 - Initiation, Review, and Approval of University Contracts and Leases:

at

In the same Section 2.3 the University of Illinois Contract $5000 or more Requiring HIPAA (Health Insurance Portability and Accountability Act of 1996) (created 5/6/13, last modified 1/29/14) is at:


Neither contract addresses the Breach notification requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The Unit should review that matter with the University of Illinois at Chicago, Office of Business and Financial Services at the time it considers allowing a contractor access to protected health information.
DCS.G.11.2 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of the HIPAA Business Associate and addressing HITECH Breach Notification requirements.

DCS.G.11.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
SS.S System Security Standard

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

SS.S.0 System Security Standard Purpose

Audience

This standard must be met by all University owned or leased Workstations\(^{101}\) and Servers\(^{102}\).

Additionally, all systems under Policy SS.11 Non-secure Systems will benefit by following as many of the SS.S.3b Workstation Standards below and the SS.G.1-11.3.1.b.2, Workstation Guidelines to be used with the SS.S.3b.2 Standard as practical.

Introduction

This standard serves to identify baseline technical requirements for the configuration and operation of Workstations or Servers. Compliance with these requirements will help ensure the secure operation of Workstations and Servers and the protection of any information assets stored on, or processed by, those computer systems.

Note that this Standard contains several sections depending on the type of device and the classification of the data stored on the device. The Standard to be met for any particular device must be the aggregate of all sections of this Program that apply to the device.

---

\(^{101}\) See “Workstation” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”

\(^{102}\) See “Server” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
SS.S.1 System Acceptable Use Agreement Standard

a. Units must be compliant with the requirements of this standard by 10/30/2015.

b. As required by Policy SS.2 Establish Workstation and Server Access Controls, each user must consent to the following System Acceptable Use Agreement before utilizing a Workstation or Server allowing access to High Risk Data or Sensitive Data Collections:

“Any individual who uses any University information technology resources including University Information Assets, whether with University or personally owned equipment, consents to all of the applicable portions of the University Information Technology Security Program and agrees to comply with all its conditions and terms of use, as well as applicable state and federal laws and regulations. The individual has a responsibility to use University resources in an ethical and lawful manner. Consequences of violations of this Program are stated in RC.2.4, Sanctions for non-Compliance. (Reference; UIC Information Technology Security Program Policy SPO.2.1, Individual Compliance).”

SS.S.3.b System Standard for all University Workstations, Portable data storage devices (including Laptops), and Servers

1. Units must be compliant with the requirements of this SS.S.3.b Standard for all University Workstations, Portable data storage devices (including Laptops), and Servers by 10/30/2015.

SS.S.3.b.2 System Standard for all Workstations

Note: SS.G.1-11.3.b.2, Workstation Guidelines to be used with the SS.S.3.b.2 Standard, lists Best practice specifications intended to be used in conjunction with this Standard for Workstations

2. The following standards must be met by any Workstation; for reference, a Workstation is defined as “any computer hardware which is implemented to provide user access to University systems, applications, or data regardless of the technology by which the data is stored, transmitted to, or accessed by that Workstation”

   i. All Workstations must operate a vendor supported operating system and be kept current with their provided security updates/patches.

   ii. All default vendor-supplied passwords must be changed before Workstations are connected to a network or deployed in production.

   iii. All user accounts must utilize the user’s University identity management system identifier (netid).
iv. Workstations must be configured with separate user and administrative accounts. Thus, unique privileged accounts must be created for each user with a need for access to elevated privileges on a system. Daily user activities must be performed from the non-privileged user account. Shared accounts with elevated privileges (such as root accounts on Unix systems) must only be used as a last resort and login access to these accounts must be documented.

v. All Workstations not bound to the campus Active Directory must be configured to require strong authentication which complies with the ACCC Common Password Strong Password Policy given at http://password.uic.edu.

vi. Workstations must be configured to automatically 'lock' and require re-authentication after a period of inactivity no longer than 10 minutes. This locking process must prevent local access to the system including preventing the execution of any non-scheduled programs. Any systems which contain Sensitive Data, Sensitive Data Collections, or High Risk Data must be locked immediately if they are left unattended. Locked systems must require re-authentication to restore access.

vii. Partial exception to previous Standard: Public Access Systems\textsuperscript{103} and Instructional Systems\textsuperscript{104} not containing or having access to Sensitive Data, Sensitive Data Collections, or High Risk Data may be configured with an extended inactivity lockout interval.

viii. Activities of privileged user accounts must be logged in accordance with policy SS.9 Audit Control Mechanisms.

ix. All Workstations not connected to the campus Active Directory must be configured to log all authentication activity in accordance with policy SS.9 Audit Control Mechanisms.

x. Applications on Workstations must be updated regularly. For applications known to cause business continuity problems if automatically updated (such as has been seen with Java and Banner), application updating may be delayed as appropriate.

xi. Workstations must have a host-based firewall installed, configured, and enabled to deter unauthorized access to the system. The access control configuration should be documented. The native Windows and OSX firewalls are considered sufficient to meet this control.

\textsuperscript{103} See Public Access Systems in "UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions"

\textsuperscript{104} See Instructional Systems in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions"
xii. Intrusion detection must be implemented, and the detection logs reviewed regularly, for Workstations containing data classified as High Risk Data or Sensitive Data Collections.

xiii. Campus site licensed security (antivirus/malware) software (or equivalent) must be installed and enabled to protect the Workstation from malicious software. See http://accc.uic.edu/tag/antivirus for further information.

xiv. Workstations must be placed in locations which will protect them from environmental hazards and unauthorized physical access in accordance with Policy P.2 Analyze Physical Attributes of Surroundings.

xv. Unless specifically required for University business processes, file sharing should not be installed or enabled on Workstations. The utmost care should be made to ensure that only data intended to be shared is shared via file sharing. Any Workstation containing High Risk Data, Sensitive Data Collections, or Sensitive Data must not install and enable file sharing granting access to any High Risk Data, Sensitive Data Collections, or Sensitive Data stored on that system. Where file sharing of such data is necessary for a University business process, it must be established on a securely configured Server.

xvi. Non-public information assets must not be left unattended unless they are secured. In the case of removable storage media, information assets must be physically secured when they are not in use.

xvii. All Workstations not connected to the campus Active Directory must have their system clock synchronized with an authoritative Network Time Protocol (NTP) source such as ntp-0.cc.uic.edu or ntp-1.cc.uic.edu.

**SS.S.3b.3 System Standard for all Portable data storage devices (including Laptops)**

1. The following standards must be met by any Portable data storage device utilized as a Workstation; for reference, a Portable data storage device is defined as “any physical data storage device designed to be readily picked up and transported by persons from workplace to workplace, as opposed to “desktop computers” or other bulkier and less transportable systems such as Servers generally meant to be utilized at a relatively permanent and single fixed physical location. Portable data storage devices include tablet, laptop, or notebook computers, handheld devices such as PDAs, USB interface storage devices including “thumb drives” and “flash drives”, and all types of removable data storage media.”

   Portable data storage devices utilized as a Workstation include laptops.

---

105 See “Portable data storage device” in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
In addition to all the above SS.S.3b.2 Workstation Standards:

i. All laptop systems that may be used to store High Risk Data or Sensitive Data Collections must be configured and operate with Whole/Full Disk Encryption\textsuperscript{106} software or hardware.

ii. Partial Exception to previous Standard: Older systems not capable of running Whole/Full Disk Encryption software may be configured to use software that fully encrypts all non-public University data stored on the computer.

iii. Laptop systems remotely accessing High Risk Data, Sensitive Data Collections, or Sensitive Data must use a Virtual Private Network (VPN) connection. VPN access and configuration information is available from http://gateway.uic.edu.

SS.S.3b.4 System Standard for all Servers

2. The following standards must be met by any Server, defined as “any system, application, or data storage device which is configured to allow access to it by a more than one user (excluding a single user per device and the system administrator, if separate from the user) either concurrently or in total.”

i. Intrusion detection must be implemented, and the detection logs reviewed regularly, for any Server containing data classified as High Risk Data or Sensitive Data Collections.

(This section has not been developed yet)

SS.S.4.1 Establish Protection from Malicious Software Standard

Each Unit, after tabulating the systems or Servers it administers in UIC Information Security Program S.1W Workstation Inventory, must identify which systems or Servers can readily permit installation and operation of security software, and on those systems have that software installed and operational.

The Unit must establish a mechanism to document and report for each system that the system security software is operational and current with manufacturer updates.

A specific explanation must be provided by the Unit for each and every system which does not have security software implemented upon it, or which is not protected by a security appliance providing compensating security coverage for multiple systems.

The University of Illinois provides site licensed antivirus and system security software for Unit and individually owned systems at its Software Sales website:

\textsuperscript{106} See Whole/Full Disk Encryption in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
SS.S.9.1 System Remote Access Standard

a. Any system meant to be accessed remotely by one or more users must meet the requirements of UIC Information Security Program Procedure PER.P.2.1 Identify Access Needs of all Users.

b. Remote access to a system by a workforce member must follow the UIC Information Security Program Procedure PER.P.5 Access Authorization.

c. Remote access connections must implement authentication, encryption, and connection logging.

SS.S.1.4 Automatic Inactive Session Locking Standard

a. Any Server or Workstation that stores or accesses High Risk Data or Sensitive Data must be configured to automatically lock the device after 10 minutes of inactivity. Once locked, the system must require re-authentication to restore access.

b. When leaving a Server or Workstation unattended, the user must place the device in a password-protected state either by activating the screen lock, locking the logged-in session, or logging off of the system.

c. Exception to above two Standards: Public Access Systems and Instructional Systems are exempt from this Automatic Inactive Session Locking Standard.

SS.S.1.8 Remote access Standard

a. Remote access connections must implement authentication, encryption, and connection logging.

b. Remote access endpoint devices must employ malware detection and protection mechanisms, if available for those devices.
SS.S.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator</th>
<th>Description</th>
<th>Submission Date</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Ed Zawacki</td>
<td>Initial composition</td>
<td>Oct. 22, 2013</td>
<td></td>
</tr>
<tr>
<td>0.9</td>
<td>UIC IT Security Program Committee</td>
<td></td>
<td></td>
<td>March 1, 2014</td>
</tr>
<tr>
<td>1.0</td>
<td>Esteban Perez and Barry White</td>
<td>Incorporation of Urbana standards, modified or replaced by UIC specifications</td>
<td></td>
<td>August 26, 2014</td>
</tr>
</tbody>
</table>
SS.G System Security Guideline

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

SS.G.1-11.0 Purpose

This System Security Guideline establishes the recommended measures needed to protect University information accessed through University computers and networks from being disclosed to unauthorized persons and to provide accountability for usage of Workstations and Servers. In addition to this guideline, the reader should be aware that there are also System Security Standards that must be followed. Each member of the workforce is responsible for maintaining the physical security of computer resources, including systems, which they are granted use of by the University. That responsibility includes protecting the integrity and confidentiality of the data stored, accessed, or maintained on those resources.

Note: In most of the Guidelines, a specific Guideline has been prepared for each section or sub-section of the Security Policy Sections, e.g. DCS.G.2.1 and DCS.G.2.3; the standard Guideline .0, .1, .5 and so forth sections are appended to the Security Policy Sections to identify the standard Guideline sections – e.g. DCS.G.2.2.1 is the Information Systems Classification Guideline.

In this Guideline, all of the Systems Security Guidelines are combined, and the second digit in the numbering series for the Guideline section refers to the calling Security Policy section, thus hereunder:

Security Policy Section | corresponding Guideline
---|---
SS.2 | SS.G.1-11.2.1 Establish System Access Controls Guideline
SS.3 | SS.G.1-11.3.1 Identify System Types and Functions or Uses, and Ensure their Security Guideline
SS.4 | SS.G.1-11.4.1 Establish Protection from Malicious Software Guideline
SS.1-11 | SS.G.1-11.2 Responsibility for Implementation
SS.G.1-11.2.1 Establish System Access Controls Guideline

a. Establishing System Access Controls begins by obtaining or updating an inventory of systems administered by a Unit. This inventory is built from the UIC Information Security Program P.W.1.a Facilities Worksheet which is a Unit’s listing of the locations under its control. That worksheet is easily obtained initially as an export from the UIC Office of Facility Planning and Space Analysis (FPSA), as detailed in the UIC Information Security Program Physical Security Guideline P.G.

1. Each individual system in the Unit must be tabulated, for example, in a column added to the P.W.1.a Facilities Worksheet or in a separate table or spreadsheet linked to that worksheet.

2. Continuing with the P.W.1.a Facilities Worksheet, the Unit must identify whether or not each system is capable of or actually connected to a network, and if it is portable. The resulting completed tabulation, or report of it, is identified here at this stage as the UIC Information Security Program SS.W.1 Workstation Inventory.

b. The Unit must establish a mechanism such as a login banner requiring the user’s consent to a System Acceptable Use Agreement before they are allowed to utilize a Workstation or Server allowing access to High Risk Data or Sensitive Data Collections. This mechanism, the language of the consent agreement, and how the mechanism is enforced must be documented.

As an example, a standard login banner or equivalent information display should state:

Any individual who uses any University information technology resources including University Information Assets, whether with University or personally owned equipment, consents to all of the applicable portions of the University Information Technology Security Program and agrees to comply with all its conditions and terms of use, as well as applicable state and federal laws and regulations. Users have a responsibility to use University resources in an ethical and lawful manner. Consequences of violations of this Program are stated in RC.2.4, Sanctions for non-Compliance. (Reference; UIC Information Technology Security Program Policy SPO.2.1, Individual Compliance).

