| UIC UNIVERSITY OF ILLINOIS AT CHICAGO | **DCS.G.1 Data Classification and Security Guideline** | |
|---|---|---|
| | **Effective Date** | **Date of Last Revision** |
| | **July 1, 2014** | **July 1, 2014** |

## 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 Data48. In addition, this Program also defines a Sensitive Data Collection1, which is a stored aggregate of Sensitive Data.

[48] 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)[49] 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.

[49] 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.

| Data Items | High Risk Data | Sensitive Data | Internal Data | Public Data |
|---|---|---|---|---|
| SSN (including parent's and donor's) | X | | | |
| Protected health information (PHI) | X | | | |
| Employee choice of wellness programs | | X | | |
| Education records | | X | | |
| Responses to faculty survey | | X | | |
| Driver's license number | | X | | |
| State identification card number | | X | | |

| Data Items | High Risk Data | Sensitive Data | Internal Data | Public Data |
|---|---|---|---|---|
| University Identification Number (UIN) | | | | X |
| Credit or debit card numbers | X | | | |
| Credit or debit card numbers security code | X | | | |
| Credit or debit card numbers password that permits access to account | X | | | |
| Bank account number | | X | | |
| Academic record | | X | | |
| Certificates/license numbers | | X | | |
| Customer account information (i.e. payments, transactions or collections) | | X | | |
| Student loan agreements, loan balances, transactions, collection | | X | | |
| Employee counseling | | X | | |
| Health of employee | | X | | |
| Applicant interview results | | X | | |
| Employee benefit claim information | | X | | |
| Benefit enrollments, beneficiaries, workers comp/disabilities/family status change | | X | | |
| Employee retirement information | | X | | |
| Payroll deduction selections, registers, direct deposit, payroll reports, tax forms | | X | | |
| Tax ID number | | | X | |
| Donor personal information, credit cards, bank accounts, employment, family info, amount donated, medical history | X | | | |
| Procurement Card numbers (P-Card) | X | | | |

| Data Items | High Risk Data | Sensitive Data | Internal Data | Public Data |
|---|---|---|---|---|
| Source files, license keys and installation documentation | | X | | |
| Student Date of birth (if student wants private) | | | X | |
| Ethnicity | | | X | |
| Employee gender | | | X | |
| Religion | | | X | |
| Disability (physical, sight, or hearing) | | | X | |
| Marital status | | | X | |
| Color or race | | | X | |
| Information on when/where people used building access cards | | | X | |
| Point of sale transactions | | | X | |
| ID cards | | | X | |
| Student cardholder accounts | | | X | |
| Information gathered on prospective applicant | | | X | |
| Convictions | | | X | |
| Resume | | | X | |
| Parent's financial records | | | X | |
| Veteran status | | | X | |
| Scholarship information | | | X | |
| Email communications on confidential matters | | | X | |
| Telephone number/fax number (could be public if part of student directory) | | | X | |
| University Course Catalog | | | | X |

| Data Items | High Risk Data | Sensitive Data | Internal Data | Public Data |
|---|---|---|---|---|
| General web site information | | | | X |
| Information on classes, totals, demographics | | | | X |
| General counseling services offered | | | | X |
| General wellness program offerings | | | | X |
| Public job openings, duties, qualifications | | | | X |
| General pay range for position opening | | | | X |
| Employee recruiting program | | | | X |
| General employee benefits offered | | | | X |
| Payroll cycle/periods | | | | X |
| General payroll deduction offerings | | | | X |
| Student Directory information (unless student wants private) | | | | X |
| Employee compensation (can be found in gray book) | | | | X |
| Email address (unless student invokes student confidentiality) | | | | X |
| Age (unless student invokes student confidentiality) | | | | X |
| Date and place of birth (unless student invokes student confidentiality) | | | | X |
| Photographs (unless student invokes student confidentiality) | | | | X |
| Student (unless student invokes student confidentiality) | | | | X |
| Campus maps | | | | X |

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**[50] are given above in section DCS.G.1.0, *Introduction*.

## DCS.G.1.5 Revision History

| Version | Source | Description | Approval Date |
|---|---|---|---|
| 0.1 | Ed Zawacki | Initial document | Dec. 18, 2012 |
| 1.0 | UIC CIO, UIC CISPO, UIC IT Security Program Committee | UIC IT Security Program enacted effective 7/1/14 | July 1, 2014 |

[50] Data steward, Data custodian and Data user definitions are replicated in "UIC Information Technology Security Policies, Procedures, Standards, Worksheets and Guidelines Definitions"