Protecting Personal and Confidential Data at UIS

Introduction

Of all the various asset types that the University of Illinois at Springfield controls and maintains, data is one of the most valuable. The University and its employees are constantly in the process of gathering, 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 UIS 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 negative financial impacts, potential legal ramifications, and damage to the University's public reputation.

As is in the case 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 determine classification levels for the data, and then to proceed with the actual classification of all of our valuable data assets. The objective of this document is to provide a body of information, resources, and guidance that can assist employees in addressing the following questions regarding classifying data:

- Need: Why is it necessary to classify data?
- Roles: Who should classify what data?
- Methods: How should data be classified?

Why Is This Important to Me? Why Now?

As is the case at other University of Illinois campuses, the Springfield campus is responsible to ensure its information assets are protected in a fashion that conforms with legal requirements and other industry best practices. As a public Illinois university, UIS data collection activities fall within the scope of several federal, state and University regulations that require that data be classified and to have processes in

place to ensure its protection[1]. **This year, campus administration has made it a priority to determine what the current level of protection is for the data in use on our campus, to determine what areas of risk may exist, and to implement a plan to address those risks.** This document is the first step in proceeding down the path of assuring that the information assets in use on the UIS campus are being properly protected.

This document is primarily an educational tool, one intended to provide UIS employees with a better understanding of what information is considered protected and how it should be handled, so that collectively we can ensure protected data is being kept safe from misuse and other potential harm. In the sections that follow, we will explain what the different classifications protected information can fall into, who or what determines those classifications, and provide some examples of how certain types of data are classified. We will also touch on the recommended guidelines that should be followed when working with protected data, based upon the data's classification. Finally, we'll look at what steps are still to come to ensure that UIS is providing adequate protection of its information assets.

Roles and Responsibilities

It is common for people to assume that since IT manages the systems, they also own the data. But this is incorrect; IT is not responsible for the function that uses the data. 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 have direct operational-level responsibility for information management – usually department 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.

Data custodians are those people 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. The campus IT department obviously plays in important part in serving as a data custodian, but there may be other individuals or groups on campus who serve in this role as well.

Data users are individuals who need and use 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 sensitive data have a position of special 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're 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

[1] see Appendix 1 – Sample Regulations, Standards, and Policies

transferred via e-mail). As data users, UIS employees and third-party contractors are obligated to handle all data appropriate to the data classification.

Data Classification Definitions

For the purposes of ensuring the proper protection of the University's data, and in coordination with other campus departments and University of Illinois IT information security bodies[2], the UIS campus information security group has developed that following four classification groups for the various information data types:

- **Highly Sensitive**: Information that if disclosed or modified without authorization would have a 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:
  - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure (for example, credit card information, which is covered by PCI-DSS)
  - Information covered by federal and state legislation (for example, health information covered by HIPAA regulations)
  - Payroll, personnel, and financial information with special privacy requirements

- **Sensitive**: 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 (NDA's), and other intellectual property are, as a minimum, in this class.

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

- **Internal**: 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.

- **Public**: 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.

[2] The content of this data classification document was coordinated with the input and guidance of the University Technology Management Team – Information Security Committee (UTMT-Security). More information on the makeup and purpose of this committee can be found here: http://www.utmt.uillinois.edu/information_security_committee_overview/.

Data Classification Guidelines

Certain data is sometimes referred to as personally identifiable information (PII). Examples of personally identifiable information are 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. This information may be used to steal a person's identity in which case it must be treated as Sensitive or Highly Sensitive data.

Certain data is sometimes referred to as directory information in which case it may be treated as Public data. Examples of directory information is information that is contained in an educational record of a student that is generally available from published sources such as a telephone directory and is normally not 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 or Highly Sensitive class. Yet the same name data may be considered directory information in when used in that capacity, 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 provide 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 UIS along with typical classifications.

Data Items	Highly Sensitive	Sensitive	Internal	Public
SSN (including parent's and donor's)	X			
Protected health information	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		
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,	X			

family info, amount donated, medical history				
Procurement Card numbers (P-Card)	X			
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
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

Note: Unless specifically designated otherwise, data should, at minimum, be considered as being classified as Internal.

Guidelines for Handling Protected Data

Once protected data has been identified and classified, it needs to be handled in a manner appropriate to its sensitivity level. Proper handling of some data types are governed by specific laws and regulations. University *High Sensitive* or *Sensitive* data is protected specifically by federal or state laws or University rules and regulations[3]. Based upon the requirements of these laws, regulations, rules, standards and other policies, appropriate security measures must exist to keep the data secure. **These security requirements extend beyond the systems owned and controlled by the University directly; non-University systems that use, store, or otherwise process protected data must still abide by University data security standards.**

The table below lists the data handling guidelines for the UIS campus. These guidelines have been developed in concert with the guidelines being used in other University of Illinois units.

Classification Type	Handling Guidelines
Public	• There are no special requirements for the handling of Public data.

