DATA CLASSIFICATION

PURPOSE

The purpose of this policy is to provide a framework for securing data from risks, including but not limited to, unauthorized destruction, modification, disclosure, access, use and removal. This policy shall be enforced in conformity with all applicable local, state, and federal regulations and laws.

SCOPE

This policy applies to all students, faculty, staff, volunteers, vendors, consultants, contractors, or others (herein afterwards referred to as "constituents") who use or have authorized access to University Information Technology Resources. This policy is supplemented by the policies of those networks to which the University is interconnected, including, but not limited to, the University of Massachusetts Information Technology Systems group, the Commonwealth of Massachusetts' Information Technology Division, UMass Online, etc. It covers all University information whether in hardcopy or electronic form and any systems which access, process, or have custody of business data. This policy also applies to all information, in any form and in any medium, network, internet, intranet, computing environments, as well as the creation, communication, distribution, storage and disposal of information.

For the purposes of this policy, "Information Technology Resources" means all computer and communication facilities, services, data, and equipment that are owned, managed, maintained, leased, or otherwise provided by the University. The Office of Information and Instructional Technology (OIT) refers to authorized personnel currently assigned to Infrastructure Services, Media Services, the Center for Instructional Technology (CIT), Technology Support Services (TSS) and Enterprise Systems. Area Security Officials shall be the supervisor of each department or program with the authority to grant access to Information Technology Resources.

The use of the University's Information Technology Resources constitutes an understanding of, and agreement to, abide by this policy. Additionally, all constituents must protect, and if necessary, intervene to assure that others protect the confidentiality, integrity, and security of all Information Technology Resources.

USER OWNERSHIP AND RESPONSIBILITIES

It is the responsibility of any person using the University's Information Technology Resources to read, understand, and follow this policy. In addition, all users are expected to exercise reasonable judgment in interpreting this policy, and in making decisions about the use of Information Technology Resources. Any person with questions

regarding the application or meaning of this policy should seek clarification from his or her supervisor, or from the Information Security Officer.

The University owns and maintains the information stored in its Information Technology Resources, and it limits access to its Information Technology Resources to authorized users. Users of Information Technology Resources have a responsibility to properly use and protect these resources, respect the rights of other users, and behave in a manner consistent with any local, state, and federal laws and regulations, as well as all University policies. Information Technology Resources, including Internet bandwidth, are shared among the community, and users must utilize these resources with this understanding.

Users must respect all intellectual property rights, including any licensing agreements applicable to information and resources made available by the University to its community.

Information technology resources are provided to support the mission of teaching and learning and to conduct official University business. Therefore, the University bears no responsibility for the loss of any personal data or files stored or located on any system.

The University does not systematically monitor all communications or files. Users must be aware of, and responsible for, material which they send or publish using its network, servers, and other resources, including the Internet.

PROCEDURES

Data must be maintained in a secure, accurate and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk. To implement these security measures and establish guidelines and procedures for compliance, data will be classified in one of the following categories:

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. Constituents that have a legal or regulatory requirement for the non-disclosure of their public information are required to notify the Human Resources Department.

1. Confidential and Sensitive data will require security measures appropriate with the impact of such loss or corruption of the data will impact the operating functions of WSU, result in financial loss or violate policy, contract, or law.

2. Security measures shall be set by the Chief Information Security Officer in collaboration with the Information Security Policy Team, and the Office of Information and Instructional Technology (OIT).

3. All suspected violations of this policy should be immediately reported to the Chief Information Security Officer. Reports of any/all violations will be considered Sensitive Data until otherwise classified by the Chief Information Security Officer or the Information Security Policy Team.

4. The Chief Information Security Officer will investigate and document all suspected violations and make recommendations for further actions.

5. A combination of any of the data items in Sensitive or Public may result in a reclassification requiring a higher level of security measures.

6. All data shall be retained in accordance with the current Massachusetts Statewide Records Retention Schedule and any breaches of this data shall be reported in accordance with MGL CH93H.

7. Nothing in this policy shall prevent the distribution of public records as defined by the Massachusetts Public Records Law, G. L. c. 4, § 7(26). Under the law, every record that is made or received by a government entity or employee is presumed to be a public record unless a specific statutory exemption permits or requires it to be withheld in whole or in part.

8. A table of classification criteria shall be provided in the OIT Data Classification Guideline and shall serve as examples of each classification and is not to be considered an all-inclusive list.

*Personally Identifiable Information (PII) – any information that can potentially be used to uniquely identify an individual

REVIEW

This policy shall be reviewed annually by the Chief Information Security Officer.