Data Classification Criteria Guideline

Per the Data Classification Policy, the following definitions have been established;

A. **Confidential** – sensitive data, information, materials and other assets that are confidential to the organization, whether by law, by contract, or otherwise. This classification includes organizational performance (pricing, costs, sales, revenue, profit, etc.), strategic planning, proprietary information, contractual agreements, security issues, financial Information and personal information (PI). This information, if made public or even shared around the organization, could seriously damage the organization, the employees or the customers and could potentially be non-compliant with the Payment Card Industry Data Security Standard and applicable state or federal laws and regulations such as Massachusetts Privacy Law (201 CMR 17.00). This category includes, but is not limited to, Personally Identifiable Information (PII)*.

B. **Sensitive** – sensitive data, information, materials and other assets that support the WSU's organizational operations and therefore must be guarded due to proprietary, ethical, contractual obligations or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This information is not intended for public use and its unauthorized disclosure could adversely impact the company, customers or employees.

C. **Public** – Data which there is no expectation of privacy or confidentiality (data, materials, and other assets) that is intended for public circulation. This information may be freely disseminated without potential harm. Information includes event schedules, Internet content, completed press releases, publication oriented personnel biographies and photos, publication archives, published materials, etc.

The classification criteria list below is intended to provide clarity as to which data falls into the classifications categories but is not intended to cover all data items. Any and all questions regarding the classification of data should be directed to the Information Security Officer.

	Confidential (Highest Level of Sensitivity)	**Sensitive (Moderate Level of Sensitivity)**	**Public (Lowest Level of Sensitivity)**
Description	Data which is regulated and data that would provide access to confidential or restricted information.	Data which has not been published or made public and data protected by contractual obligations.	Data for which there is no expectation for privacy or confidentiality.
Legal Constraints	Protection of data is required by law.	Protection of data is at the responsibility of the owner or custodian.	Protection of data is at the discretion of the owner or custodian.
Risk	High	Medium	Low
Access Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access.	May be accessed by WSU employees and non-employees who have a business "need to know."	No access restrictions. Data is available for public access.
Transmission	Transmission of confidential data through any non-WSU network or WSU guest network is prohibited (e.g. Internet). Transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is also prohibited. Financial tranactions are not allowed to be processed wirelessly.	Transmission of sensitive data through any wireless network, and any non-WSU wired network is strongly discouraged. Where necessary, use of the University's VPN is required. Transmission through any electronic messaging system (e-mail, instant messaging, text messaging,) is also strongly discouraged.	No other protection is required for public information; however, care should always be taken to use all University information appropriately.
Storage	Storage of confidential data is prohibited on non-qualified Information Technology Resources unless approved by ATSSD and the Information Security Officer. If approved, approved encryption is required on mobile computing equipment. Storage of credit card data on any Information Technology Resource is prohibited.	Level of required protection of sensitive data is either pursuant to WSU policy or at the discretion of the owner or custodian of the information. If appropriate level of protection is not known, check with Information Security Officer before storing sensitive data unencrypted.	No other protection is required for public information; however, care should always be taken to use all University information appropriately.
Backup/Recovery	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.	Documented Backup and Recovery Procedures are not necessary, but strongly encouraged.
Retention	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is not required, but strongly encouraged.
Audit Controls	Confidential data must be actively monitored and reviewed for potential misuse and/or unauthorized access. Any department that has individual procedures/security practices must provide those documents to the Information Security Officer. Educational awareness and training must be conducted, at a minimum, annually by the Information Security Officer and/or ASO's.	Sensitive data must be actively monitored and reviewed for potential misuse and/or unauthorized access Educational awareness and training must be conducted, at a minimum, annually by the Information Security Officer and/or ASO's.	No audit controls are required.

	Confidential (Highest Level of Sensitivity)	Sensitive (Moderate Level of Sensitivity)	Public (Lowest Level of Sensitivity)
Examples	**Information resources with access to confidential or restricted data (username and password).** **Personally Identifiable Information (PII): Last name, and first name and/or initial, with any one of following:** • Social Security Number • Driver's license • State ID card • Passport number • Financial account (checking, savings, brokerage, CD,etc), credit card, or debit card numbers **Protected Health Information (PHI)** • Health Status • Healthcare treatment • Healthcare payment **Personal/Employee Data** • Worker's compensation or disability claims **Student Data:** • Loan or scholarship information • Payment history • Student tuition bills • Student financial services information • Class lists or enrollment information • Transcripts; grade reports • Disciplinary action • Athletics or department recruiting information **Business/Financial Data** **Credit Card information**	**Personal/Student/Employee Data** • Income information • Personnel records, performance reviews, benefit information • Race, ethnicity, and/or nationality, gender • Date and place of birth • Directory/contact information designated by the owner as private • Employee ID • CWID – Campus Wide ID **Business/Financial Data** • Financial transactions which do not include confidential data • Information covered by non-disclosure agreements. • Contracts that don't contain PII/PHI • Records on spending, borrowing, net worth **Academic/Research Information** • Library transactions • Unpublished research or research detail/results that are not confidential data • Private funding information • Human subject information • Course Evaluations **Anonymous Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any type of gift information (e.g., amount and purpose of commitment.) or the following; • Telephone/fax numbers, e-mail & employment information • Family information • Medical information **Management Data/Systems Logs** • Detailed annual budget information • Conflict of Interest • Disclosures of the University's investment information • Server Event Logs	**Certain directory/contact information not designated by the owner as private.** • Name • Addresses (campus and home) • Email address • Listed telephone number(s) • Degrees, honors and awards • Most recent previous educational institution attended • Major field of study • Dates of current employment, position(s) • ID card photographs for University use • Publically available payroll information (i.e. information available on Open Checkbook) **Specific for students:** • Class year • Participation in campus activities and sports • Weight and height (athletics) • Dates of attendance • Status **Business Data** • Campus maps • Job postings List of publications (published research)

REVIEW

This guideline shall be reviewed annually by the Chief Information Security Officer and the Security Policy Team.

Date	Version	Updated by	Description of Changes
3-23-2016	1.0	Alan Blair	Draft
7-28-2016	1.1	Alan Blair	Draft
10-5-2016	1.2	Alan Blair	Updated with Security Policy Team (SPT)
11-2-2016	1.3	Alan Blair	Updated with SPT
8-20-2017	2.0	Alan Blair	Reviewed and Approved by SPT
3-20-2018	2.1	Alan Blair	Reviewed and Approved by SPT
10-1-2019	2.2	Alan Blair	Reviewed and Approved by SPT