FITCHBURG STATE UNIVERSITY

Written Information Security Program

Version 2.1	**Last Updated:** 10/8/2024
Security Level: Public	**Issued:** 8/15/2022

Objective

Fitchburg State University's Written Information Security Program (WISP) aims to establish robust administrative, technical, and physical safeguards for protecting Restricted Institutional Data. The program's primary goal is to ensure compliance with legal and regulatory privacy and security obligations. Restricted institutional data encompasses various data types, including those mandated by law, internally sensitive data, and confidential organizational information. The WISP addresses compliance with several key laws and regulations. It supports the University community in responsibly managing this data, tailored to the data's sensitivity and potential risks associated with its misuse.

The WISP covers all aspects of handling Restricted Institutional Data across different media, reinforcing compliance with other relevant University policies and legal standards. It also guides the development of specific security plans to meet diverse legal and regulatory requirements related to this data.

Among the applicable laws and regulations included within this program are:

- The Massachusetts Data Privacy Laws and Regulations at M.G.L. c. 93H, c. 93I and 201 CMR 17.00
- The Safeguards Rule issued under the Financial Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (the GLBA)) and associated regulations
- The Payment Card Industry Data Security Standards (PCI DSS)
- The Family Education Rights and Privacy Act (FERPA) and associated regulations
- The Health Insurance Portability and Accountability Act (HIPAA) and associated regulations
- The European Union (EU) General Data Protection Regulation (GDPR) and the United Kingdom (UK) GDPR, tailored by the UK Data Protection Act 2018 (UK DPA)

Purpose

The primary purpose of a Written Information Security Program (WISP) is to establish and maintain a comprehensive strategy for protecting an organization's sensitive and confidential information. The key objectives of the WISP include:

- Ensuring Compliance: Many organizations are required by law, regulations, or industry standards to protect certain types of information. The WISP helps comply with these requirements by providing a structured approach to information security.
- Establishing Accountability: The WISP assigns specific roles and responsibilities to staff members, creating a structure of accountability for information security within the organization.
- Risk Management: A WISP identifies potential security risks to the organization's information assets and defines strategies to mitigate these risks. This includes assessing threats and vulnerabilities and implementing appropriate security measures.
- Data Protection: The WISP outlines policies and procedures for safeguarding sensitive data from unauthorized access, disclosure, alteration, or destruction. This protection extends to data in various forms, including digital, paper, and other formats.
- Incident Response Preparedness: The WISP provides a framework for responding effectively to information security incidents, minimizing the impact of any incidents, and ensuring a coordinated response.
- Employee Awareness and Training: By including guidelines for training and awareness, the WISP ensures that employees understand their roles and responsibilities in maintaining information security and are aware of best practices.
- Maintaining Customer Trust: By demonstrating a commitment to information security, a WISP helps build and maintain University partners' trust.
- Continuous Improvement: Regular reviews and updates to the WISP ensure that the organization's information security practices remain effective and relevant in the face of changing threats and technologies.

Scope

Applicability:

- **All Employees**: Full-time and part-time employees, temporary workers, and personnel employed by third parties to perform duties on the University's premises, remotely, or at locations where the University's activities are hosted or outsourced.
- **Vendors and Service Providers**: Any external entities or individuals who are engaged in business with the University and have access to its information or systems, e.g., contractors, consultants, temporary workers, and personnel affiliated with third parties.
- **Students** (Where Applicable): The WISP may also extend to students of Fitchburg State University, depending on the relevance and necessity in specific contexts.

Data and Information Systems Coverage:

This program encompasses all forms of data (electronic, printed, or spoken) and all information systems and technologies used in the day-to-day operations, including, but not limited to, computer systems, mobile devices, network equipment, and software applications. Including:

- All electronic and physical data storage and processing facilities.
- Data in transit, at rest, and in process.

- Remote access technologies and wireless communication methods.
- Cloud-based services and third-party data management solutions.