SS.G.1-11.3.1 Identify System Types and Functions or Uses, and Ensure their Security Guideline

A Unit is responsible for ensuring adequate mechanisms are in place to establish that all systems are in a secure state before workforce is granted access to the systems, and that the systems are maintained in a verifiable secure state.

a. In order to do this, the Unit should establish broad categories of systems, for example by which of the Unit’s DCS.2.1 Identify Core Business Functions’ core business functions, or groups of those functions, are allowed to be carried out on those systems.

At the minimum, a specific category must be created for:
2) each Workstation allowed to connect to:
   I. High Risk Data,
   II. Sensitive Data, and
   III. neither High Risk Data nor Sensitive Data

or

   I. both High Risk Data and Sensitive Data, and
   II. neither High Risk Data nor Sensitive Data

and also for

3) each Server the Unit may administer containing either:
   I. High Risk Data
   II. Sensitive Data
   III. both High Risk Data and Sensitive Data
   IV. neither High Risk Data nor Sensitive Data

b. After establishing these categories, the Unit must establish policies and procedures addressing allowed usage of each category of system, identifying and accommodating their unique issues while securing them and permitting their correct utilization. The steps taken to secure every member of each category of systems must be documented, and the Unit must document when each system is taken through a complete process to bring a system to a known secure state (typically, initial configuration of a system, or its maintenance rebuild).

3. Maintaining a system’s secure state, for example with software manufacturer supplied security updates, must be documented. If the system or its installed software has the capability for automatic updates to be configured, then when that is enabled it must be documented and the operation of those automatic updates must be logged. Either the update logs must be reviewed periodically, or there must be a mechanism to run an ad-hoc test to verify the automatic update process is working correctly. Any ad-hoc system maintenance affecting the security of a system must be documented.

4. These policies and / or procedures must establish a mechanism for educating the system users about the allowed usage of the systems. Additionally, the policies and / or procedures need to address or refer to the UIC Information Technology Security Program Procedure PER.P.2 Job Descriptions, Responsibilities, and Training, Procedure PER.P.4 Access Establishment and Identification, and Procedure PER.P.5 Access Authorization. Those PER Procedures provide for documentation of when and how each of its policies and/or procedures requirements have been carried out for each staff member allowed access to a Workstation or Server.
SS.G.1-11.3.b.2 Workstation Guidelines to be used with the SS.S.3.b.2 Standard

The following general guidelines should be implemented on all University owned or leased Workstations, and are meant to be used in conjunction with the SS.S.3.b.2 Standard for all Workstations. Additionally, Policy SS.11 Non-secure Systems will benefit by following as many of these Guidelines below and the SS.S.3.b.2 Standard as practical.

i. Workstations should be managed by a qualified IT Professional. This IT Professional should be responsible for, among other duties, management of patching and updating the system.

ii. User privileges should be controlled in order to prevent unauthorized installation of software.

iii. Workstations should have an operating system capable of connecting to a centrally managed computing environment, and support file/disk encryption when available.

iv. Workstations should be bound with the campus Active Directory for authentication and group policy management.

v. Software which is not needed for the performance of University business duties should not be installed on Workstations.

vi. Changes to applications on Workstations should be controlled, and should be limited to only those changes which are needed for University business processes and continuity and which will not compromise application or data security.

vii. System and application errors on Workstations should be logged, and reviewed on a periodic basis.

viii. Workstations should be manually locked before being left unattended.

ix. Workstations which would have a significant impact on a Unit’s University business processes if they were to fail should be protected from power failures and interruptions by connecting them to uninterruptible power supplies. The Workstations should be configured to allow for appropriate system shutdown in the case of power failure.

x. Workstations should be configured and operate with Whole/Full Disk Encryption (FDE) software or hardware. Older systems not capable of running FDE software should be configured to use software that fully encrypts all non-public University data stored on the computer.

xi. Workstations should have Secunia CSI and/or PSI installed for the required application update/patch management. Both of these products have been licensed
for use on all University owned equipment and can be managed through a central console. Secunia PSI is available from the WebStore. Secunia CSI is available by contacting security@uic.edu

xii. System logs should be monitored by those parties responsible for management of the system in order to detect any unauthorized access.

xiii. When remotely accessing campus systems with High Risk Data, Sensitive Data Collections, or Sensitive Data, a VPN should be established to protect the data transfer. VPN access and configuration information is available from http://gateway.uic.edu

xiv. Security measures which should be used to protect University of Illinois non-public information assets stored on desktop computers include, but are not limited to:

A. Locking information processing devices to stationary/secure objects (i.e., using a locking cable to secure a desktop system to a desk)

B. Maintaining physical control of any removable media containing University of Illinois information assets.

C. Encryption of data on removable storage media.

D. Storage of data on central file Servers, rather than storing data locally.

E. Use of a secure data deletion program such as the use of Active@ Eraser for Windows OS available from the Webstore, or the Disk Utility's erase free space feature of Mac OS X v10.5 and later.

F. Use of a privacy screen filter should be used on devices routinely accessing Sensitive Data or High Risk Data

xv. Web browsers used on Workstations should be configured to use available add-ons to ensure secure browsing. Some examples of applicable add-ons are:

A. Web of Trust (WOT) is a website reputation and review service Firefox Add-on
   https://www.mywot.com/

B. The NoScript Firefox Add-on allows JavaScript, Java, Flash and other plugins to be executed only by trusted web sites of your choice. It is available for the Firefox, Seamonkey and other Mozilla-based browsers
   http://noscript.net/

C. Several products use the name AdBlock:
I. The AdBlock Plus for Firefox Add-on blocks ads, and optionally can block tracking, malware domains, and Social Media Buttons
   https://adblockplus.org/en/firefox

II. AdBlock for Chrome blocks all advertisements on all web pages
    https://chrome.google.com/webstore/detail/adblock

III. AdBlock Web Browser for iOS is a standalone web browser that automatically blocks downloading of unwanted resources from 9600+ known web activity tracking and advertising domains

D. Additional recommendations for securing your web browser are available from CERT at http://www.cert.org/historical/tech_tips/securing-web-browser-index.cfm

xvi. Formal acceptance criteria should be established for all new desktop systems, and appropriate tests of new desktop systems should be performed prior to acceptance. This criteria should list all security and operational requirements of each desktop system.

SS.G.1-11.3.b.3 Portable data storage devices (including Laptops) Guidelines to be used with the SS.S.3.b.3 Standard

The following general guidelines should be implemented on all University owned or leased Portable data storage devices (including Laptops), and are meant to be used in conjunction with the SS.S.3.b.3 Standard for all Portable data storage devices (including Laptops). Additionally, Policy SS.11 Non-secure Systems will benefit by following as many of these Guidelines below and the SS.S.3.b.3 Standard as practical.

In addition to all Workstation guidelines:

i. Laptop systems should have location software installed to assist in locating systems if they are stolen or misplaced. The use of Computrace LoJack, available through the Webstore https://webstore.illinois.edu/ (e.g. LoJack for Laptops Premium Personal Use - 1 year subscription license $23 as of 09/09/14) is highly recommended.

ii. Portable data storage devices should be protected by being placed in rooms with locked doors if left unattended, and physical access to them should only be granted to the minimum set of Workforce needing access.
SS.G.1-11.11.1 Non-secure Systems Guideline

As UIC Information Security Program Policy SS.11 Non-secure Systems, states, personal computers not administered and secured by Unit staff with this Guideline SS.G are non-secure systems.

UIC Information Security Program Policy SS.11 Non-secure Systems describes the reasonable steps Workforce members utilizing Non-secure systems to access University systems are responsible for taking to ensure the Non-secure systems meet a minimum security baseline.

Non-secure systems should follow the SS.G.1-11.3.b.2 Guidelines where practical, and the SS.S.3.b.2 Standard for all Workstations or SS.S.3.b.3 Standard for all Portable data storage devices (including Laptops) as applicable.

SS.G.1-11.2 Responsibility for Implementation

The UISO is responsible for this SS.G.1-11.2.1 Establish System Access Controls Guideline and the SS.G.1-11.3.1 Identify System Types and Functions or Uses, and Ensure their Security Guideline, and typically accomplishes this work in coordination with Unit IT staff.

Workforce members are responsible for implementing Policy SS.11 Non-secure Systems under the terms of this SS.G.1-11.11.1 Non-secure Systems Guideline.

SS.G.1-11.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator</th>
<th>Description</th>
<th>Submission Date</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Initial document</td>
<td>November 18, 2013</td>
<td></td>
</tr>
<tr>
<td>0.9</td>
<td>UIC IT Security Program Committee</td>
<td></td>
<td></td>
<td>March 1, 2014</td>
</tr>
</tbody>
</table>
**NS.G Network Security Guideline**

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

**NS.G.0 Network Security Guideline Purpose**

Network Security is a key component in the security of systems with active network connections.

**NS.G.1 Network Security Guideline**

a. As described at UIC Information Technology Security Program Policy [NS.2 Unit Network Perimeter Security](#), units at UIC mostly utilize the ACCC as combined Ethernet and wireless network infrastructure provider, and internet service provider. When units develop their risk management plan, they will be able to obtain documentation of the network access controls implemented by the ACCC at the Unit’s network perimeter.

b. Any Unit utilizing a different network infrastructure provider, or any different internet service provider, must obtain documentation from that provider of the network access controls implemented by the provider at the Unit’s network perimeter.
### NS.G.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
P.G.0 Purpose

This Physical Security Guideline establishes the measures needed to protect systems, buildings, and supporting infrastructure (actual physical locations) against Threats associated with their physical environment. Those Threats are defined as “(a)ny circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”

P.G.1.1 Facility Security Plan

Under the UIC Information Technology Security Program Guideline DCS.G.2.2 Identify Relevant Information Systems, each Unit will assemble, at least annually, an inventory of all systems that are used to collect, store, process, or transmit High Risk Data, Sensitive Data Collections, or Sensitive Data. As an example, this inventory can be reported on an UIC Information Technology Security Program DCS.W.2.2 Relevant Systems Inventory Worksheet or document of similar format.

a. In conjunction with that inventory, a summary table of locations where systems used to collect, store, process, or transmit High Risk Data, Sensitive Data Collections, or Sensitive Data should be tabulated in an UIC Information Technology Security Program P.W.1.a Facilities Worksheet or equivalent report. This location information can readily be obtained from the UIC Office of Facility Planning and Space Analysis (FPSA):

1. Obtain authorization to access the FPSA system. Have your Unit’s “Gatekeeper” designated by FPSA. https://fimweb.fim.uic.edu/SpaceSurvey/gate.asp contact FPSA http://www.fsp.uic.edu/Contact.html via email with a request to grant your netid access to the FPSA system.

2. Login to the FPSA web site https://fimweb.fim.uic.edu/mainnew.asp with your UIC netid credentials.

3. Select Organizational Data. To review the data by department, go to https://fimweb.fim.uic.edu/OrganizationalData/department.asp and select your department. This will bring you to the Reports Menu, and there you can select the Department Room By Room Report, then select Export in Excel. This downloaded file will act as your Unit’s UIC Information Technology Security Program P.W.1.a Facilities Worksheet.

c. Utilizing the definitions and the Advised or Required Physical Security by Security Level table below, categorize each room or area (defined below) as Physical Security Level 1, 2, 3 or 4 (levels also defined below). You can easily add a column to the P.W.1.a Facilities Worksheet you have exported from FPSA, for example, to contain that security level categorization determination you have made.

I. Definitions specific to this P.G.1.1.c Facility Security Plan (not replicated in this Program’s Definitions document, “UIC Information Technology Security Policies, Procedures, Standards, Forms and Guidelines Definitions”): any reference to these terms is in underlined font in the remainder of the document to indicate it is a defined term hereunder -

Area

Two or more adjacent, interconnected, adjoining, or contiguous rooms which for physical security purposes cannot be adequately segregated in physical terms.

Server Room

All Servers should be located in a Server room. Servers containing High Risk Data or Sensitive Data Collections must be located in a Server Room.

Server Rooms must meet the specifications of Security Level 4 (see following Section III. Advised or Required Physical Security per Security Level).

A Server Room must be prepared under an architectural plan formulated to meet the individual and aggregate manufacturers’ environmental specifications and requirements to operate planned 1) mainframe, minicomputer, or Server equipment plus 2) all interconnected external storage devices, network or telecommunication equipment, ancillary, peripheral or terminal equipment in the same room or area which are a
functional part of an infrastructure which facilitates or allows collection, processing, transmittal or storage of data.

Typically, a Server room is planned with a certain expansion capacity. A current table should be kept of the design capacities and current usage of the network, electric power supply, UPS, and HVAC utilities so that each utility is not overloaded. When new equipment is added, or equipment is removed, this table should be updated. If too much equipment is connected to the power supply, for example, the UPS runtime may fall below the minimum needed to allow safe shutdown of equipment, and circuit breakers at the power distribution panel may also be tripped. If the cooling capacity of the HVAC system is exceeded, the Server room may not stay within Server manufacturer operating specifications for ambient air temperature, in particular if the room is subject to significant heat flow from the exterior and on days when the external temperature is much warmer than the design Server room operating temperature. This in turn can lead to insufficient cooling of Server equipment dependent upon ambient air in the Server room for cooling.

Computer Equipment

Any type of computer equipment including personal computers (PCs), monitors, printers, external data storage units, peripherals and associated equipment.