[3] see Appendix 1 – Sample Regulations, Standards, and Policies

Internal	• All personnel with access to protected data should be trained in the appropriate handling of said data. • Internal data should not be shared without the explicit permission of the applicable data steward. • A current inventory should be maintained which lists which users have access to Internal data assets. This includes power users (such as developers) and system administrators who could escalate their privileges in such a fashion as to grant them access to Internal data assets. The inventory list should be reviewed at least annually by each unit to verify that only authorized users are allowed access to the data. • All systems (including servers, desktops, notebooks, and portable computing devices) that store Internal data should be protected by system firewalls configured to ensure the minimum access levels needed to perform the business duties. • Backups of Internal data should be stored and managed with the same restrictions as the original data.
Sensitive	Requirements for handling Sensitive data include all of the requirements for handling Internal data, plus the following requirements: • Systems used for the storage and management of Sensitive data should be professionally managed. • Sensitive data should not be accessed from non-campus IP addresses unless access is through an on-campus VPN service. • Sensitive data should not be stored on unencrypted removable media such as CDs, DVDs, and USB keys. • All transport of Sensitive data to off-campus IP addresses should be encrypted. • Sensitive data should not be stored with a third-party service that does not have a contractual relationship with the University of Illinois. • Authentication and authorization for access to Sensitive data should be performed using a central authentication and authorization service (such as Active Directory), or a more secure authentication method. • Peer to peer software may not be used on systems used to store or access Sensitive data. • Keys or access badges for rooms or file cabinets containing Sensitive data should not be left in areas accessible to unauthorized personnel. • All units should maintain a list of users with keys, access badges, or tokens that allow access to Sensitive data, as well as all users with maintenance privileges/responsibilities to keys, access badges, and tokens. • Paper documents that contain Sensitive data should be stored in a locked drawer and in a locked room, or in another secure location approved by the appropriate data steward. • All personnel with access to Sensitive data should be trained in the appropriate handling of said data. • Sensitive data should not be stored on a server that is also used to host a web site open to the public without authentication. • Systems that store Sensitive data should have a vulnerability scan performed before being placed into production. Thereafter, periodic

	vulnerability scans should be performed on at least a quarterly basis. • Sensitive data stored in paper form should be securely destroyed when disposed of. This destruction should be accomplished via use of a crosscut shredder or an authorized document disposal service. • Systems and/or paper that stores Sensitive data should not be physically moved from an approved secure location without prior approval of the appropriate data steward. • An audit trail should be maintained for all access to Sensitive Data, and this audit trail should be maintained for at least 1 year. • Any suspected or confirmed security breaches of systems that store or access Sensitive Data should be reported immediately to the campus ISO (e-mail InfoSec@uis.edu or call 217-206-7355).
Highly Sensitive	• Requirements for handling Highly Sensitive data include all of the requirements for handling Sensitive data, plus the following requirements: • If Highly Sensitive data is stored within a database, it should be stored in an encrypted format. • Access control for Highly Sensitive data should use two-factor authentication. An SSL certificate or SSH key will be considered an acceptable substitute for a physical token or ID card. • Highly Sensitive data should not be sent or stored using email under any circumstances. Highly Sensitive data received via email should be transferred to an acceptable storage mechanism as soon as possible and immediately deleted from the applicable email account.

Roadmap

It is necessary for the UIS campus to verify that the information assets we are all entrusted with are being adequately protected from harm. Not only is this our intrinsic responsibility, it is also a minimum requirement that University auditors rightfully require we (the collective UIS community) validate is being done properly and consistently.

Towards that end, the campus Information Security Officer will soon be requesting feedback from each campus department about what types of protected data they deal with and how it is being used, stored and protected. This feedback will come in the form of responses to an information security survey derived from each campus department head (or their designee). Once the feedback has been received, a consolidated inventory of data types in use on our campus will be developed. Once the inventory process has been completed, the ISO will assist data stewards to determine if their data is being adequately protected and, if needed, help provide relevant employee educational opportunities regarding protected data as well as facilitate implementation of any additional controls or other security solutions that may be deemed necessary. The final objective of this process is to ensure all protected data types in use on the UIS campus are being secured appropriately and consistently.

All of these efforts are part of the larger, comprehensive information security plan being established for the UIS campus. This information security plan will ensure that all aspects of protecting our information

assets area being addressed and periodically reviewed and updated. In that vein, you should expect to see ongoing risk assessment reviews with corresponding updates to the information security policies, processes, standards, and guidelines to accommodate the ever-changing risk landscape.

Summary

Information is, in many ways, the lifeblood of the work performed at UIS. The protection of that information is the responsibility of everyone who interacts with it. Some data types require higher levels of protection than other data, but all of the data is valuable. If the any of the data becomes damaged, unreliable or otherwise unusable, the damaging effect to the University can be severe. It is incumbent on our community that we ensure these valuable assets are properly secured from harm, both accidental and intentional. To that end, we all need to be willing to become more knowledgeable about securing the data we work with every day and to be diligent in ensuring it is used, stored and transmitted appropriately.

Appendix 1 – Sample Regulations, Standards, and Policies

Here is a sampling of some of the pertinent regulations, policies, and standards that govern or influence how protected data is used, stored and transmitted:

Federal and State

- Health Insurance Portability and Accountability Act Privacy Rule (HIPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Personal Information Privacy Act (PIPA)
- Equal Employment Opportunity (EEO)

University of Illinois

- Section 19:5 of University of Illinois Business and Financial Policies Manual
- University of Illinois Information Technology Policies
- University of Illinois Social Security Number Policy (SSN)
- Section 19:2 of University of Illinois Business and Financial Policies Manual

Industry Standards

- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27000 series standards

Data Export Controls

The handling of export controlled information is not specifically addressed in this data classification guideline document. However, it is important to be aware that certain information may fall within the scope of data export laws. For this reason, please be aware of the following:

> The transfer of export-controlled information or software source code to a foreign national (someone who is not a U.S. citizen or green card holder) is deemed to be an export to the person's home country. Depending upon which export restrictions apply, a deemed export license may be required.

For more information about dealing with information covered by export control laws, please contact the campus Information Security Officer at InfoSec@uis.edu or call 217-206-7355.