Information Security Areas:

- Physical Security: Securing physical access to information systems and data storage areas.
- Network Security: Protecting data in transit within and outside the organizational network.
- Access Control: Ensuring only authorized individuals have access to sensitive data and systems.
- Incident Response and Management: Procedures for managing and responding to security incidents.
- Compliance and Legal Requirements: Adhering to applicable laws, regulations, and contractual obligations related to information security.

Definitions

Institutional Data

All information created, discovered, collected, licensed, maintained, recorded, used, or managed by the University, its employees, and agents working on its behalf, regardless of ownership or origin, is institutional data regardless of the ownership of any device, machine, or equipment used to create, discover, collect, store, access, display, or transmit the information. This broad definition ensures that all information the University handles is comprehensively covered under the WISP.

Institutional Systems

All electronic and physical systems used by the University to handle institutional data, including computers, mobile devices, servers, research equipment, and various communication and storage systems. Even if these systems are installed on non-university devices, they are governed by University policies.

Encryption

Encryption refers to the process of converting data into a secure format through the use of algorithms or equally secure methods. This ensures that the data remains unintelligible without access to the necessary confidential process or key, significantly reducing the likelihood of unauthorized interpretation or use.

Restricted Institutional Data

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:

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.

Defined Data Types

The provided definitions aim to clarify the types of data classified as Restricted Institutional Data within the university's framework. These definitions are essential for understanding the specific categories of data that fall under this classification and their significance within the university's data management policies.

Sensitive Personal Information (SPI)

1. All Massachusetts Personal Information;
2. Biometric indicators (as included in the definition of personal information subject to c. 93I of the Massachusetts Data Privacy Laws and Regulations); and
3. Any government-issued identification card numbers, whether issued by the United States government, a state government, or a foreign government, and includes, without limitation, passport numbers and visa numbers.

References
https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents

Massachusetts Personal Information

As defined in and referenced by c. 93H of the Massachusetts Data Privacy Laws and Regulations.

An individual's first name and last name or first initial and last name, in combination with that person's:

1. Social Security number;
2. Driver's license or other state-issued identification card number; or
3. Credit or debit card number or other financial account number, in each case with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

"Massachusetts Personal information" does not include publicly available information.

References
https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents

Financial Customer Nonpublic Personal Information under the GLBA (Financial Customer GLBA Data)

Any personally identifiable information:

1. A student, patient, customer or other person provides in order to obtain a financial service or product from Fitchburg State University,
2. About a student, patient, customer or other person resulting from any transaction with Fitchburg State involving a financial service or product, or
3. Otherwise obtained about a student, patient, customer or other person in connection with providing a financial service or product to that person.

Financial Customer GLBA Data does not include publicly available information.

Examples of Financial Customer GLBA Data include addresses, phone numbers, bank and credit card account numbers, income and credit histories, account balances, tax return information, and Social Security numbers.

References
https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Cardholder Data under Payment Card Industry Security Standard (PCI DSS)

At a minimum, cardholder data consists of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Additionally, sensitive authentication data, including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks used to authenticate cardholders and/or authorize payment card transactions.

References
https://www.pcisecuritystandards.org/glossary/#glossary-c

Personally Identifiable Information in Student Educational Records under FERPA

Personally Identifiable Information in Student Educational Records (each as defined in the statute and the associated regulations) is subject to protection under FERPA, and includes, but is not limited to:

A. The student’s name;
B. The name of the student’s parent or other family members;
C. The address of the student or student’s family;
D. A personal identifier, such as the student’s Social Security number, student number, or biometric record;
E. Other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name;
F. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
G. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

References
https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

https://studentprivacy.ed.gov/ferpa#0.1_se34.1.99_13

Federal Tax Information (FTI)

Safeguarding FTI is critically important to continuously protect taxpayer confidentiality as required by IRC § 6103. FTI consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control that is covered by the confidentiality protections of the IRC and subject to the IRC § 6103(p)(4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive But Unclassified (SBU) information and may contain personally identifiable information (PII).

FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS) or Centers for Medicare and Medicaid Services (CMS) or another entity acting on behalf of the IRS pursuant to an IRC § 6103(p)(2)(B) Agreement.

FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

References
https://www.irs.gov/pub/irs-pdf/p1075.pdf
https://www.irs.gov/privacy-disclosure/safeguards-program

Protected Health Information (PHI) under HIPAA

Includes all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."

"Individually identifiable health information" is information, including demographic data, that relates to:

1. The individual's past, present or future physical or mental health or condition,
2. The provision of health care to the individual, or
3. The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. "Individually identifiable health information" includes many common identifiers (e.g., name, address, birth date, Social Security Number).

References
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge

Personal Data under the European Economic Area (EEA) GDPR and the UK GDPR

Personal Data, as defined under the GDPR regulations of both the European Economic Area (EEA) and the United Kingdom (UK), encompasses any information that can identify a natural person. This includes, but is not limited to, details like names, identification numbers, location data, online identifiers (such as IP addresses), and images. The handling of such data by Fitchburg State University is subject to specific conditions:

1. For EEA or UK-based Activities: When Fitchburg State University conducts programs or activities within the EEA or the UK, the collection and processing of Personal Data apply to these activities, irrespective of whether the data processing occurs within the EEA or the UK.
2. For Non-EEA Based Programs: In the case of Fitchburg State University programs operating outside of the EEA, the regulations apply to the Personal Data of individuals who are in the EEA or the UK at the time of providing their data. This is relevant when these individuals are either:
   - Offered goods or services by the University, or
   - Subject to behavior monitoring by Fitchburg State University.

References
https://gdpr.eu/what-is-gdpr/

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) refers to information that the United States government creates or possesses or that an entity creates or possesses for or on behalf of the government. CUI is not classified information but is sensitive and requires protection due to its potentially damaging impact on national security if disclosed.

Examples of CUI include but are not limited to:

- Personal information: such as health records, social security numbers, and personnel files.
- Financial information: including budgetary details, contracts, and unclassified financial data that is sensitive, e.g., FAFSA data.
- Law enforcement data: including information related to investigations, intelligence activities, and other law enforcement-sensitive data.

References
https://www.archives.gov/cui/registry/cui-glossary.html
https://www.archives.gov/cui

Criminal Justice Information Services (CJIS) Data

Criminal Justice Information is the term used to refer to all of the FBI CJIS-provided data necessary for law enforcement and civil agencies to perform their missions, including, but not limited to, biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describes the various data sets housed by the FBI CJIS architecture:

1. **Biometric Data**—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

2. **Identity History Data**—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. **Biographic Data**—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. **Property Data**—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. **Case/Incident History**—information about the history of criminal incidents.

The following types of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

References
https://datastandards.cjis.gov/

Roles and Responsibilities

Chief Information Security Officer (CISO)

The Chief Information Security Officer is responsible for overseeing the overall strategy and implementation of information security measures. The CISO ensures the program aligns with the organization's objectives and compliance requirements. The CISO will have the following key responsibilities:

1. WISP Implementation: Overseeing the initial setup and implementation of the Written Information Security Program (WISP).
2. Regular Testing: Conducting periodic assessments and testing of the WISP's protective measures to ensure its effectiveness.
3. Third-Party Vendor Evaluation: Assessing and ensuring that third-party service providers (as outlined in the Vendor Management Policy) are capable of and committed to maintaining appropriate security measures for restricted information. This includes contractually mandating these measures and ensuring they report any security incidents involving restricted information.
4. Responsible for identifying, assessing, and mitigating risks to information security as outlined in the Risk Management and Risk Assessment and Audit Policy.
5. Annual Review and Update: Conducting at least an annual review of the WISP's security measures, especially in the event of significant changes in business practices that might affect the security or integrity of records containing restricted information. The Chief Information Security Officer will inform management about the outcomes of this review and suggest any necessary enhancements for improved security.
6. Training and Certification: Organizing training sessions, either electronically or in person, for all individuals (including owners, managers, employees, independent contractors, and temporary/contract workers) with access to restricted information on the elements of the WISP. Participants must certify their attendance and understand the university's

requirements for protecting restricted information as outlined in the Security Training and Awareness Policy.