Personal Computer(s) - PC(s)

Individual computer units with their own internal data processing and storage capabilities, intended for dedicated use by one individual at a time.

II. Categorization of Risk into Security Levels

The University’s Office of Business and Financial Services (OBFS) University Property Accounting and Reporting (UPAR) office administers detailed records of all items of real property and movable equipment in the custody of University units, regardless of location, acquisition method, or funding source:
http://www.obfs.uillinois.edu/equipment-management/equipment-records/

UPAR maintains the FABweb System which reports the value of computer equipment as the “Cost” of the equipment.
The above URL can be referenced to review the procedure to run a Report on Fixed Assets by Organization, and that report can then be used to obtain the cost of individual items of computer equipment in the Unit.

Guidelines for actions to mitigate threats to physical security are segregated by the location and cost of the equipment into four security levels:

Security Level 4: A single room or area containing Computer Equipment with a total cost in excess of $200,000 per room or area, or where the location is a Server Room.
Security Level 3: A single room or area containing Computer Equipment with a total cost between $20,000.00 and $200,000.00 per room or area.

Security Level 2: A single room or area containing Computer Equipment with a total cost LESS than $20,000.00 per room or area.

Security Level 1: All locations containing Computer Equipment which are open to access by the general public, and not monitored by staff during the times those locations are open to public access. Examples include classrooms, lecture halls, public conference rooms, public reception areas, open shared or common laboratories and analytical facilities, hallways and foyers.
## III. Advised or Required Physical Security per Security Level

<table>
<thead>
<tr>
<th>#</th>
<th>Security Feature</th>
<th>Security Level Feature Action:</th>
<th>1 Public area</th>
<th>2 &lt; $20K</th>
<th>3 &gt;$20K and &lt;$200K</th>
<th>4 Server room or &gt; $200K</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Marking of Equipment</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>2</td>
<td>Lockdown Device</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Positioning of computers away from windows</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>High Risk Situation(s) - Window locks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Blinds for windows where interior is observable</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>6</td>
<td>Door and lock specification for entry to room or area</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Certified Security System Alarm System</td>
<td>RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Protection of alarm signal transmission to Alarm Receiving Center</td>
<td>RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Location of Intruder Detection devices and Intruder Alarms</td>
<td>RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Walk test of movement detectors</td>
<td>RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Check that movement detectors are not obscured</td>
<td>RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Anti-masking intruder alarm sensors in room or area</td>
<td>RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Break glass alarm sensors</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Individual alarm zoning of the room or area</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Alarm shunt lock at entry</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Visual or audio alarm confirmation</td>
<td>RI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Additional Requirements for Security Level 4 Server Room</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Additional requirements for High Risk Situation Server Room</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Temperature and humidity monitoring for Server Room</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Where a table entry is shown as N/A (not applicable), this is due to a generally higher specification being required thereby removing the necessity for the lower security feature.
Security Feature Descriptions

(Ordered by the above Advised or Required Physical Security by Security Level table)

1. Security Marking

All Computer Equipment meeting the University definition of “Equipment” as stipulated in the University Office of Business and Financial Systems (OBFS) document “Equipment Management”

http://www.obfs.uillinois.edu/equipment-management/

where feasible must have a physical label affixed to it. The requirements for the type of label and its placement, and exceptions for this requirement, are given in the OBFS document “Equipment Management - Reference Numbers and Labels”

http://www.obfs.uillinois.edu/cms/one.aspx?portalId=909965&pageId=913241

OBFS mandated labelling techniques cannot be substituted by marking with paint or ultraviolet fluorescent ink (indelible or otherwise), or by affixation of adhesive labels with the same wording as OBFS supplied labels unless the substitute labels have a chemical etching ability.

2. Lockdown Device(s)

A combination of two metal plates, one for affixing to furniture, or to the building structure, and the other for restraining Computer Equipment, which is immobilized when the two plates are locked together or permanently attached with a security cable. The plate attached to the Computer Equipment should incorporate an enclosure or other mechanism which will hinder unauthorized removal of the outer PC or other Computer Equipment casing and render access to internal components difficult.

Computer Equipment in a Level 1 area, or any item of Computer Equipment with a purchase price in excess of $20,000 which is in a room or area not covered by a Certified Security System Alarm System, should have a Lockdown Device attached to it and locked. The Unit should restrict access to the lockdown keys to staff responsible for maintaining the Computer Equipment, and should have a documented procedure for issuance and return of the keys. When it is impossible or undesirable to anchor hardware with a Lockdown Device, Computer Equipment can be moved to a security storage room or locked cabinet outside normal hours of room occupation.

Computer Equipment fitted with a Lockdown Device will be kept locked at all times unless being repaired or serviced by authorized personnel.
3. **Positioning of Computers away from windows**

A High Risk Situation is any room or area which is in a remote, concealed or hidden location, or which is accessible from an exterior elevation by a door or window located:

   a) at ground floor level
   
   b) along the adjoining roof
   
   c) at any building elevation level accessible via external fire escapes or other features which in turn are readily accessible from ground level.

Where possible, Computer Equipment should be kept at least 1.5 yards away from external windows in High Risk Situation(s).

4. **High Risk Situation(s) - Window Locks**

All windows in a High Risk Situation capable of being opened must be fitted with key operated locks or security devices/fasteners and kept locked or fastened.

5. **Blinds**

All external windows providing the public with unrestricted external view to within rooms containing Computer Equipment should be fitted with window blinds or obscure filming. These blinds should be closed before the room is locked.

6. **Door and Lock Specification**

All doors giving access to a room or area both should be constructed, at a minimum, out of solid wood or metal, and preferably be windowless.

Level 3 rooms or areas containing Computer Equipment not secured by lockdown devices should have doors with locks unless they are part of an internal suite for which all entry doors have locks, and the entry doors are locked when the suite is closed at the end of regular business hours. The door to a Level 3 room or area should be locked at the end of regular business hours.

Doors with locks should have key issuance administered by the University Locksmith. The lock should keyed to a Medeco lock system, and not an earlier non-bastard lock system such as Best or Russwin – in addition to keys specific to the lock, non-bastard locks can also be opened with great grand master keys and building master keys. Installation of a Medeco lockset costs approximately $40 more than a Best or Russwin lockset, and the key copy costs are the same.

Keys to a Level 3 room should only be issued to Unit staff requiring access to the room.
Door fittings should comprise 3 hinges. Inward opening doors to the room or area should have a metal strip strengthening the locking post of the doorframe.

Where a door is windowed as a fire safety code requirement, and entry is possible by breaking the window to reach an internal manually opened door bolt or lock, or an alarm control panel or alarm disabling mechanism, the window should be supplemented internally with laminated glass while retaining wired glass if required by code for fire resistance.

7. **Certified Security System Alarm System**

A commercial alarm system must have a valid and current Underwriters Laboratory Alarm system certificate designating the system has been installed, maintained, tested and monitored under the requirements of the Underwriters Laboratory Alarm System Certificate program.

ystems/cert/

8. **Protection of Alarm Signal Transmission**

The Security System Alarm System signaling to the Alarm Receiving Center should have a continuous monitoring capability so that an alarm is generated at the Receiving Center if the signal channel is disrupted or broken.

9. **Location of Intruder Detection devices and Intruder Alarms**

Intrusion detection devices should be located within the room or area, and if necessary elsewhere in the premises, to ensure that unauthorized access to the room or area is not possible without detection. The alarm location specification should include an assessment as to whether access to the alarm is possible via external elevations, doors, and windows etc.

10. **Walk test of movement detectors**

A walk-through test of movement detectors should be undertaken on a regular basis in order to ensure that all Computer Equipment is located within the alarm-protected area. This test is necessary due to the possible ongoing changes in the position of furniture, screens and partitions which may seriously impede the field of coverage provided by existing detection devices.

11. **Check Detectors**

Building managers should ensure, as part of their normal duties at locking up time, that internal space alarm movement detectors have not been individually obscured nor had their field of vision restricted.
12. Anti-Masking Intruder Alarm

Anti-masking intruder alarm movement sensors are recommended to immediately detect a movement within the room or area. This feature used to detect attempts to blind a detector by blocking the detector’s field of view (for example, by placing objects in its field of view, or spraying the lens with paint or taping it over). Masking may be attempted on an alarm to allow intruders to enter the premises at a later stage without being detected; or when the system startup (for example, on a programmed schedule) is actuated by the detector itself.

13. Break Glass Alarm Sensors

Break Glass alarm sensors are recommended to detect forced entry through any external windows of the room or area.

14. Alarm Zoning

The ability to zone the intruder alarm from the building main alarm control panel should be provided if the same alarm system shall enable authorized usage of other areas of the building outside normal hours, whilst retaining alarm detection within the room or area.

15. Alarm Shunt Lock

The alarm should have the facility for setting and unsetting the alarm within the room or area independently of the status of the main premises control panel via a shunt lock on the room or area access door. It should not be possible to set the main premises alarm if the room or area detection is 'shunted out'.

16. Alarm Confirmation

Visual or audio alarm confirmation should be provided at the central monitoring facility for all alarm activation within the room or area.

17. Additional Requirements for Security Level 4 Server Room

Partitions separating the Server Room from adjoining rooms and corridors should meet or exceed the minimum local building code requirements for rooms of devoid of windows or other openings except for secure doors as defined below. If the perimeter of the Server Room has windows, they should be backed internally with mesh or laminated glass.

Secure doors giving access to the Server Room from within the building should be solid metal and without windows. The door lock mechanism should at a minimum have a unique registered keyset or be a keypad touch lock or identification card reader with the access restricted to authorized personnel. Unless required otherwise by fire safety codes, Server Room doors should be inward opening. Door fittings, if outward opening, should comprise 3 hinges with security hinge studs to provide additional security against forced entry. All doors providing access to a Server Room must be set in a metal doorframe.
To reduce the risk of flooding, no water, sewage, rainwater or drainage pipes should run within the Server Room or within a grade which leads to the Server Room.

If water must be supplied to or stored in the Server Room, each grade area of the Server Room must have a floor drain capable of discharging the maximum flow possible from the water supply or storage source. The floor drain system should also be able to accommodate the expected flow from any source outside the Server Room which can enter it by any openings in the ceiling, walls, or floor.

The Server Room equipment should be sufficiently elevated on a rack or pediment to be above the maximum water level expected in the room in case of a flood event. A raised false floor would permit computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.

Electrical power distribution and control switches and equipment should be raised from the floor above the maximum water level expected in the room in case of a flood event to allow safe shutdown of computer systems in case of flooding.

Where possible, computer grade generator power should be provided to the Server Room to help sustain runtimes as needed for the computer systems in the case of a main power failure.

All Server Room equipment should be connected to a UPS system to provided regulated and backup power.

Access to the Server Room must be restricted to designated Server administrator individual staff.

The Unit staff responsible for physical security of the Server Room must be notified of the expected presence and provided with the details of all work to be carried out by any maintenance staff or external contractors at least 2 business days in advance of the commencement of the work. Any maintenance staff or external contractors requiring access to the Server Room must have their access logged in the P.W.5 Facility Maintenance Log Worksheet or equivalent, and they cannot be left unaccompanied by Unit staff in the Server Room.

18. Additional requirements for High Risk Situation Server Rooms

Where the room or area is classified as being in a High Risk Situation and is at Security Level 4 it must have the following additional protection:

Windows to external elevations should be fitted with security shutters or bars instead of locks.

Any door in the external elevation and providing direct access to a High Risk Situation room should be provided with a security shutter where practical.
Considerations should be given to replacement of standard fire exit doors which cannot be secured in this fashion, and any other doors designated as fire escapes by the Fire code, with special purpose security fire exit doors and frames. It may be necessary to add Certified Security System Alarm System coverage to such fire exit doors.

19. Temperature and humidity monitoring for Server Room

Each Server Room must have temperature and humidity sensory equipment and the established procedures to follow in the case of a sensor alert. The sensors should have alert thresholds set to match the maximum and minimum operating temperatures (typically 34 to 82 degrees Fahrenheit) and humidity (typically 20% relative humidity to 65% relative humidity) designated for the Server Room. The monitoring equipment should be tested on an annual basis to verify it is operating as specified and configured. This testing includes verification that end to end transmission of alerts occurs correctly.

The environmental monitoring system must be able to transmit alerts when configured thresholds are exceeded to the Alarm Receiving Center, or to designated staff responsible for the physical security of the Server Room. These alerts and the response taken to them must be logged.

The alert procedures should segregate response by whether the alert is a warning or critical. Warning alerts indicate normal operating ranges are exceeded, but equipment is still operating within manufacturer environmental specifications. Critical alerts indicate variance from specifications is so large that damage to equipment is imminent, and requires its shutdown within a designated time frame. Some Server and equipment management systems may be configured to automatically initiate shutdown when critical alert thresholds are met. If equipment and/or a service outage is expected due to a critical alert and there is sufficient time, staff utilizing the equipment or service should be informed in advance of the outage. The alert procedures should address clearing alarms and resetting monitoring equipment.

c. Facility Access Vulnerability Assessment

After completing the Physical Security Level categorization for each room or area in the P.W.1.a Facilities Worksheet, any deficiencies with respect to the required or advisable actions as listed in P.1.b.III for each location should be recorded, for example in an additional column on the P.W.1.a Facilities Worksheet originated as an export from FPSA.

