DEPAUW UNIVERSITY
DATA CLASSIFICATION POLICY AND HANDLING RECOMMENDATIONS
(05-01-2016)

I. PURPOSE

The purpose of this policy is to define a framework for classifying and handling Institutional Data based on its level of sensitivity, value and criticality to the University.

Data classification, in the context of information security, is the classification of data based on its impact to the University should that data be disclosed, altered or destroyed without authorization. Classification of data helps determine what baseline security controls are appropriate for safeguarding that data.

II. SCOPE

This Policy applies to all employees and third-party Agents of the University as well as any other University affiliates who access, process, or store Institutional Data.

III. ACKNOWLEDGEMENTS

This policy was borrowed from resources referenced in the **EDUCAUSE Information Security Guide: Effective Practices and Solutions for Higher Education** (http://www.educause.edu/library/resources/information-security-guide-effective-practices-and-solutions-higher-education), including http://www.cmu.edu/iso/governance/guidelines/data-classification.html and http://security.mtu.edu/policies-procedures/DataClassificationAndHandlingPolicy.pdf.

IV. INSTITUTIONAL DATA CLASSIFICATION LEVELS

Institutional Data is any data related to the business of the University including, but not limited to, financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the department level as well as centrally, regardless of the media or system on which they reside. In the case of data in digital format, Institutional Data includes records that are stored in on-premise University data systems as well as systems provided by means of Internet-hosted service providers (i.e., "Cloud" hosted systems or applications).

All Institutional Data is classified into one of three classifications: Restricted, Private, or Public.

A. Restricted Data

Data should be classified as *Restricted* when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data.

Confidential Data / *Sensitive Data* are generalized terms that typically represent data classified as Restricted, according to the data classification scheme defined in this Guideline. These terms are often used interchangeably.

B. Private Data

Data should be classified as *Private* when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

C. Public Data

Data should be classified as *Public* when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Non-public Information is defined as any information that is classified as Private or Restricted Information according to the data classification scheme defined in this Guideline.

Data Collections

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address and social security number, the data collection should be classified as Restricted even though the student's name and address may be considered Public information.

V. Classification of Institutional Data

Classification Process

Classification of Institutional Data	
Institutional Data Type	**Specific Data Governor(s)**
Student records	Office of the Registrar, Office of Student Life, Office of Financial Aid
Student Health records	Office of Student Life, Student Disability Services Coordinator, Office of Health Services
Employee records (including faculty members, staff members, affiliates, retirees, and applicants)	Office of Human Resources, Office of Academic Affairs
Prospective Student records	Office of Admission and Financial Aid, Student Disability Services Coordinator
Alumni and other persons included in Advancement records	Office of Development and Alumni Engagement
Financial and Business records	Office of Business and Finance
Academic Intellectual Property (including faculty and student work)	Academic Affairs, Office of the Registrar
Academic and Course records (including course assessments, learning management system content and tracking, etc.)	Academic Affairs
University Website (www.depauw.edu)	Office of Communications
Institutional Research and Survey data	Office of Institutional Research
Library records	Library

Table 1

Classification of Institutional Data (See Table 1) is performed by an appropriate University *Data Steward* in cooperation with Information Services and related *Data Governors*.

A *Data Governor* is the relevant office that is responsible for the accuracy, integrity, and timeliness of certain data, and that has authority to grant or deny permission to access to that data.

A *Data Steward* is a senior-level employee of the University assigned by the relevant Data Governor to oversee the lifecycle of one or more sets of Institutional Data.

On a regular basis, the Data Steward should evaluate the classification of Institutional Data to ensure the assigned classification is appropriate based on changes to legal and contractual obligations or changes in the use of the data or its value to the University. Conducting an evaluation on at least an annual basis is encouraged.

If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

In general, University Institutional Data is managed according to protocols defined by the following offices (See Table 2):

Management of University Information	
University Information	**Managing Office**
Students	Office of the Registrar or the Office of Student Life
Faculty members	Office of Academic Affairs
Staff members, affiliates, and retirees	Office of Human Resources
Parents of current students	Office of Student Life
Prospective students and parents	Office of Admission and Financial Aid
Alumni and other persons included in Advancement records	Office of Development and Alumni Engagement
Financial and Business records	Office of Business and Finance

Table 2

VI. RUBRICS FOR CLASSIFICATION

In some cases, appropriate data classification is guided by state or federal laws that require the University to protect certain types of data (e.g., personally identifiable information such as a social security number or FERPA-protected student education records). In other cases, Data Stewards will consider each security objective using Table 3 as a guide.

