Data Classification

Issued 6/17/2024

Version 63

Purpose

The purpose of the Data Classification Policy is to define the levels of information within the organization at Salem State University (SSU). This includes levels of information that can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of SSU without proper authorization.

Scope

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

Policy

The information within the Salem State University environment shall be consistently protected from the time of origination 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 three categories:

- Public
- Internal
- Restricted

Public:
Information (data, materials, and other assets) that is intended for public circulation. This information may be freely disseminated without potential harm. Examples include event schedules, Internet content, completed press releases, publication-oriented personnel biographies and photos, publication archives, published materials, etc.

Internal:
Sensitive data, information, materials and other assets that support SSU 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 use. This information is not intended for public use and its unauthorized disclosure could adversely impact the company, customers or employees. Examples include but not limited to Personnel and Student Records, Immigration Records.

Restricted:
Sensitive data, information, materials and other assets that are confidential to the organization, whether by law, by contract, or otherwise. Examples include information security, PII (which may include Personnel and Student Records, Immigration Records), and legal records. 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) and NIST SP 800-171 Revision 2 and the Gramm-Leach-Bliley Act.

Role

ITS Security Team: Ensure compliance with this policy. Ensure that this policy and all associated polices and procedures are maintained and implemented.

Staff: Understand and adhere to this policy.

References CIS

3.1 – 3.14 Data Protection

References PCI

PCI
Requirement 3: Protect stored cardholder data.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

Security Level Public