Each Unit should consider how it would replace damaged or lost equipment as part of its business continuity plan. The University of Illinois Property Insurance program is subject to a very high casualty loss deductible of $500,000 per occurrence. To address this relatively high uninsured loss a Unit might face, the University of Illinois’ Office of Risk Management administers a Computer Insurance Plan that can cover computers and other electronic equipment. This coverage is not automatic. A University Unit needs to contact UORM if they want to participate in the Plan:
P.G.1.2 Analyze Physical Attributes of Surroundings

The Unit should review the P.W.1.a Facilities Worksheet completed at P.1.c and determine if any locations require greater, or lesser, physical access controls to safeguard the equipment and data contained on each Workstation, data storage device or Server. Any changes in physical access controls or equipment location required in order to reduce risk associated with the physical location to a level acceptable by the Unit should be input to the DCS.2.4 Conduct Risk Assessment of Data procedure or guideline.

P.G.1.3 Access Control and Validation Procedures

Authorization for key issuance to rooms or areas, and return of keys by exiting or discharged staff, is administered by the University Locksmith and Unit staff through the UIC Facilities Management FMWeb Service Request System:

http://fmweb.fm.uic.edu:8888/famis/

The University Locksmith installs and maintains Lockinetics devices to restrict lock entry to the I-card numbers of authorized individuals. Lockinetics devices cost approximately $1000 to purchase and install.

Every Security Level 4 Server Room must have its access controlled by such a Lockinetics device. The Unit is responsible for requesting periodic downloads of Lockinetics lock activity and for review of those access logs to detect unauthorized access. The Unit is also responsible for periodic review of the current list of staff, and their permitted access time of day and day of week, on the authorization list for each Lockinetics device.

If the Unit utilizes a legacy pre-Lockinetics University Police monitored physical key-controlled and metal recording tape location identification access control and alarm system requiring telephone confirmation to the University Police of each alarm system activation and deactivation, the Unit must also periodically review the current list of staff on the authorization list for that device.

For both the pre-Lockinetics and Lockinetics devices, the Unit must have a procedure to remove discharged or exiting staff from the device access list. This procedure should be part of the staff exit/discharge procedure described in Procedure PER.P.6 Termination of Access.

P.G.1.4 Access to Software Programs

As part of a Unit’s risk assessment, it should determine whether, and if so – how, it should control access to the source code for software programs used to acquire, modify, or report High Risk, Sensitive Data Collections, or Sensitive Data.
Depending on the importance of the programs to the Unit’s University business processes, the Unit may need to institute a procedure for authorizing access to program code, backing up and recovering programs, and for verifying the integrity of program code. Periodic checks of code integrity are part of the vigilance needed to ensure unintended, accidental, or malicious changes to code or corruption of it has not occurred. In some units, the importance of code integrity may rise to the level that the program code is managed through a formal revision control system.

**P.G.1.5 Maintenance Records**

Repairs and modifications to the physical components of a facility that are related to its physical security must be documented in a [P.W.5 Facility Maintenance Log Worksheet](#).

**P.G.2 Responsibility for Implementation**

The Unit head or delegate is responsible for the overall implementation of this Physical Security Guideline.

The UISO is responsible for preparing the Unit’s Facility Security Plan, annually Analyzing Physical Attributes of Surroundings – or when there are significant changes to them, and periodically reviewing Maintenance Records.

The Unit head or delegate is responsible for implementing Access Control and Validation Procedures.

The head of the IT unit, with review by the UISO, is typically responsible establishing guidelines for Access to Software Programs.

**P.G.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
Placeholder for insertion of P.W.1.a page 1 of 1 into PDF version of this document
Placeholder for insertion of P.W.5 page 1 of 1 into PDF version of this document
DP.1P Data Backup Plan Procedure

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

DP.P.1.0 Data Backup Plan Procedure Purpose

This document describes a procedure designed to fulfill the requirements set in Policy DP.1 Data Backup Plan, of the UIC Information Technology Security Program.

The intent of that policy is to ensure that backups are reliably and regularly created, securely stored, and reliably able to be used for recovery.

DP.P.1.1 Data Backup Plan Procedure

a. Prep work:

1. Decide which of your computers have important data on them. Typically, this will include all file Servers you maintain, as well as the Workstations of key individuals in your Unit.

2. Determine how much data you will be backing up. Include all the data from all the sources you decided on in the first step.

3. Determine the sensitivity classifications of your data. Use the definitions given in the UIC Information Technology Security Policy DCS.1 Data Classifications. You may have different types of data according to these classifications. If you do, determine the size of each type of data.

4. Investigate different methods of backup. There might be a way to back up your data without doing it yourself. Talk to ACCC representatives, people in your college’s IT department, or other knowledgeable people.
5. If the best choice is to do it yourself, decide the medium on which you will back up your data. Typically, this is done onto magnetic tape, but there are other options depending on the amount and sensitivity of the data to be backed up. Keep in mind that most cloud storage/backup solutions are not permitted for Internal Data, Sensitive Data, Sensitive Data Collections, or High Risk Data.

6. Create your Data Backup Plan. It must include the following information:
   i. Which systems will be backed up
   ii. Schedule of backups – will they be run daily? Weekly? Yearly? What level of backup (full or incremental) will be run?
   iii. The media the backup system will use
   iv. The software the backup system will use to schedule and control media and backup events
   v. Security considerations
   vi. Location used to store the backups
   vii. Location and vendor used to store offsite backups, if necessary
   viii. Procedure for recovery of the backup data, written so that someone who is not IT-trained could understand and follow it.
   ix. If your Unit handles Protected Health Information (ePHI), your plan must also include a way to make an ad hoc backup of that information before the equipment it is stored on gets moved.

7. Purchase and install the equipment and/or services necessary to implement your plan.

b. Running Backups

1. Once all steps are in place to run backups, make sure that your plan is followed. Backups should be reliably, and as automatically as possible, run according to your planned schedule.

2. Your Data Backup Plan must be available at all times to all key personnel. The suggested way to do this is to put it in your Unit’s University of Illinois READY system at https://us.ready.kuali.org. See the UIC Information Technology Security Policy DP.2 Disaster Recovery Plan, for more information about University of Illinois READY.

c. Verifying Your Plan

1. Every so often (recommended 1-2 times a year), run a recovery drill. Verify that data backed up to your media can indeed be restored. For maximum rigor, have untrained personnel perform a recovery using just the information from your Data Backup Plan, to simulate all of your Unit’s IT personnel being unavailable during an emergency.
DP.P.1.2 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of the Data Backup Guideline. The head of the Unit’s IT department, with review by the UISO, is typically responsible for making sure that the data backup plan is implemented.

DP.P.1.3 Definitions

<table>
<thead>
<tr>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full backup</td>
<td>A backup of all data and configurations including metadata on a system as well as installed programs and the operating system.</td>
</tr>
<tr>
<td>Incremental backup</td>
<td>A backup of only files which have changed since the last full backup.</td>
</tr>
<tr>
<td>Offsite backup</td>
<td>Backup media physically stored elsewhere besides your Unit’s office area or data room.</td>
</tr>
</tbody>
</table>

DP.P.1.4 Resources


DP.P.1.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial composition</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

108 Full backup, Incremental backup, and offsite backup definitions are replicated in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
DP.G.1 Data Backup Plan Guideline

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

DP.G.1.0 Data Backup Plan Guideline Introduction

This document describes a guideline designed to fulfill the requirements set in UIC Information Technology Security Policy DP.1 Data Backup Plan.

The intent of that policy is to ensure that backups are reliably and regularly created, securely stored, and reliably able to be used for recovery.

The Data Backup Plan should align with the Unit’s disaster recovery plan (DR plan), business continuity plan (BCP), to meet objectives such as recovery time objective (RTO), recovery point objective (RPO), location of the plan and geographic separation of backups from production systems and data.

DP.G.1.1 Data Backup Plan Guideline Procedure

a. Prep work

1. In accordance with Policy DCS 2.3 Annually Classify Data, decide which of your computers have important data on them. Typically, this will include all file Servers you maintain as well as the Workstations of key individuals in your Unit

2. In accordance with Policy DCS 2.4 Conduct Risk Assessment, determine the sensitivity class of your data. Use the definitions given in Policy DCS.1 Data Classifications. You may have different types of data according to these classifications. If you do, determine the size of each type of data. It is allowable to treat lower-sensitivity data as data of higher sensitivity.
3. Decide which of your computers are running important applications. Include these systems into your backup plan.

4. If your computers store electronic protected health information (EPHI), you must also perform a Data Criticality Analysis. See Policy DP.6 Applications and Data Criticality Analysis, and Guideline DP.G.6 Applications and Data Criticality Analysis for information about this requirement.

5. Sizing and Methods:
   i. Investigate different methods of backup. There might be a way to back up your data without doing it yourself. ADSM is a service offered by ACCC. Talk to ACCC representatives, people in your Unit’s IT department, or other knowledgeable people.
   ii. Determine how much data you will be backing up. Include all the data from all the sources you decided on in 2.1a and 2.1c.

6. If the best choice is to do it yourself, decide the medium on which you will back up your data. Typically, this is done onto magnetic tape, but there are other options depending on the amount and sensitivity of the data to be backed up. Keep in mind that most cloud storage/backup solutions are not permitted for Internal Data, Sensitive Data, Sensitive Data Collections, or High Risk Data unless they have signed a business associate agreement (BAA) and the appropriate parties have accepted the risk involved. Consult with your UISO if you are interested in implementing a BAA for a cloud solution.

7. Create your Data Backup Plan to include the following information:
   i. Which systems will be backed up
   ii. How much data will be backed up based upon the results of your storage backup requirements as determined in 2.1d.
   iii. Identify the staff responsible in your Unit for data backup and recovery, including a secondary person in the event the primary person is unavailable in a disaster.
   iv. How much data can your Unit afford to lose (recovery point objective (RPO))? If your Unit’s answer is one week's worth, backups should be run AT LEAST weekly.
      1. Ensure your Unit is willing to accept the risk of loss of the recovery point objective you set and they have agreed this is acceptable loss or can regenerate the data in a timely way.
   v. Schedule of backups – When will backups be run? Will they be run during the day or night? How will backups impact the performance/operation of systems they are run on? How frequently should they be run? Daily? Weekly? Monthly? What level of backup (full or incremental) will be run?
   vi. The media the backup system will use, quantity needed, and expiration dates based on vendor recommendations.
   vii. The software the backup system will use to schedule and control media and backup events
   viii. Security considerations - Who has access to backup media? Does it need to be encrypted? Backup media storing High Risk Data must be encrypted if moved off-site.
   ix. Location used to store onsite backups
   x. Location and vendor used to store offsite backups, if necessary.
Procedure for recovery of the backup data, written so that someone who is not IT-trained could understand and follow it.

If your Unit handles Protected Health Information (ePHI), your plan must also include a way to make an ad hoc backup of that information before the equipment it is stored on gets moved.

Additional considerations:
Databases have special needs for backups. Consider investigating technologies such as snapshot capability for resiliency or temporarily halting database operations.

8. Purchase and install the equipment, media and/or services necessary to implement your plan.

b. Running Backups

1. Once all steps are in place to run backups, make sure that your plan is followed. Backups should be reliably run according to your planned schedule as automatically as possible.

2. Your Data Backup Plan must be available at all times to all key personnel. The suggested way to do this is to put it in your Unit’s University of Illinois Ready system at https://us.ready.kuali.org/uic/. See Policy DP.2 Disaster Recovery Plan, and Guideline DP.G.2 Disaster Recovery Plan Guideline, for more information about University of Illinois READY. It is recommended to periodically verify all personnel have appropriate access to the plan and consider printing and distributing copies of that plan to personnel to store offsite.

c. Verifying Your Plan

1. Periodically run a recovery drill. Verify that data backed up to your media can indeed be restored. For maximum rigor, have untrained personnel perform a recovery using just the information from your Data Backup Plan, to simulate all of your Unit’s IT personnel being unavailable during an emergency.

d. Sample Plan

<table>
<thead>
<tr>
<th>Action</th>
<th>Frequency</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Backups to tape</td>
<td>Weekly</td>
<td>Saturday night at 11 PM</td>
</tr>
<tr>
<td>Incremental Backups to disk</td>
<td>Nightly except for Saturday</td>
<td>11 PM</td>
</tr>
<tr>
<td>Full backup ship offsite</td>
<td>Every 2 weeks</td>
<td>Tuesday at 9 AM</td>
</tr>
<tr>
<td>Recovery Drill</td>
<td>Annually</td>
<td>Random weekend in November</td>
</tr>
</tbody>
</table>
Sample Process

**NB:** This is just a sample process. The process you develop to be appropriate for your Unit’s needs might be different.

1. Before going home on Friday, a system administrator verifies that a tape is ready to be written to for the full backup on Saturday night.

2. During the day on Monday, a system administrator verifies that the Saturday backup ran correctly. If it didn’t, he or she corrects the problem and either runs a backup manually or re-schedules a backup to run Monday night. Once a successful backup is run, the system administrator prepares the tape for Tuesday’s offsite shipment.

3. On Tuesday, a representative from the offsite storage facility arrives to collect the full backup tape, and brings back the backup tape from three weeks ago.

4. In October of every year, the UISO determines the date in November for the annual recovery drill. When that day arrives, the system administrators follow the procedures to restore the backups, but without impacting normal production operations.

**DP.G.1.2 Responsibility for Implementation**

The Unit head or delegate is responsible for the implementation of the Data Backup Guideline. The head of the IT unit, with review by the UISO, is typically responsible for making sure that the data backup plan is implemented.