7. Incident Response Management: Executing the Incident Response Policy and associated procedures in the event of information security incidents.
8. Critical Passwords Management: Maintaining a highly secure master list of all critical passwords to safeguard access to sensitive information and systems. Passwords will adhere to the University Password Policy.

Technology Department Security Team

The Technology Department Security Team is responsible for the technical aspects of information security, including system monitoring, vulnerability assessments, incident response, and the implementation of security tools and processes.

Technology Department Managers

All management and supervisory staff at Fitchburg State University Technology Department hold a critical responsibility for enforcing and ensuring adherence to the Written Information Security Program (WISP). This includes the vital task of disseminating the WISP to guarantee that all employees are informed about, accept, and comply with its stipulations. Every employee is obligated to follow the university's policies, particularly those related to Information Security, and any other reasonable and authorized directives issued by the university.

In the event of serious violations of the WISP, employees are required to report such incidents to one of the following designated individuals:

- Chief Information Security Officer Eric Boughton
- Chief Information Officer Stefan Dodd

System Administrators

Information Technology Administrators encompass a broader group beyond those in the Technology Department. This role also extends to individuals outside the department who are responsible for managing systems that process, transmit, or store data. Regardless of their departmental affiliation, these administrators are integral to effectively and securely handling our organization's data systems. System Administrators play a pivotal role in collaborating with faculty and staff to ensure the secure and reliable management of Internal and Restricted Institutional Data. Their responsibilities include:

1. **System Maintenance and Operation**: They are tasked with maintaining and operating our institutional systems at a level of security that is appropriate for the confidentiality requirements of the Restricted Institutional Data these systems hold or access.
2. **Policy Adherence**: They rigorously follow and implement a range of applicable policies, guidelines, standards, and procedures specifically designed for the management of Restricted Institutional Data.

3. **Access Control**: In accordance with decisions made by management, Administrators are responsible for effectively managing access to institutional data, including both the granting and disabling of such access as necessary.

These individuals play crucial roles in ensuring a high standard of data security and integrity across our institution's information systems. Their work is fundamental to maintaining the trustworthiness and efficiency of our data management processes. Some examples include:

- Admissions Department managing Slate application
- Finance administrating Touchetnet Marketplace

Department Heads and Managers

Department Heads are individuals who are responsible for implementing and enforcing the WISP within their respective departments, ensuring that their staff complies with security policies and procedures.

Fitchburg State University Employees

Every employee has a role in the WISP, primarily related to adhering to the policies and procedures, maintaining security best practices, and reporting any security incidents or vulnerabilities they observe.

Program Components

Risk Assessment and Strategy

Fitchburg State University is dedicated to upholding the highest data security and confidentiality standards. To this end, the Technology Department will conduct an annual Technology Risk Assessment aimed at fortifying our data protection measures. The objectives of this assessment are to:

1. **Risk Identification**: Detect any reasonably foreseeable internal and external threats to the security, confidentiality, and integrity of electronic, paper, or other records containing Restricted Information.
2. **Access Permissions Revie**w: Conduct a thorough examination of access permissions to critical data systems for all users, making necessary adjustments to ensure data security.
3. **Threat Evaluation**: Assess the likelihood and potential impact of these threats, especially in the context of the sensitivity of the Restricted Information.
4. **Safeguard Evaluation**: Critically evaluate the adequacy of current policies, procedures, information systems, and other safeguards currently employed to mitigate identified risks.