As the total potential impact to the University increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the Office of the CIO for assistance.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 3*

*The table is an excerpt from Federal Information Processing Standards ("FIPS") publication 199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf) published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

VII. Predefined Types of Restricted Data

The University has defined several types of Restricted Data based on state and federal regulatory requirements. These are defined as follows:

1. Authentication Verifier

An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to:

- Passwords
- Shared secrets
- Cryptographic private keys

2. Personally Identifiable Information ("PII")

For the purpose of meeting security breach notification requirements, PII is defined as a person's Social Security number or their first name or first initial and last name in combination with one or more of the following data elements:

- Social Security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical/health information

3. Personally Identifiable Education Records – Covered under FERPA

Personally Identifiable Education Records are defined as any Education Records that contain one or more of the following personal identifiers:

- Student number
- Grades, GPA, credits enrolled
- Social Security Number
- A list of personal characteristics or any other information that would make the student's identity easily traceable

Note: The University classifies directory information that is generally considered to be public information as Public. See DePauw's Student Records Policy (FERPA) (http://www.depauw.edu/academics/academic-resources/advising/registrar/ferpa-notification) for more information on this directory information and on what constitutes an Education Record.

4. Payment Card Information

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

5. Federal Tax Information ("FTI")

Federal Tax Information (FTI) is defined as any return, return information or taxpayer return information that is entrusted to the University by the Internal Revenue Services. See "Internal Revenue Service Publication 1075: Tax Information Security Guidelines" (http://www.irs.gov/pub/irs-pdf/p1075.pdf) under for more information.

6. Health Information

6. A. Protected Health Information

Protected Health Information ("PHI") is individually identifiable health information, including demographic information collected from an individual, and is created or received by a health care provider, a health care clearinghouse, or a health plan, which relates to:

- An individual's past, present or future physical or mental health or condition,
- Providing health care to an individual, or
- The past, present or future payment for providing health care to an individual,

and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

The information identifies the individual if it contains one or more of the following identifiers of the individual or of relatives, employers, or household members of the individual:

- Names
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death; and exact age if over 89
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual

This Policy includes any PHI of the DePauw University Group Health Plan (including health, dental and vision coverage).

6.B. Other Information

Restricted Data shall also include personally identifiable (see paragraph 3 above) student health and billing information considered "education records" or "treatment records" under FERPA, as well as health related information received by University in its role as an employer including, but not limited to:

- Health insurance enrollment form
- Life insurance application form
- Request for medical leave of absence
- Workers' compensation report of injury or illness
- OSHA injury and illness reports
- Genetic or medical information obtained in the course of pre-employment physicals, medical exams, or related to disability

The list of documents (above) may vary based on the situation and necessary involvement of the Human Resources Office and contents of an individual's employment records.

VIII. Related state or federal privacy regulations

Laws that influence and affect these guidelines include but are not limited to:

- **Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act)**
  http://www.cleryact.info
- **Children's Online Privacy Protection Rule (COPPA)**
  https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
- **The Digital Millennium Copyright Act (DMCA)**
  http://www.copyright.gov/legislation/dmca.pdf
- **Electronic Communications Privacy Act of 1986 (ECPA)**
  https://it.ojp.gov/default.aspx?area=privacy&page=1285
- **Family Educational Rights and Privacy Act (FERPA)**
  http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- **Higher Education Opportunity Act (HEOA)**
  http://www2.ed.gov/policy/highered/leg/hea08
- **Gramm-Leach-Bliley Act - Privacy of Consumer Financial Information (GLBA)**
  https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/privacy-consumer-financial-information
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
  http://www.hhs.gov/ocr/hipaa/
- **Payment Card Industry (PCI) Security Standards Fair and Accurate Credit Transactions Act (FACTA) and related PCI Security Standards**
  https://www.pcisecuritystandards.org
- **USA Patriot Act**
  http://www.justice.gov/archive/ll/highlights.htm
- **Indiana Security Breach Notification Law**, Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.
  http://iga.in.gov/legislative/laws/2015/ic/
- **Various State Security Breach Notification Laws**
  http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

IX. Related Policies and Guidelines

- **Student Records Policy**
  http://www.depauw.edu/academics/academic-resources/advising/registrar/ferpa-notification
- **HIPAA Policy**
  http://www.depauw.edu/files/resources/2013-notice-of-privacy-practices.docx
- **Record Retention and Document Destruction Policy**
  http://www.depauw.edu/handbooks/employee-guide/rrddp
- **Federal Information Processing Standards Publication 199: Standards for Security Categorization**
  http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- **Internal Revenue Service Publication 1075: Tax Information Security Guidelines**
  http://www.irs.gov/pub/irs-pdf/p1075.pdf