**DP.G.1.3 Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full backup</td>
<td>A backup of all data and configurations including metadata on a system as well as installed programs and the operating system.</td>
</tr>
<tr>
<td>Incremental backup</td>
<td>A backup of only files which have changed since the last full backup.</td>
</tr>
<tr>
<td>Offsite backup</td>
<td>Backup media physically stored elsewhere besides your Unit’s office area or data room.</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective. The maximum tolerable period in which data might be lost from an IT service due to a major incident.</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective. The duration of time within which a University business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity.</td>
</tr>
</tbody>
</table>

---

109 Full backup, Incremental backup, Offsite backup, RPO and RTO definitions are replicated in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
**DP.G.1.4 Resources**

University of Illinois READY, authenticate in using Bluestem [https://us.ready.kuali.org/uic/](https://us.ready.kuali.org/uic/)

**DP.G.1.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial composition</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
**DP.G.2 Disaster Recovery Plan Guideline**

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Date of Last Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2014</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>

**DP.G.2.0 Disaster Recovery Plan Guideline Purpose**

This document describes a procedure designed to fulfill the requirements set in the UIC Information Technology Security Policy *DP.2 Disaster Recovery Plan*.

The intent of that policy is to ensure that disaster recovery plans are created, regularly updated, and reliably able to be used for recovery.

**DP.G.2.1 Disaster Recovery Plan Guideline**

**NB** – The terms “disaster recovery” and “business continuity” are often treated in the general IT community as synonymous. **They are not!!** Disaster Recovery specifically refers to actions related to *continuing information technology* service after a disaster; Business Continuity refers to *resuming all* facets of business as usual (as in regular practice to meet University business process needs) after a disaster. Disaster Recovery is a **subset** of Business Continuity.

- The standard tool in use at UIC for business continuity planning, including disaster recovery, is a Web-based tool called University of Illinois Ready, also known as UI Ready or Kuali Ready. The URL for Ready is [http://www.ready.uic.edu/university_of_illinois_ready/](http://www.ready.uic.edu/university_of_illinois_ready/). Kuali Ready requires training; go to the above website to determine the next scheduled training class.

- Some **key components** for disaster recovery are **not covered** in UI Ready. You will need:
1. An estimate of how much work your Unit can afford to lose in the event of a disaster. This is called a Recovery Point Objective (RPO)\(^{110}\) and is measured in units of time. Your RPO will determine how long your Unit can go between successful backups.

2. Estimates of how long your Unit’s various functions can afford to go without computing resources. This is called a Recovery Time Objective (RTO)\(^{111}\) and is also measured in units of time. There are widely varying levels of RTO criticality, ranging from less than a minute for clinical operations, to days for other time-dependent functions like billing, to a month or longer for nonessential operations.

3. A backup plan which describes regularly-scheduled backups done at least as often as your Unit’s RPO requires.

4. The hardware and software to implement your Unit’s backup plan.

5. Plans for what to do if your Unit’s data center is unavailable for different lengths of time, keeping in mind what your Unit’s RTOs are.

6. At least one contact at ACCC to help your Unit with coordination of network and as needed other Campus Information Technology Principals’ capabilities.

7. A list of which systems need to be up and in what order. This is closely tied with your Unit’s RTO.

c. Recovery Point Objective (RPO)

A recovery point is a point in time when a backup was performed. A recovery point objective (RPO) is the maximum amount of time your Unit can afford to lose data. In other words, it’s the amount of time between a disaster and the backup which happened just before it.

An RPO is the answer to the question “Once we recover from a disaster, how much data are we comfortable with re-entering or losing entirely?”

Your Unit’s optimal RPO depends a great deal on the criticality and change volume of the data you deal with. If your data doesn’t change very often, your RPO will be longer than in a Unit whose data changes constantly. Likewise, if your Unit’s data can be re-entered before any critical issues arise due to its disappearance, your RPO can be longer than someone whose data is more critical.

Typically, recovery points happen on a daily or weekly basis. It is possible to have the RPO be less, but backup solutions typically get more complex and more intrusive at RPOs less than 24 hours.

---

\(^{110}\) See RPO in “[UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions](#)"

\(^{111}\) See RTO in “[UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions](#)"
d. Recovery Time Objective (RTO)

A recovery time objective is the maximum amount of time data can be unavailable after a disaster before critical issues arise. In other words, it’s the longest you Unit can afford to take to restore its data from its last recovery point.

An RTO is the answer to the question “Once we have a disaster, what is the maximum amount of time we can take to bring our systems and data back online?”

Your Unit’s optimal RTO will depend on the criticality of its data, as well as the time a disaster might occur. A life-support system, for instance, has an RTO measures in seconds or minutes. A historical document archive might have an RTO of months. A database of graduating students has a shorter RTO in April than it has in November.

e. Coordinating with your Business Continuity planners

Don’t make your Unit’s DR plan in a vacuum. Work closely with the people who are in charge of your Unit’s Business Continuity plan.

f. Coordinating with other units like ACCC

Your Unit’s disaster recovery plan should note other units and services upon which its’ recovery plan depends. For example, if your Unit’s network access is most likely provided by ACCC and in the event of a disruption of network services in a disaster, the ACCC may need to be involved in the restoration of that service. The disaster recovery plan should include contact information for these units and thoughts on how service could be restored. Be sure to communicate to all these other units what your DR needs are, and work with them to ensure that your requirements are met.

If there are organizations outside the University who rely on your Unit’s services being available, such as business associates or grant agencies, you might have a legal or contractual obligation to let each entity know what your DR plans are. Check the contracts or agreements your Unit has with these organizations before assuming all aspects of your Unit are covered by the difficulty of surviving there.

g. Store your plan in UI Ready

Your plan is required to be accessible off-site. The best place to do this is in the UI Ready tool.

h. Keep Training Up-To-Date

If a person is given a responsibility in your DR plan, make sure that he or she is trained to be able to meet that responsibility.
DP.G.2.2 Responsibility for Implementation

The head or delegate is responsible for the implementation of the Disaster Recovery Plan. The head of the IT unit, with review by the UISO, is typically responsible for making sure that the IT System components of it are developed and tested periodically.

DP.G.2.4 Resources


DP.G.2.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial revision</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
**DP.G.3.0 Contingency Operations Plan Guideline Purpose**

This document describes a procedure designed to fulfill the requirements set in UIC Information Technology Security Policy [DP.3 Contingency Operations Plan](#).

The intent of that policy is to provide an overarching view so that Contingency Operations (defined as "the bare minimum services a Unit needs to operate its University core business processes")\(^{112}\) can be implemented on a Unit level.

This policy is **REQUIRED** for units which handle electronic protected health information (ePHI)\(^{113}\), and a Best practice for all other units.

**DP.G.3.1 Contingency Operations Plan Guideline Procedure**

**Coordinating With Campus Units**

If a Unit stores ePHI on its systems, Policy [DP.3 Contingency Operations Procedures](#) requires the Unit to develop and communicate with other campus units plans to ensure that it can access its systems and data in order to perform data restoration tasks.

The Unit must make sure that it has communicated and planned with the following groups:

---

\(^{112}\) See “Contingency Operations” in [“UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”](#)

\(^{113}\) See “ePHI” in [“UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”](#)
UIC Information Technology Security Program Procedures, Standards, Guidelines and Worksheets ver 1.0

a. Facilities Management, including Locksmith  
b. ACCC (for network access and core services)  
c. External vendors  
d. UIC Police  
e. Any other departments which the Unit relies upon for disaster recovery.

DP.G.3.3 Responsibility for Implementation

The Unit head or delegate is responsible for the implementation of this Contingency Operations Plan Guideline. The head of the Unit’s IT department, with review by the UISO, is typically responsible for making sure that the IT System components of it are developed and tested periodically.

DP.G.3.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial revision</td>
<td>June 10, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DP.G.4 Emergency Mode Operation Plan Guideline

Effective Date | Date of Last Revision
--- | ---
July 1, 2014 | July 1, 2014

DP.G.4.0 Emergency Mode Operation Plan Guideline Purpose

This document describes guidelines designed to assist your Unit in fulfilling the requirements set forth in UIC Information Technology Security.

Emergency Mode Operations ("EMO") refers to the period of time after Policy DP.4 Emergency Mode Operation Plan a disaster from when recovery activities start until the resumption of normal operations (i.e. the emergency is over and all systems and functions have been restored).

Policy DP.4 Emergency Mode Operation Plan, on which this guideline is based, is required for units which handle electronic protected health information (ePHI)\(^{114}\), and is Best Practice for all other units.

DP.G.4.1 Emergency Mode Operation Plan Guideline

The Unit’s Emergency Mode Operation (EMO) plan will be closely linked with its Disaster Recovery/Business Continuity plan.

a. As part of the risk analysis process described in Policy DCS.2.4 Conduct Risk Assessment of Data, the Unit will determine which services it provides are critical business functions. Using this information, the EMO plan must ensure that these services have priority for restoration.

b. In addition, a critical portion of the Unit’s EMO plan must address how the security of the restored services will be safeguarded while running in the degraded service environment.

---

\(^{114}\) See ePHI in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
In other words, it is recognized that while running in EMO it is possible that all the normal security functions may not be available, but the EMO plan must address what controls will be used to ensure the security of the data in place of the missing controls.

c. Coordinate with Other Campus Units

If the Unit has ePHI on its systems, Policy DP.4 Emergency Mode Operation Plan requires it to incorporate in this EMO plan’s communications with other campus units to ensure that the Unit can access its systems and data in order to perform data restoration tasks. Make sure that the Unit has communicated its requirements, and created its EMO Plan, including the following groups:

1. Facilities Management, including Locksmith
2. ACCC (for network access and core services)
3. External vendors
4. UIC Police
5. Any other departments which the Unit relies upon for disaster recovery.

d. Coordinate With Organizations External to Campus

Other organizations or individuals might need to be key players in a Unit’s EMO plan. The UISO will have to use their best judgment here. If the Unit utilizes an outside service to store offsite backups, for instance, then the Unit will have to coordinate with them to make sure that it can use the outside service in a reliable manner during an emergency.

Likewise, any organization that relies on a Unit’s services will need to know what to expect from the Unit in the event that the Unit enters its EMO.

e. Establish Procedures

The University of Illinois Ready tool (also called Kuali Ready; see DP.G.2 Disaster Recovery Plan Guideline) has definitions for different criticalities of University business processes. It is just as important to keep a Unit’s ePHI secure when in Emergency Mode as it is when it is in its normal operating mode.

Once a Unit knows what its Critical 1, 2, and 3 systems\(^{115}\) are, it needs to make a plan to ensure the ePHI on those systems is secure while they are being operated or accessed in EMO.

---

\(^{115}\) See Critical 1, 2, and 3 in “UIC IT Security Program Policies, Procedures, Standards, Forms and Guidelines Definitions”
f. Train Personnel

Everyone who will be responsible for ePHI in EMO needs to be trained on their duties in case an EMO situation arises.

g. Document the Emergency Mode Operations Plan

The University of Illinois Ready tool is, once again, the best place to store a Unit’s EMO documentation. Even if the Unit’s plan is not stored on University of Illinois Ready, it should have the following sections:

1. Service Level Agreements and contact information for vendors
2. Service Level Agreements and contact information for other campus groups, like ACCC, which the Unit depends on
3. Offsite work facilities
4. Facilities Management - especially Locksmiths if the Unit has a locked data area
5. UIC Police contacts and phone numbers

h. Test the Emergency Mode Operations Plan

The Emergency Mode Operations Plan must be tested on a periodic basis.

**DP.G.4.2 Responsibility for Implementation**

The Unit head or delegate is responsible for the implementation of the Emergency Mode Operation Guideline. The head of the IT unit, with review by the UISO, is typically responsible for making sure that the IT System components of it are developed and tested periodically.

**DP.G.4.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial revision</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
DP.G.5.0 Testing and Revision Guideline Purpose

This document describes a guideline designed to help fulfill the requirements set in UIC Information Technology Security Program Policy DP.5 Testing and Revision Procedure.

The intent of that policy is to ensure that the plans created to meet Policies DP.1 Data Backup Plan, and DP.2 Disaster Recovery Plan, and, as appropriate, DP.4 Emergency Mode Operation Plan, are tested periodically. As the old saying goes, “no plan survives contact with the enemy.” In Disaster Planning projects, the enemy is an actual disaster. The more you test your plan ahead of time, the more likely you will be able to predict and handle the unknown events of an actual disaster if and when it occurs.

DP.G.5.1 Testing and Revision Guideline Procedure

a. Prep work

Before a Unit can fulfill the requirements of this Guideline, the plans required by the preceding DP.G.1 Data Backup Plan Guideline, DP.G.2 Disaster Recovery Plan Guideline, and DP.G.3 Contingency Operations Plan Guideline must be completed. Additionally, if the Unit is required to implement an Emergency Mode Operation plan, it must complete the DP.G.4 Emergency Mode Operation Guideline.
b. **DP.5 In a Nutshell**

The keys to fulfilling the requirements to this Guideline are 1) training the people in the Unit in their roles and responsibilities during a disaster, and 2) periodically testing the Unit’s Disaster Recovery Plan.

c. **Training The People In The Unit**

1. In creating the three Plans, the specific roles required to successfully meet the requirements of the Program should have been identified, and these roles should have been assigned to key individuals within the Unit. Those people now need to be trained. Training includes, but is not limited to:

   A. Attending classes or otherwise learning how to operate the various hardware devices and software programs the Plans utilize.

   B. Becoming familiar with the personnel in other departments the Unit is dependent on, and which are dependent on the Unit.