5. **Safeguard Implementation Plan**: Develop and execute a Technology Department Strategic Plan to establish robust safeguards that effectively minimize risks, in line with our commitment to confidentially handle and protect Restricted Information against data breaches.
6. **Monitoring and Review**: Continually monitor the effectiveness of these safeguards, ensuring they remain capable of addressing evolving threats and vulnerabilities.

Incident Response

In accordance with the Fitchburg State Incident Response Policy. Indications of unauthorized access, misuse, loss, theft or destruction of Restricted information will trigger a notification to the incident response team. Upon notification, the team will follow the Incident Response Plan.

Employees are required to report information security incidents and suspicious incidents to either their manager or the IT Security Team.

Applications, Tools, and Services

The management of Restricted Institutional Data at Fitchburg State University, encompassing its collection, use, storage, handling, processing, and access, must strictly adhere to methods, applications, tools, and services that comply with all applicable regulatory and contractual requirements. Additionally, the self-provisioning of cloud services for handling Restricted Institutional Data is strictly prohibited. Instead, offices, departments, and employees must collaborate with the Technology Department to evaluate and mitigate the risks associated with using such services for Restricted Institutional Data.

Data Encryption

Encryption Policy for Restricted Institutional Data

1. Encryption of Restricted Data at Rest:
   - It is mandatory for all Restricted Institutional Data stored on servers, storage areas networks (SAN), and portable devices, including but not limited to laptops, tablets, mobile phones, external hard drives, USB sticks, and other data storage media, to be encrypted.
2. Encryption of Data in Transit:
   - Any transmission of files and records containing Restricted Institutional Data across public networks or via wireless means must be encrypted.
   - Recommended protocols include SSL/TLS (Secure Sockets Layer/Transport Layer Security) for web-based transmissions and VPN (Virtual Private Network) services for remote access.
3. Encryption Key Management:
   - Encryption keys must be securely managed and accessible only to authorized personnel.

- Key management practices must include secure key storage, periodic key changes, and immediate key revocation when a key is compromised or when personnel with access leave the University.

4. Secure Electronic Communication:
    - Restricted Information must only be transmitted electronically if:
        1. It is encrypted over public networks, like the Internet.
        2. It is sent over Fitchburg State University’s private network.
        3. It is sent via a secure VPN with two-factor authentication for remote access.
    - For external email communication, Restricted Information may only be sent using encryption tools provided by Fitchburg State University. If encryption is impossible, an alternative secure delivery method must be used.
    - To the extent feasible, emailing of Restricted Information should be minimized to avoid the need for printing. If printed, the data must be protected per the hardcopy restricted Information guidelines.

Collection & Access to Restricted Information

Fitchburg State University shall limit the collection of Restricted Information to what is essential for its legitimate business operations or to fulfill Confidentiality Obligations.

Access Control

- Access to both electronic and hardcopy records containing Restricted Information will be strictly limited to individuals who require this information to execute Fitchburg State University's legitimate business objectives or to comply with state, or federal regulations.
- Accessing Restricted Institutional Data that is not directly relevant to one's job duties or contractual obligations, including employee, student, or patient records, is strictly forbidden. This applies even if the intention is benign and regardless of whether the information is subsequently disclosed or not.
- Calls or other requests for Restricted Institutional Data are to be referred to responsible individuals who are knowledgeable in the regulatory requirements applicable to the requested information.
- Access to offices should be restricted to authorized personnel only. Any loss or theft of keys or ID cards granting access must be immediately reported to the appropriate authority.
- Desktop and laptop screens should be positioned to prevent unauthorized viewing. Users must lock their screens or log off when leaving their devices unattended. Technology Services automatically sets University Machines to lock after a period of inactivity.
- Devices like copiers, scanners, printers, and fax machines used for handling Restricted Institutional Data should be located in secure work areas during the day and in locked spaces after business hours.

