Data Classification Policy

Version 1.2	**Last Updated:** 8/8/2025
Security Level: Internal	**Issued:** 9/7/2022

Purpose

The purpose of the Data Classification Policy is to define the levels of information within the organization at Fitchburg State University. Further instructions include 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 Fitchburg State University without proper authorization.

Scope

This policy applies to all information owned or maintained by Fitchburg State University, including hard copy and electronic records. The Written Information Security Program provides further definitions and examples.

Policy

The information within the Fitchburg State University environment shall be consistently protected from the time of origination until the time of destruction according to the 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) 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:

Internal data is information that supports Fitchburg State University’s 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 are not limited to, personnel records, procedural documents, some memos, correspondence, meeting notes, and vendor information.

Restricted:

Restricted Data includes information that Fitchburg State University has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. If made public or even shared around the organization, this information could seriously damage the organization, its employees, or its 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.

Examples include but are not limited to, PII, SSNs, PCI Data, CUI Data, organizational performance, strategic planning, proprietary information, contractual agreements, financial Information, security incidents, Fitchburg State University Senior Management and Board-related communications and information, organizational trusts, government or military records, legal proceedings, and results. This also includes Attorney-Client Privileged information, Federal Information Security Management Act (FISMA) data, and Authentication data, including passwords, keys, and other electronic tokens.

Roles

Technology 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

CISv8 3.1- 3.14 Data Protection
PCIv4 Requirement 3 - Protect Stored Account
MA 201 CMR 17:00 Section 17.04

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 in 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.

Revision History

Date of Change	Revision	Responsible	Summary of Change
9/7/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
5/31/2024	1.1	Eric Boughton, CISO	Formatting and updating to match WISP
8/08/2025	1.2	Eric Boughton, CISO Stefan Dodd, CIO	Annual review, Formatting