   C. Walking through the procedures outlined in the Unit’s plans.

d. **Testing the Disaster Recovery Plan**

1. While developing and updating the disaster recovery plans is a good first step, it is by no means an adequate enough precautionary measure if there is no testing after the plan is agreed upon. Testing is what indicates the effectiveness of a plan, so it is important that as much care be exercised in testing the plan as in developing it. Time has a way of eroding a plan’s effectiveness since a Unit’s environment will change and Unit key personnel will likely forget parts of the plan.

2. A yearly tabletop exercise in Business Continuity is typically arranged by UIC’s Business Continuity department. If the Unit used UIC Ready to create its Disaster Recovery plan, the Unit’s participation in this exercise should be sufficient to meet this Guideline requirement to test the Disaster Recovery Plan.

3. If a Unit wants to put together its own test, there are many ways of going about it. Some common testing scenarios are:

   i. **Structured Walk-Through Testing**

      During a structured walk-through test, disaster recovery team members meet to verbally walk through the specific steps of each component of the disaster recovery process as documented in the disaster recovery plan. The purpose of the structured walk-through test is to confirm the effectiveness of the plan and
to identify gaps, bottlenecks or other weaknesses in the plan.

ii. Checklist Testing

A checklist test determines if the proper materials are stored offsite, telephone number listings are current, and a copy of the recovery plan and necessary operational manuals are available. Under this testing technique, the recovery team reviews the plan and identifies key components that should be current and available. The checklist test ensures that the organization complies with the requirements of the disaster recovery plan.

A combination of the checklist test and the structured walk-through test is suggested for initial testing to determine modifications to the plan before attempting more extensive testing.

iii. Simulation Testing

During this test, the organization simulates a disaster so normal operations will not be interrupted. A disaster scenario should take into consideration the purpose of the test, objectives, type of test, timing, scheduling, duration, test participants, assignments, constraints, assumptions, and test steps. Testing can include the notification procedures, temporary operating procedures, and backup and recovery operations. During a simulation, the following elements should be thoroughly tested: hardware, software, personnel, data and voice communications, procedures, supplies and forms, documentation, transportation, utilities (power, air conditioning, heating, ventilation), and alternative site processing. It may not be practical or economically feasible to perform certain tasks during a simulated test (e.g., extensive travel, moving equipment, eliminating voice or data communication).

If the Unit decides to carry out a simulation test, it needs to set its scope so that it is neither too small nor too large. “A network cable gets unplugged somewhere” is too small; “a meteor obliterates all of Chicago” is too large. The typical scope of a UIC Ready business continuity test is “both sides of campus become uninhabitable for a week to a month, but the rest of Chicago is unaffected.” Also, make the scenario realistic. “A fire hits one campus building and spreads to three others” is realistic; “a computer virus eats all the copper wiring in the University’s network” is not.

iv. Parallel Testing

A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as yesterday’s transactions, are processed against the preceding day’s backup files at the contingency processing site or hot-site. All reports produced at the alternate site for the current business date should agree with those reports produced at
v. **Full-interruption Testing**

A full-interruption test activates the total disaster recovery plan. This test is costly and could disrupt normal operations. Therefore, it should be approached with caution.

The Unit will need to schedule adequate time for this testing. Initially, the Unit should not schedule the test at critical points in the normal processing cycle, such as the end of the month. The duration of the test should be predetermined to measure adequate response time.

Various test scenarios could be planned to identify the type of disaster, the extent of damage, recovery capability, staffing and equipment availability, backup resource availability, and time/duration of the test. The test plan should identify the persons responsible and the time they need to perform each activity. However, only part of the plan should be tested initially. This approach identifies the workability of each part before attempting a full test. Also, it may be best at first to test the plan after normal business hours or on weekends to minimize disruptions.

Eventually, unannounced tests can be performed to emphasize preparedness.

e. **Testing the Data Backup and Emergency Mode Operations Plans**

The tests for these plans should be similar to the examples of the different tests given above.

f. **Revisions**

As business functions and their supporting IT systems change, the respective plans should be revised and tested. Upon successful completion of the testing, the relevant plan(s) should be updated.

**DP.G.5.2 Responsibility for Implementation**

The Unit head is responsible for ensuring that the proper testing, and training of the involved staff members, has been completed for the relevant plan(s). The head of the IT unit, with review by the UISO, is typically responsible for making sure that IT systems related disaster recovery testing is performed periodically, and that as system modifications occur timely updates are made to the relevant plan(s).
DP.G.5.4 Guidance


DP.G.5.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial revision</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
<tr>
<td></td>
<td>Program Committee</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DP.G.6.0 Applications and Data Criticality Analysis Purpose

This document describes a guideline designed to fulfill the requirements set in UIC Information Technology Security Program Policy DP.6 Applications and Data Criticality Analysis.

The intent of that policy is to ensure that the system, application, and data access interdependencies of the plans created to meet Policies DP.1 Data Backup Plan, DP.2 Disaster Recovery Plan, and DP.3 Contingency Operations Plan are correctly defined. Additionally, Policy DP.6 Applications and Data Criticality Analysis is utilized to ensure that if so required, the DP.4 Emergency Mode Operation Plan meets the special requirements which the Health Insurance Portability and Accounting Act (HIPAA) places on systems which store electronic personal health information (EPHI).

The HIPAA Security Standard lists an applications and data criticality analysis as an addressable implementation specification. That means that a Unit doesn’t have to perform a criticality analysis if it can prove that it’s not reasonable or appropriate for the Unit. But experts agree that just about every organization needs to conduct a criticality analysis to identify what’s most critical to its operations. You don’t want to have to decide what software and data are most important to your organization after a disaster strikes. Performing a criticality analysis now will tell a Unit what to restore first so its Workforce can remain calm and immediately start to bring the Unit’s most critical systems online.
DP.G.6.1 Applications and Data Criticality Analysis Procedure

a. Prep work

1. Get Staff Input

Meet with department heads, or their representatives, and ask them about the applications and data their department uses. Meet also with the IT staff to find out what computer systems support those applications and data—those are the systems which must be brought up first if a disaster or emergency occurs.

2. Track Input With Forms

A typical Data Criticality Analysis form should have at least the following fields:

   i. Applications
   ii. Type of data that application uses
   iii. The function of that application on that data
   iv. The IT systems which support that application/data/function
   v. The consequences of disruption
   vi. Workarounds if that application/data/function became unavailable
   vii. The recovery time objective, or RTO\(^\text{116}\) (for more information on RTOs, see the DP.G.2 Disaster Recovery Plan Guideline)

An excellent sample of a form can be found on the HC Pro’s web site, at http://www.hcpro.com/content/42684.pdf, page 3.

b. Determine Criticality Level

Once the Unit has received input from all the core business functions its IT department supports or depends upon, the Unit can go through the input and decide the order in which systems should be brought online or reconnected to in the case of a disaster.

\(^{116}\) See RTO in “ITGC Policies, Procedures, Standards, Forms and Guidelines Definitions”
**DP.G.6.2 Responsibility for Implementation**

The head of the IT unit, with review by the UISO, is responsible for making sure that input is collected and a thorough applications and data criticality analysis is performed.

**DP.G.6.4 Resources**


**DP.G.6.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Doug McCarthy</td>
<td>Initial revision</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
PER.P Personnel Procedure

PER.P.0 Personnel Procedure Purpose

This document describes a procedure designed to fulfill the requirements set in UIC Information Technology Security Program Policy PER, Personnel.

PER.P.1 Identify Access Needs of All Users

Units must create procedures to determine access needs using the following guidelines:

a. Create an inventory of applications, systems, and data repositories housing High Risk Data or Sensitive Data Collections.

b. Create procedures for requesting access that include supervisory and data owner approval.

PER.P.2 Job Descriptions, Responsibilities, and Training

Units must:

a. Create Unit procedures in line with current University security training to assure that staff accessing data are trained on policies and procedures related to securing that data.

b. Create plan to audit access lists on an, at minimum, annual basis.
PER.P.4 Access Establishment and Modification

Units must create Unit procedures that assure that any staff with altered job duties are reviewed prior to their shift in responsibility. This review should assure that access is still current and approved by the appropriate body in the same fashion as new access is granted.

PER.P.5 Access Authorization

Units must:

a. As stated in Procedure PER.1, users accessing High Risk Data or Sensitive Data must be approved by their supervisor and the owner of the data.

b. The procedure for granting access must include a provision for retaining documentation of this access.

PER.P.6 Termination of Access

Units must create a procedure by which access to all University systems, data and applications is terminated upon termination of engagement with the University.

PER.P.7 Responsibility for Implementation

The Unit’s business units, HR, IT staff and UISO are responsible for the coordinated implementation of these personnel procedures.

PER.P.8 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Jason Maslanka</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
PM.P Policy Maintenance Procedure Purpose

This Procedure implements a structured representative framework for Information Systems Security Policy Planning within UIC. This planning provides the foundation for good information systems security practices within Units of the University and their constituent business units. This Procedure shall establish an orderly process for bringing proposals for addition, modification, or deletion to the UIC Information Technology Security Program to attention of the body charged by the UIC Information Technology Governance Committee’s Infrastructure and Security Subcommittee (InfraSec) with maintaining that Program, the UIC Information Technology Security Program Committee.

PM.P.1 Program Component creation and maintenance

The UIC Information Technology Security Program Committee shall create and maintain the UIC Information Technology Security Program’s Policies, Procedures, Standards, Forms, Guidelines and Definitions (“Program Components”) needed to establish and execute the Program. These Program Components aim to be complete, accurately stated, and generally agreed upon by relevant parties prior to submission via the Information Technology Governance Committee to the Provost for approval.

When a Program Component no longer serves the intended or a useful purpose it shall be modified or removed by the P&P Committee. The UIC Information Technology Security Program Committee must consider the full effects of a proposed, modified, or removed Program Component on University activities both at present and in the future when the component comes to it for review.
a. Program Component proposals from the Campus Community

The participants in the UIC Information Technology Security Program are defined at the Security Program Overview, SPO.7 Roles and Responsibilities, and consist of the ITGC Infrastructure and Security Committee, its UIC Information Technology Security Committee, the Campus Chief Information Officer, the Campus Information Security and Privacy Officer, Unit Heads, Unit Information Security Officers, and the Campus Community. A member of the Campus Community may propose additions of or to, modifications to, or removal of Program Components to the UIC Information Technology Security Program Committee after first presenting their Proposal to their UISO for review. If their submission is approved by their UISO, then the proposal may be submitted to the UIC Information Technology Security Program Committee.

b. Necessary considerations for Program Component submissions

1. A proposal for additions, modifications, or removal of Program Components ("Program Component Proposal") should include relevant supporting detail to support Program Component Proposal review by the UIC Information Technology Security Program Committee.

2. The Program Component Proposal, where appropriate, shall include an explicit discussion of financial implications to Business Units to comply with the Proposal, and also the financial implications to Business Units if the proposal is not addressed.

3. Organizational units most obviously affected by the Program Component Proposal shall be consulted if they are not represented by the UIC Information Technology Security Program Committee.

4. The UIC Information Technology Security Program Committee shall consult with the necessary University Counsel or University Combined Covered Entity HIPAA Privacy or Security Officer whenever regulatory or compliance issues are addressed.

c. Program Component Proposal Review and Approval Process

1. All Program Component Proposals shall be reviewed on a periodic basis by the UIC Information Technology Security Program Committee or subcommittee it establishes. Proposals may be rejected, returned to the originator with comment, or advanced by the UIC Information Technology Security Program Committee to Interim Draft status. Any Proposal advanced to Interim Draft status will be conformed to contain the Standard Sections per Procedure section PM.P.1.d below.
2. The UIC Information Technology Security Program Committee shall establish a review and comment interval for an Interim Draft status Program Component Proposal and place it in the Review and Comment Process.

3. In the Review and Comment Process, the Proposal shall be distributed by the UIC Information Technology Security Program Committee to any staff whom they believe should participate in the review and comment process, and also be distributed to the campus and be placed upon a website accessible for comment via the established policycomment@uic.edu email account.

4. At the conclusion of the review and comment interval, the UIC Information Technology Security Program Committee shall consider, but not necessarily act upon, any comments in the Comment Repository before deciding whether to reject, revise, or accept the Program Component Proposal.

5. If the UIC Information Technology Security Program Committee accepts the Program Component Proposal, it will advance it to Final Draft status, establish a review and comment interval, and place the Proposal in the same Review and Comment Process as in (PM.P.1.c.3) above.

6. At the conclusion of the Final Draft status interval, the UIC Information Technology Security Program Committee shall consider comments as in (PM.P.1.c.3) above and then determine whether to return the Proposal to Interim Draft status or to present the Proposal to Infrasec to be reviewed and considered for forwarding to the Provost for review and approval.

d. Standard Policy, Procedure, Guideline, and Standards Sections

All UIC Information Technology Security Policies:

1. Shall have an implementation date defined by the UIC Information Technology Security Program Committee and included on the Policy when it is submitted as a Proposal to the Provost for review and approval.


