

Information Classification Policy

Version: 1.0
Issued: 4/12/2017

PURPOSE

The purpose of the Information Classification Policy is to define the levels of information within the organization at **Fitchburg State University (FSU)**. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE

The scope of this policy applies to all information owned or maintained by **Fitchburg State University** including both hard copy and electronic records.

POLICY

The information within the **Fitchburg State University** environment shall be consistently protected from the time of origination or receipt until the time of destruction according to level of sensitivity, criticality, and business "need to know". Information owned, created, or maintained by **Fitchburg State University** shall be classified into the three categories:

- Public
- Sensitive
- Confidential

Public:

Information (data, materials, and other assets) that is intended for public circulation. This information may be freely disseminated and is subject to disclosure upon request. Information in this classification may include information such as event schedules, Internet content, completed press releases, publication oriented personnel biographies and photos, publication archives, and published materials. Public information shall be defined in accordance with Massachusetts General Laws, Chapter 4, Section 7(26), the Massachusetts Public Records Law.

Sensitive:

Sensitive information (data, materials, and other assets) that supports **FSU** organizational operations and therefore must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other unauthorized use. This information is not intended for public use and its unauthorized disclosure could adversely impact the institution, its customers, or employees. Such information may be withheld from public disclosure only in accordance with the Massachusetts Public Records Law.

Confidential:

Sensitive data, information, materials, and other assets that are confidential to the organization, whether by law, by contract, or otherwise. This classification includes personally-identifiable information (PII) for students, employees, vendors, or other organizations for whom the institution stores data, as well other proprietary information. Unauthorized disclosure of this information may violate state or federal law and/or constitute an unwarranted invasion of someone's privacy rights.

ENFORCEMENT

Any employee found to have violated, intentionally or unintentionally, this policy may be subject to disciplinary action, up to and including termination of employment.

Information Classification Policy

Version: 1.0
Issued: 4/12/2017

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Management Team	Ensure compliance with this policy. Ensure that this policy and all associated policies and procedures are maintained and implemented.
Legal Counsel	Provide guidance on organizational records management and retention.
Staff	Understand and adhere to this policy.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
PO.2 Define the information architecture	<u>PCI</u> Requirement 3: Protect stored cardholder data. <u>MA 201 CMR 17:00</u> Section 17.04	
Classification of Information	Massachusetts General Laws, Chapter 4, Section 7(26), the Massachusetts Public Records Law.	

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	7/28/2015	Compass ITC	Initial Draft