Marshall University Information Technology Council

GUIDELINE ITG- 4

Guidelines for Data Classification

1. General Information

1.1. Scope:

This Policy applies to all faculty, staff and third-party Agents of the University as well as any other University affiliate who is authorized to access Institutional Data. In particular, this Guideline applies to those who are responsible for classifying and protecting Institutional Data, as defined by the Information Security Roles and Responsibilities.

1.2. Passage Date:

September 16, 2010

1.3. Effective Date:

September 16, 2010

1.4. Revision Date:

August 19, 2019

1.5. Purpose:

The purpose of this Guideline is to establish a framework for classifying institutional data based on its level of sensitivity, value and criticality to the University as required by the University's Information Security Policy. Classification of data will aid in determining baseline security controls for the protection of data.

2. Definitions

Refer to ITP-10 for Terms and Definitions.

3. Data Classification:

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications:

3.1. 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.

3.2. 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.

3.3. 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.

Classification of data should be performed by an appropriate Data Steward. Data Stewards are senior-level employees of the University who oversee the lifecycle of one or more sets of Institutional Data. See Information Security Roles and Responsibilities for more information on the Data Steward role and associated responsibilities.

4. 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.

5. Reclassification

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well

as changes in the use of the data or its value to the University. This evaluation should be conducted by the appropriate Data Steward. Conducting an evaluation on an annual basis is encouraged; however, the Data Steward should determine what frequency is most appropriate based on available resources. 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.

6. Calculating Classification

The goal of information security, as stated in the University's Information Security Policy, is to protect the confidentiality, integrity and availability of Institutional Data. Data classification reflects the level of impact to the University if confidentiality, integrity or availability is compromised.

There is no perfect quantitative system for calculating the classification of a particular data element. In some situations, the appropriate classification may be more obvious, such as when federal laws require the University to protect certain types of data (e.g. personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide. It is an excerpt from Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

Security Objective	**POTENTIAL IMPACT**		
	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.

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 Information Security Office for assistance.

7. Additional Information

If you have any questions or comments related to this Guideline, please send email to the University Information Security Office at infosec@marshall.edu.

Additional information can also be found using the following resources:

7.1. Information Security Policy

http://www.marshall.edu/board/files/Policies/MUBOG%20IT-2%20Information%20Security%20Policy%20(amended).pdf

7.2. Information Security Roles and Responsibilities

https://www.marshall.edu/it/files/ITP-27.pdf

7.3. Identity Theft Prevention Program

http://www.marshall.edu/board/files/Policies/MUBOG%20FA-12%20Identify%20Theft%20Prevention%20Program.pdf

7.4. Federal Information Processing Standards Publication 199: Standards for Security Categorization

http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

7.5. Internal Revenue Service Publication 1075: Tax Information Security Guidelines

http://www.irs.gov/pub/irs-pdf/p1075.pdf

Appendix A - Predefined Types of Restricted Information

The Information Security Office and the Office of General Counsel have defined several types of Restricted data based on state and federal regulatory requirements. They're 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:

1.1. Passwords

1.2. Shared secrets

1.3. Cryptographic private keys

2. Covered Financial Information

See the University's Identity Theft Prevention Program.

3. Electronic Protected Health Information ("EPHI")

EPHI is defined as any Protected Health Information ("PHI") that is stored in or transmitted by electronic media. For the purpose of this definition, electronic media includes:

3.1.

Electronic storage media includes computer hard drives and any removable and/or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

3.2.

Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, an extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks and the physical movement of removable and/or transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exists in electronic form before the transmission.

4.

5. Export Controlled Materials

Export Controlled Materials is defined as any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations ("EAR") published by the U.S. Department of Commerce and the International Traffic in Arms Regulations ("ITAR") published by the U.S. Department of State.

6. Federal Tax Information ("FTI")

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 Exhibit 2 for more information.

7. 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:

7.1. Cardholder name

7.2. Service code

7.3. Expiration date

7.4. CVC2, CVV2 or CID value

7.5. PIN or PIN block

7.6. Contents of a credit card's magnetic stripe

8. Personally-Identifiable Education Records

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

8.1. Name of the student

8.2. Name of the student's parent(s) or other family member(s)

8.3. Social security number

8.4. Student number

8.5. A list of personal characteristics that would make the student's identity easily traceable

8.6. Any other information or identifier that would make the student's identity easily traceable

See the section on Privacy Rights of Students and Parents in the Marshall University Student Catalog for more information on what constitutes an Education Record.

9. Personally-Identifiable Information

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

9.1. Social security number

9.2. State-issued driver's license number

9.3. State-issued identification card number

9.4. Financial account number in combination with a security code, access code or password that would permit access to the account

9.5. Medical and/or health insurance information

10. Protected Health Information ("PHI")

PHI is defined as any “individual health information that is transmitted or maintained in any form or medium”, as defined by the Marshall University HIPAA Terms Glossary, and related to one or more of the following:

10.1. Past, present or future physical or mental health condition of an individual.

10.2. Provision of health care to an individual.

10.3. Past, present or future payment for the provision of health care to an individual.

The following records are exempted from the definition of protected health information (PHI):

10.4. student records maintained by an educational institution;

10.5. treatment records about a post-secondary student meeting the requirements of 20 USC 1232(a)(4)(B)(iv); and

10.6. employment records held by a covered entity in its role as employer.

PHI is considered “individually identifiable” if it contains one or more of the following identifiers:

10.7. Name

10.8. Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)

10.9. 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)

10.10. Telephone numbers

10.11. Fax numbers

10.12. Electronic mail addresses

10.13. Social security numbers

10.14. Medical record numbers

10.15. Health plan beneficiary numbers

10.16. Account numbers

10.17. Certificate/license numbers

10.18. Vehicle identifiers and serial numbers, including license plate number

10.19. Device identifiers and serial numbers

10.20. Universal Resource Locators (URLs)

10.21. Internet protocol (IP) addresses

10.22. Biometric identifiers, including finger and voice prints

10.23. Full face photographic images and any comparable images

10.24. Any other unique identifying number, characteristic or code that could identify an individual

If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe that the information can be used to identify an individual, it is not considered “individually identifiable” and; as a result, would not be considered PHI.