3. All UIC Information Technology Security Program Procedures, Guidelines, Standards, and Worksheet documents shall be named as the corresponding Policy section, and with a P, G, S, or W appended to the source Policy Section alphabetical portion of the name to form the Procedure, Guideline, Standard, or Worksheet name (e.g. Policy DP.1 becomes Procedure DP.P.1, Guideline DP.G.1, and Standard DP.S.1). The documents shall have the following sections:
i. The document shall contain as its section 0 an explicit statement of its Purpose and need. In some instances, this may not be necessary for a Standard.

ii. The document shall contain as its section 1 a statement of the terms of the procedure or process necessary to execute it including the area of information technology where the procedure operates, how the procedure operates, the affected systems and staff, and the technical and / or operational requirements of the procedure. Whenever a procedure assigns more than one specific responsibility and/or task then each should appear as a separate subsection

iii. The document shall contain as its section 2 a definition of the role(s) assigned Responsibility for Implementation.

iv. If the document introduces any new terms requiring definitions, they shall be specified in its section 3, Definitions, and also be added to UIC Information Technology Security Program Policies, Procedures, Standards, Worksheets and Guidelines Definitions document.

v. If good guidance or further information is available from external sources or references, section 4 of the document, Resources, shall be added.

vi. The Revision History of the document shall be tabulated in its Section 5, listing the author(s) of the document, a Description of the changes made, a Submission Date for the draft to the UIC Information Technology Security Program Committee, and the Approval Date of the new version of the Procedure.

vii. The document in general does not need to specify a Violations consequence. Where particularly necessary, such consequences can be defined in section 9, Violations, of the document, otherwise, the overlying applicable Policy Violation terms will apply. The standard terms of Policy Violation given at RC.3 Sanctions for non-Compliance are:

*Any individual found to have violated this policy may be subject to disciplinary action up to and including termination of employment.*

viii. Each document shall have an anticipated implementation date defined by the UIC Information Technology Security Program Committee and included at the top of the document when it is submitted as a Proposal to the Provost for review and approval.
4. UIC Information Technology Security Program Worksheets (Forms) do not have standard sections, but shall cite the referring Policy, Procedure, Form, Guideline, or Standard.

e. Standard Hierarchy of Subsection Numbering

1. As already directed in this Procedure 1.4.a for Policy and 1.4.b for Procedures, Guidelines, and Standards, each discrete required action, specification or assigned responsibility shall appear as a separate section or subsection. The reason for this requirement is that it facilitates Program requirements analysis.

2. The hierarchy for numbering subsections is:

   a. b. c. ...

   1. 2. 3. ...

   i. ii. iii. ...

   A. B. C. ...

   I. II. III. ...

f. Unit Policy Maintenance Guideline

An annual review of all Unit created Program Policies, Procedures, Guidelines, Standards, and Worksheets (“Components”) by the Unit’s UISO is required. The PM.G Unit Policy Maintenance Guideline describes the process for that review.

g. Annual Review

All UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines (“Program Components”) shall be reviewed on an annual basis by the UIC Information Technology Security Program Committee in order to determine that they still meet the overall Program Purpose and Goals, and the specific Program Component Purpose and Goals. The review work may be subdivided as the UIC Information Technology Security Program Committee determines best meets its resources. The review shall consider any external statutory or regulatory changes, or University policy, procedure or guidelines changes, impacting the Program Component. The annual review also needs to consider the burden and necessity of any Program Exceptions granted in the review period, and whether or not those Exceptions require revision of the underlying Program Component.

PM.P.5 Revision History
<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Initial document</td>
<td>November 7, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
PM.G.0 Unit Policy Maintenance Guideline Purpose

This Procedure implements a structured framework, representative of Unit stakeholders, for Unit created components of the UIC Information Technology Security Program.

The UIC Information Systems Security Program is designed to establish oversight of that Program’s work as it is distributed through the University’s organizational structure to subordinate Units to ensure sufficient Information Systems Security activities are planned, done, and reviewed to reasonably reduce risk to the University from adverse events potentially affecting the availability, integrity and confidentiality of University data, and of the reputation of the University.

This planning and oversight provides the foundation for good information systems security practices within Units of the University and their constituent business units. Within that, this particular Procedure shall establish an orderly process for bringing proposals for additions, modifications, or deletions to Unit created components of the UIC Information Technology Security Program to its UISO.

PM.G.1 Creating and Maintaining the Information Security Program

An annual review of all Unit created Program Policies, Procedures, Guidelines, Standards, and Forms (“Components”) by the Unit’s UISO is required.

a. UIC IT Security Program Procedure PM.P.1.a, Program Component proposals from the Campus Community, allows Unit members to submit requests for additions to, modifications to, or removal of Program Policies, Procedures, Guidelines, or Standards to their UISO for review. If the proposal is approved by the UISO, it may be submitted to the UIC IT Security Program Committee.
b. The UISO should develop a Procedure defining any necessary considerations for Program Component Proposal submissions, and a review and approval process.

c. The Unit created Components shall follow the Procedure PM.P.1.d, Standard Policy, Procedure, Guideline, and Standards Sections requirements and PM.P.1.e Standard Hierarchy of Subsection Numbering.

PM.G.3 Responsibility for Implementation

The UISO is responsible for ensuring the Unit created Components are created and maintained.

PM.G.6 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>UIC IT Security Program Committee</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
RC.S.0 Reporting and Compliance Standards Purpose

The following individual standards list minimum specifications that must be maintained to be in compliance with the Reporting and Compliance Policy and Guideline.

**RC.S.1.1 Audit Control and Review Plan**
The RC.1 Policy, [Audit Control and Review Plan](#), lists the specifications of this Plan which each Unit must develop.

At a later date, standard plans for generic function Servers may be defined and documented here. At this version of the Standard, there are no specifications to give here for the Plan.

**RC.S.1.2 Develop and Implement the Information Systems Activity process**

As of this version of the Standard, the ACCC CISPO Office has not yet specified what must be logged for each data type and OS type.

Each Unit must review the logs specified under their Audit Control and Review Plan weekly. A centrally administered tool provided by the ACCC will allow each Unit to define customizable alerts based on common parameters such as particular types of activity and threshold settings such as number of occurrences within a particular time interval. The alerts generated by the tool must be actionable and be sent to the appropriate personnel.

**RC.S.1.4 Common Incident Response and Reporting System**

The ACCC RT-IR instance must be used to handle incident reporting.
RC.S.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Mike Kirda</td>
<td>Initial composition</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
**RC.G.0 Reporting and Compliance Guidelines Purpose**

As stated in [SPO.4 UIC IT Security Program Goals](#), reporting and auditing are used to validate compliance with the UIC Information Security Technology Program.

**RC.G.1.1 Audit Control and Review plan**

The Risk Management Plan called out in UIC Information Technology Security Policy [DCS 2.5 Implement Risk Management Program](#), is a prerequisite for this section. To put it simply, the Unit needs to look at the machines and applications running in its environment, decide what must be logged for each, ensure that the data is captured, define how often it will be reviewed and by whom. The UISO must make sure that the above is done.

The UISO of each Unit is responsible for developing the Unit’s own operational procedures for this section.

**RC.G.1.2 Develop and Implement the Information Systems Activity process**

The Standard [RC.S.1.2 Develop and Implement the Information Systems Activity process](#) section lists what must be logged for each data type.

The Unit must put in place a system to review the logs regularly. The UISO must ensure compliance with the [RC.S.1.2 Develop and Implement the Information Systems Activity Process](#) Standards.

The UISO of each Unit is responsible for developing the Unit’s own operational procedures for this section.

**RC.G.1.3 Sanctions for non-Compliance**
All workforce members must follow the UIC Information Technology Security program. This is specifically called out at Policy SPO.2 Mandatory Adoption and Compliance. Furthermore, Policy RC.3 Sanctions for non-Compliance states, in part:

Any individual found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

The CISO is responsible for developing its any operational procedures beyond what is called for in Policy RC.3 Sanctions for non-Compliance for this section. A Unit may optionally develop its own sanctions procedures for specific types of incidents.

**RC.G.1.4 Common Incident Response and Reporting System**

Units must utilize the RT System provided by ACCC to report IT Security incidents.

**RC.G.1.5 Reporting and Responding to IT Security Incidents**

Workstation, or account, breach or compromise occurs when there is unauthorized access to it. Workforce members believing a Workstation or account has been or might be compromised must notify their UISO. The UISO must follow the RC.P.5 Reporting and Responding to IT Security Incidents Procedure workflow to ensure that the incident is reported and investigated promptly and properly. It is highly recommended that the IT staff of each Unit have a dedicated machine available for forensic imaging. The RC.P.5 Procedure recommends that this forensic imaging system have a current version of FTK Imager installed, a hard drive dock preferably with cooling should be connected to it, and secure file storage space should be provided to hold forensic images generated. The file storage space could be on an external hard drive, a dedicated internal hard drive, or secure space on a file Server.

**RC.G.1.6 Unit Information Security Officer Annual Report**

The UISO is responsible for compiling and sending a UISO Annual Report forward to their Unit Head, the IT Governance Council and the Provost. Depending upon the Unit organization, the UISO may tap others within their Unit to help gather the required data for the report. The main purpose of the UISO Annual Report is to help evaluate the effectiveness of the IT Security program. This section of the Guideline will be updated within the first year of the implementation of the Program with a list of the reportable items for the UISO Annual Report. The UISO of each Unit is responsible for developing the Unit’s own operational procedures for obtaining the information needed for this section.

**RC.G.1.7 Retention of the UISO Annual report**

The Unit must retain copies of their UISO Annual report in accordance with the UIC Records Management Program.
RC.G.2 Responsibility for Implementation

In coordination with their Unit IT staff, data custodians, and data stewards, the UISO of each Unit is responsible for developing the Unit’s own operational procedures for its RC.G.1.1 Audit Control and Review Plan, RC.G.1.2 Develop and Implement the Information Systems Activity Process, RC.G.1.3 Sanctions for non-Compliance, and also preparing and retaining the RC.6 Unit Information Security Officer Annual Report Policy.

The UISO utilizes the RC.G.1.4 Common Incident Response and Reporting System to carry out RC.G.1.5 Reporting and Responding to IT Security Incidents, and directs any Unit IT staff who utilize it.

RC.G.5 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Source</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Mike Kirda</td>
<td>Initial document</td>
<td>Jan. 23, 2013</td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
RC.P.5 Reporting and Responding to IT Security Incidents Procedure

RC.P.5.0 Reporting and Responding to IT Security Incidents Procedure: Purpose

This procedure has been created to ensure that all IT Security Incidents are handled in a uniform, coherent and efficient manner, best reducing potential damage to University Information Assets, University data, University business processes, and the University's reputation.

UIC Information Technology Security Program Policy RC.5 Reporting and Responding to IT Security Incidents, requires that “Any IT Security Incident, defined as “an activity which may act as a threat to detrimentally affect or has affected the confidentiality, integrity, or availability of University data”, involving High Risk Data or Sensitive Data Collections must be reported and responded to by following Procedure RC.P.5, IT Security Incident Response and Reporting”.

IT Security Incidents affecting other classes of University data (Internal Data, Public Data, or Sensitive Data) should broadly be responded to as in the following RC.P.5.1.b.1 for loss or theft of a device, RC.P.5.1.b.2 for breach of a Workstation, RC.P.5.1.b.3 for breach of a Server, or RC.P.5.1.b.4 for any other type of IT Security Incident, but without any requirement to report outside the affected Data Custodian, Data Steward, or UISO.

A compromised or breached system is a University Information Asset which has been affected by an IT Security Incident such that unauthorized changes to its configuration, programs, or data has caused it

---

117 See Breach definition in “UIC Information Technology Security Policies, Procedures, Standards, Forms and Guidelines Definitions”
or the data accessed by or stored on it to become insecure. An insecure system no longer can be guaranteed to meet intended University confidentiality, integrity, or availability needs and Standards. Units must ensure that all relevant IT personnel in the Unit that may be called upon to respond to security incidents are made aware of this Procedure, and that they understand its contents before an incident occurs. Having a dedicated forensic analysis system with the proper tools installed and ready ahead of time is highly recommended.

**RC.P.5.1 Reporting and Responding to IT Security Incidents: Procedure**

a. The Unit must establish procedures for the Campus Community including the Unit’s Workforce to contact them in the case of an IT Security Incident, train their Workforce in those procedures, and notify non-Workforce Campus Community members of those procedures.

b. Types of Incidents

Although each incident may be unique, they can be segregated into the four broad categories:

1) Loss or theft of a University Information Asset\(^{118}\) including a Workstation or data storage device (such as Portable Data Storage Devices) : see **RC.P.5.1.1 Case scenario: Loss or theft of University Information Asset (including Workstations, Portable Data Storage Devices, and Laptops)**

2) Breached Workstation or Portable Data Storage Device : see **RC.P.5.1.2 Case scenario: Breached Workstation or Portable Data Storage Device (including Laptop)**

3) Breached High Risk Data or a Sensitive Data Collection stored on a Server : see **RC.P.5.1.3 Case scenario: Breached High Risk Data or a Sensitive Data Collection stored on a Server**

4) Other type of IT Security Incident : see **RC.P.5.1.4 Case scenario: Other type of IT Security Incident**

Other incidents may occur that do not neatly fit into one of these categories. If, after reading this document, you have questions regarding whether a specific incident needs to be reported, please contact the UIC Chief Information Security and Privacy Officer at cispo@uic.edu

**RC.P.5.1.1 Case scenario: Loss or theft of University Information Asset (including Workstations, Portable Data Storage Devices, and Laptops)**

a. Notification

\(^{118}\) See University Information Asset definition in “UIC Information Technology Security Policies, Procedures, Standards, Forms and Guidelines Definitions”
User must notify:

1. Police
   i. Theft Occurs Off-campus
      A. The local police must be contacted and a police report number must be obtained
      B. The UIC police (312-996-2830) must also be contacted. They will want a copy of the above mentioned police report number in addition to other details related to the lost/stolen University Information Asset
   ii. Theft Occurs On-campus
      A. The UIC police (312-996-2830) must be contacted.