X. Data Handling Recommendations

The following table outlines recommended safeguards for protecting data and data collections based on their classification. In addition to the following data security guidelines, any data covered by federal or state laws or regulations or contractual agreements should meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	Data Classification		
	Public	**Private**	**Restricted**
Access Controls (Who has privileges to access information; technical controls for access)	No restriction for viewing. Authorization by Data Governor is required for access to modify. Authentication is required for access to modify.	Access to view or modify is restricted to authorized individuals as needed for business-related roles. Authorization by Data Governor is required for access. Authentication is required for access. Multi-factor authentication is recommended. Remote access by third party for technical support is limited to authenticated, temporary access via direct connection or secure protocols over the Internet. Network access via local network or VPN is recommended.	Access to view or modify is restricted to authorized individuals as needed for business-related roles. Authorization by Data Governor is required for access. Authentication is required for access. Multi-factor authentication is recommended. Confidentiality agreement is required. Remote access by third party for technical support is limited to authenticated, temporary access via direct connection or secure protocols over the Internet. Network access via local network or VPN is recommended.
Copying/Printing/Transmission (Applies to both paper and electronic format)	No restrictions.	Copies should be limited to individuals with a need to know. Data should not be left unattended on a printer/fax. Copies can be sent via Campus Mail or University email system. Digital encryption is recommended (e.g., via SSL or secure file transfer protocols).	Copies must be limited to individuals authorized to access the data and who have signed a confidentiality agreement. Data must not be left unattended on a printer/fax. Digital encryption is recommended (e.g., via SSL or secure file transfer protocols). Should not transmit via e-mail unless encrypted and secured with

			a digital signature.
Network Security (The network to which to the system hosting or managing the data is directly connected.)	May reside on a public or unsecure network. Protection with a firewall is recommended. Protection only with router access control lists (ACLs) acceptable. IDS/IPS (intrusion detection system / intrusion prevention system) protection is recommended.	Protection with a network firewall is required. Protection with router ACLs is recommended. System or server hosting the data should not be visible to entire Internet. IDS/IPS protection is recommended.	Protection with a network firewall is required. Protection with router ACLs is recommended. System or server hosting the data must not be visible to the entire Internet nor to unauthorized subnets. IDS/IPS protection is recommended.
System Security (The system that hosts or manages access to the data. Applies to both centrally-managed and end-user devices)	Should follow general best practices for system management and security. Host-based software firewall is recommended.	Must follow University-specific and OS-specific best practices for system management and security. Protection with a firewall is recommended. IDS/IPS protection is recommended. Use of system managed in University Data Center or University-approved Cloud Provider is recommended.	Must follow University-specific and OS-specific best practices for system management and security. Protection with a firewall is required. IDS/IPS protection is recommended. Use of system managed in University Data Center or University-approved Cloud Provider is required.
Physical Security (Physical security of area where the system hosting or managing access to the data is located)	System or location should be locked or system logged out when unattended.	System should be locked or logged out when unattended. Located in a secure locked location is recommended; the University Data Center or University-approved Cloud Provider is recommended.	System must be locked or logged out when unattended. Located in a secure locked location is required; the University Data Center or University-approved Cloud Provider is required.
Data Storage	No restrictions.	Storage on a secure server is recommended. Storage in University Data Center or University-approved Cloud Provider is recommended. If data stored on individual workstation or mobile device, encryption is recommended.	Storage on a secure server is recommended. Storage in University Data Center or University-approved Cloud Provider is recommended. If data stored on individual workstation or mobile device, encryption is required. Hard copies must not be left

		Storage of hard copies in secure location is recommended.	unattended and must be stored in a secure location.
Backup/Disaster Recovery	Regular data backup is recommended.	Daily backup is recommended. Off-site storage is recommended. Encryption on backup media is recommended.	Daily backup is required. Off-site storage in a secure location is required. Encryption on backup media is recommended.
Media Sanitization and Disposal (Hard drives, CDs, DVDs, tapes, paper, etc.)	No restrictions.	Shred hard copies; wipe/erase media.	Shred hard copies. Destroy or overwrite electronic media.
Security Awareness Training	General security awareness training is recommended.	General security awareness training is required. Data security training is required.	General security awareness training is required. Data security training is required. Applicable policy and regulation training is required.
Workstations and Mobile Devices (E.g., individual workstations, laptop computers, tablets, smartphones, or similar devices)	Password protection is recommended; workstation inactivity auto-lock is recommended.	Password protection is recommended; workstation inactivity auto-lock is recommended. Encryption is recommended when data stored on device or in transmission.	Password protection is required; inactivity auto-lock is required. Encryption is required when data stored on device and recommended when in transmission.

Definitions

University-approved Cloud Provider – An externally hosted service or system that has been designated by the University as appropriate for specific data storage or management functionalities. Examples include Google Apps for Education (DePauw domain), Box.com (DePauw domain), iModules (Alumni portal), Slate (Admission), SchoolDude (HelpDesk), and Horizons (Hubbard Center), among others. These services have been vetted and contracted (typically) by the University to meet specific information security and data handling standards as appropriate to the type of information processing performed by each system.