2. Data Steward
3. Department/Unit Head
4. Department/Unit IT staff via normal channels
5. OBFS also has a procedure that must be followed: [http://www.obfs.uillinois.edu/equipment-management/unlocatable-stolen-equipment/](http://www.obfs.uillinois.edu/equipment-management/unlocatable-stolen-equipment/)

b. Decision and action by staff specified in Unit IT Security Incident Reporting Procedure:
Was the lost or stolen Workstation used in a research protocol?

   1. If YES: The IRB must be notified by submitting a PROMPT report [http://tigger.uic.edu/depts/ovcr/research/protocolreview/irb/forms/](http://tigger.uic.edu/depts/ovcr/research/protocolreview/irb/forms/) then continue at c. below
   2. If NO, continue at c. below

c. Determine encryption status:

   Decision and action by staff specified in Unit IT Security Incident Reporting Procedure:
   Was the lost or stolen University Information Asset ENCRYPTED using a DCS.S.4 Data Encryption Storage Standard approved encryption solution, and is the encryption key secure?

   1. If YES: (the device was ENCRYPTED and is the encryption key secure)

      The Unit must verify that the Asset was encrypted when the IT Security Incident occurred, and that the security of the encryption key has not been compromised. If both are true, the encryption has rendered the data unreadable to unauthorized parties as they do not possess the encryption key to decrypt the data.

---

119 See encryption in “UIC Information Technology Security Policies, Procedures, Standards, Forms and Guidelines Definitions”
The incident must be reported to the CISPO office’s RT-IR queue via email to secincident@uic.edu with the primary information that the system was lost or stolen (give the specifics), the type and nature of any High Risk Data (including whether or not ePHI was present) or Sensitive Data Collection stored on the system, and the basis for asserting the Workstation was ENCRYPTED and that the security of the encryption key has not been compromised.

2. If NO (the University Information Asset was not ENCRYPTED, or the security of the encryption keys was compromised):

   **Decision:** Did the device contain High Risk Data or Sensitive Data Collections?

   i. If YES:

   A. **Decision:** Did the device contain ePHI?

   If YES, (the device was UNENCRIPTED or the security of the encryption keys was compromised, and it contained ePHI):

   The incident must be reported to the CISPO office’s RT-IR queue via email to secincident@uic.edu with the primary information that the system was lost or stolen (give the specifics), the type and nature of any High Risk Data (including that of any ePHI present) or Sensitive Data Collection stored on the system.

   The CISPO Office may then require additional action by the Unit to respond to and resolve the incident. The CISPO Office will liaison with the Combined Covered Entity’s HIPAA Security and/or HIPAA Privacy Officer as needed.

   B. If NO (the device was UNENCRIPTED or the security of the encryption keys was compromised, it did not contain ePHI, but it did contain High Risk Data or a Sensitive Data Collection):

   The incident must be reported to the CISPO office’s RT-IR queue via email to secincident@uic.edu with the primary information that the system was lost or stolen (give the specifics), the type and nature of any High Risk Data or Sensitive Data Collection stored on the system.

   The CISPO Office may then require additional action by the Unit to respond to and resolve the incident.

   ii. If NO (the device was UNENCRIPTED or the security of the encryption keys was compromised, but it did not contain any High Risk Data or a Sensitive Data Collection):
No exposure of High Risk Data or Sensitive Data Collections occurred. The incident must be reported to the CISPO office’s RT-IR queue via email to secincident@uic.edu with the primary information that the system was lost or stolen (give the specifics), and the basis for asserting no High Risk Data or Sensitive Data Collection was present on the Workstation.
RC.P.5.1.2 Case scenario: Breached Workstation or Portable Data Storage Device (including Laptop)

a. Notification

The Unit Workforce member must notify their Unit IT Staff via their Unit’s RC.P.5.1a IT Security Incident Reporting Procedure.

b. Decision and action by staff specified in Unit IT Security Incident Reporting Procedure: Was the breached device used in a research protocol?

   a. If YES: The IRB must be notified by submitting a PROMPT report http://tigger.uic.edu/depts/ovcr/research/protocolreview/irb/forms/
      then continue at c. below

   b. If NO, continue at c. below

c. Determine classification of data on Asset

   Decision and actions by staff specified in Unit IT Security Incident Reporting Procedure: Does the Workstation/portable data storage device contain High Risk Data or Sensitive Data Collections?

   1. If NO:
      i. To reuse the Workstation,
         A. Get data off drive or Workstation.
         B. Wipe drive with low-level format techniques, i.e. Drive eraser tool
         C. Re-image the drive using a known good backup copy (or reinstall the operating system from the original media).
         D. Restore the end-user’s data from the backup copy made in step A. above.
         E. Give Workstation back to user with their data.

      ii. Otherwise, to give the user a NEW Workstation,
         F. Replace hardware
         G. Restore data from backups, if available
         H. Exit this Procedure

   2. If YES, the Workstation does contain High Risk Data or Sensitive Data Collections, and assuming the Workstation is still powered on:
i. Grab a screenshot if possible.

ii. Grab a list of running processes using pslist:
   
   A. Pslist \computername >c:somedir\file.txt
   
   B. Pslist –d \computername >c:somedir\file-details.txt
   
   C. Run FTK Imager Lite. FTK Imager Lite can be run off of a thumb drive
   and can hold a memory dump. Run it from a temporary admin
account that doesn’t share passwords with any other account.  (FTK
Imager Lite can be downloaded from AccessData:
http://www.accessdata.com/support/product-downloads)
   Alternatively, utilize a similar imaging utility.

iii. Turn off the Workstation

iv. Remove the hard drive from the Workstation.

v. Use a hardware-based write blocker (such as the Tableau TS35es) to create
a hard drive image using a current version of FTK Imager. It is highly
suggested to use a hard drive cooler during the image creation period. After
creation, the image must be stored in a secure manner such as on the sFTP
Server, a file Server with access tightly controlled via AD groups or via
external hard drive stored in locked safe.

vi. Export the file hash list from FTK Imager, storing them in a secure manner as
in v. above. The generated hashes can be used later on to verify the
integrity of the image.

vii. Use FTK Imager to mount the image as evidence to export user's files. (Add
Evidence Item under File). Note: Image files appear to be read-only via FTK
Imager.

viii. **Decision and action by staff specified in Unit IT Security Incident Reporting
Procedure:** Did the breached device contain ePHI?

   A. If YES:

      The incident must be reported to the CISPO office’s RT-IR queue via
email to secincident@uic.edu with the primary information that
the system was breached (give the specifics), the type and nature
of any High Risk Data (including that of any ePHI present) or Sensitive Data Collection stored on the system.

The CISPO Office may then require additional action by the Unit to respond to and resolve the incident. The CISPO Office will liaison with the Combined Covered Entity’s HIPAA Security and/or HIPAA Privacy Officer as needed.

Further include in the report all of the items under B. below:

B. If NO, **Report incident via RT-IR queue:** Email a report to secincident@uic.edu including the following information for the CISPO Office:

   A. Unit name
   B. Primary and secondary contact name(s), NetID(s), Work and Cell telephone numbers
   C. Data Custodian name and NetID
   D. Date and time IT Security Incident:
      I. detected,
      II. reported,
      III. and responded to
   E. Hard drive capacity and interface type
   F. Procedure used to image hard drive, size and number of hard drive image(s) obtained
   G. MAC Address and IP address
   H. Machine Name in Active Directory if applicable
      I. OS version/SP version
   J. AntiVirus software used
   K. Installed software, if available
   L. Screen shot, if available
   M. Process list via pslist or Process Explorer
   N.Verbose description of problem including how it was detected and symptoms
   O. If virus, suspected type
   P. Logs from Virus console
   Q. Event logs if available
R. Nature and extent of High Risk Data or Sensitive Data Collections, if known
S. Was this data involved in a research protocol authorized by the IRB?
T. Proposed arrangements, if any, by Unit to transfer device and memory images to CISPO Office. If none are provided, the CISPO Office will initiate the dialog as needed.

ix. Contact Unit Head, or their Designate for IT Security Incidents in the Unit, and inform them a Workstation or portable data storage device containing High Risk Data or Sensitive Data Collections has been involved in an IT Security Incident, and that the Incident is being investigated and remediated per UIC IT Security Policy. Inform them of all parties contacted under this Procedure so far, and of the substance of the contact.

x. Get the user back up and running. The boot partition on the drive must be wiped completely via low level format before system restore or reinstall in case of virus or rootkit infection. Any non-boot partitions or drives on the system must be scanned for any malware infection and if detected have that remediated.

xi. The CISPO Office must inspect the information at their disposal and decide within 72 hours:

**Decision and actions by CISPO Office:** Send to forensics?

A. If No, CISPO Office:
   I. Closes IT Security Incident report ticket
   II. Sends short report sent to Unit Head, CCing UISO, which explains the extent and likely impact of the IT Security Incident, and also the reason for the decision not to send the device for forensic examination.

B. If YES:
   I. Send hard drive to external company for forensic examination and initial report of the examination within a 24 to 72 hour timeframe

   II. Identify University Liaison with external company (the Liaison will likely be the CISPO Office, or staff in the Unit) to coordinate transfer of custody of hard drive from Unit to company, and distribution by the Liaison of any reports from external company
III. Liaison to create ticket with company and let Unit know where/how to send the hard drive to the company

IV. Liaison to get report(s) and disseminate as appropriate. Forensic report distribution to include the Head of affected Unit

V. **Decision and actions by CISPO Office:** Was a breach of confidentiality identified on the basis of the forensics examination?

a. If NO:
   1. CISPO Office identifies threat resulting in IT Security Incident (infection or compromise vector) and works with Unit to tighten security policies to mitigate the threat
   2. CISPO Office issues final report to Unit Head and higher level administration at the University (Provost, or most likely their delegate)
   3. Ticket closed out

b. If YES:
   1. The CISPO Office notifies the Data Steward to authorize their Data Custodian to be prepared to provide pre- and post-breach copies of files identified as breached from the previously acquired drive image to parties identified by the CISPO Office. (The post-breach copies have been acquired at step RC.P.5.1.2.b.2.v above, the drive imaging step.)
   2. The CISPO Office is available to assist the Unit in identifying the type and extent of data breached.
   3. CISPO Office must follow notification procedures if so specified by regulation based on type of data involved in the breach (e.g. HIPAA/FERPA/PIPA regulations, et al.)
4. After incident is remediated, CISPO Office issues final report to Unit Head and higher level administration at the University (Provost, or most likely their delegate)

5. Ticket closed out
RC.P.5.1.3 Case scenario: Breached High Risk Data or a Sensitive Data Collection stored on a Server

This section of the procedure has not been published yet.

Contact the CISPO Office by emailing a report of the case to secincident@uic.edu and direction will be provided for the procedure to follow in the instance of a breach of confidentiality of High Risk Data or a Sensitive Data Collection stored on a Server.

RC.P.5.1.4 Case scenario: Other type of IT Security Incident

This section of the procedure has not been published yet. Contact the CISPO Office by emailing a report of the case to secincident@uic.edu and direction will be provided for the procedure to follow in the instance of an IT Security Incident not falling into the first three categories.

RC.P.5.1.5 Public/Regulatory Notification

a. In any IT Security Incident the Unit in which the incident occurs is responsible for all associated response and remediation costs required by the CISPO, including:
   1. those for any forensic examination initiated under RC.P.5.1.1 through RC.P.5.1.4,
   2. the costs of notification (including notification required by regulation) of affected individuals or entities, and
   3. the costs of remediating the breach following all recommendations of the forensics analysis remediation recommendations, as further revised by the CISPO.

b. The CISPO Office will provide the Notification Procedure which must be followed when an IT Security Incident requires notification, and will identify the party which will initiate the notification and respond to the notification.

RC.P.5.2 Responsibility for Implementation

The Unit head or delegate is responsible for the Unit’s implementation of this Procedure.

The UISO is responsible for ensuring the Unit establishes RC.P.5.1.a contact procedures, that the Unit’s SA.G.1 Security Training Program includes training the Unit Workforce on the IT Security Incident reporting procedure established by the Unit, and that non-Workforce Campus Community members are notified of the Unit IT Security Incident reporting procedure as is appropriate for the type of University data they access.

The UISO is responsible for advising and directing any Campus Community member in correctly reporting a possible or actual IT Security Incident according to this Procedure.
With the advice and consent of the Data Steward and Data Custodian involved, the UISO is responsible for directing any Unit Workforce assigned by the UISO to respond to an IT Security Incident in their Unit.

The CISPO Office has further designated responsibilities in certain circumstances under RC.P.5.1.1 through RC.P.5.1.4.

**RC.P.5.5 Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Creator</th>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Mike Kirda</td>
<td>Initial document</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>UIC CIO, UIC CISPO, UIC IT Security Program Committee</td>
<td>UIC IT Security Program enacted effective 7/1/14</td>
<td>July 1, 2014</td>
</tr>
</tbody>
</table>
Section 9 Index

Placeholder for bookmark for end of Index section, to be replaced by last word of Index. This bookmark must be preserved otherwise the preceding Section page numbering will be thrown off
Section 10 : Back Sheet

Placeholder for bookmark for end of Back sheet section. This bookmark must be preserved otherwise the preceding Section page numbering will be thrown off
Section 11: Post-Back Sheet

Placeholder for bookmark for end of Back sheet section. This bookmark must be preserved otherwise the preceding Section page numbering will be thrown off.