Terminated Employee Protocols:

- Upon termination, employees must return all forms of Restricted Information in their possession, including data on portable devices (laptops, phones), files, records, work papers, etc.
- Immediate revocation of both physical and electronic access to Restricted Information is required for terminated employees. This includes surrendering all items that grant access to university premises or information (keys, OneCard/IDs, access codes, business cards, etc.).
- Remote electronic access, including voice, voicemail, email, VPN, WiFi/Network, and passwords, must be disabled for terminated employees.

Visitor Access Regulations:

- Visitor access in buildings where Restricted Information is processed, transmitted, or stored will be strictly controlled.
- Visitors are required to sign in and wear visible “GUEST” badges at all University Data Centers and the Technology Department areas.
- Unescorted visitor access to areas containing Restricted Information is prohibited.

Electronic Access and Transmission of Restricted Information

1. **Scope of Electronic Access:**

   Electronic access to Restricted Information at Fitchburg State University includes the use of computers and laptops, primarily through email, file services, and electronic document storage. This also extends to mobile devices like smartphones, tablets, thumb drives, and similar storage devices.

2. **Controlled Access and Downloading:**
   - Employees are prohibited from copying or downloading electronic records containing Restricted Information onto any device unless:
     - The device is encrypted.
     - The download has a clear and legitimate business purpose.
3. **User Access Management:**
   - Electronic access to Restricted Information is strictly limited to active users and user accounts.
   - Following multiple unsuccessful access attempts, user identification must be automatically blocked.
   - Employees must maintain secure user IDs and passwords according to the Technology Department's system requirements, avoiding vendor-supplied or default passwords.
   - Access to electronically stored Restricted Information requires a unique login ID. Automatic re-login is mandated after a period of inactivity, as specified by the Technology Department’s system configuration requirements.

Hardcopy Access, Transmission, and Transport of Restricted Information

1. **Access to Hardcopy Restricted Information:**
   - Access to Restricted Information in hardcopy form should be strictly limited to necessary Fitchburg State University personnel who require it for legitimate business purposes.
   - Each department handling Restricted Information must establish internal controls to verify the legitimacy of disclosure requests.

2. **Secure Handling and Storage:**
   - Employees cannot leave files containing Restricted Information open and unattended on their desks. When not actively in use, such documents should be securely stored.
   - All hardcopy Restricted Information and electronic media must be kept in a securely locked office, cabinet, or storage facility outside of business hours to prevent unauthorized access.

3. **Sharing and Redacting Restricted Information:**
   - When sharing any electronic or hardcopy records containing Restricted Information with internal or external parties who are not authorized to access certain parts of this information, it is mandatory to redact the Restricted Information before sharing.
     - For instance, if the Human Resources department needs to provide an employee’s records to a department manager, any Restricted Information within those records, whether in hardcopy or electronic form, must be thoroughly redacted.

Storage of Restricted Information

1. **Departmental Storage Guidelines:**
   - Every department at Fitchburg State University is required to formulate written procedures that clearly define how access to restricted information is controlled, taking into account their unique business needs, and to enforce reasonable restrictions on access to electronic and hardcopy records.
   - Departments must ensure the secure storage of these records in locked facilities, secure areas, or containers. Under no circumstances should Restricted Information be stored in unsecured locations, such as unlocked cabinets or offices.
2. **Prohibited Storage Practices:**
   - Restricted Information must not be left unattended in areas prone to unauthorized access, like unsecured copy machines or printer stations.
   - It is strictly forbidden to permanently store Restricted Information on any mobile device, laptop, or desktop computer's local drive belonging to Fitchburg State

University. Restricted information must be stored in the institution's secure storage location once necessary tasks have been completed.

3. **Personal Devices Handling Restricted Institutional Data**
    - Storage on Personal Devices:
        - Restricted Institutional Data must not be stored on any personal desktop, laptop, smartphone, or similar device, unless:
            A. The device is under the management of the Technology Department.
            B. The device is managed following specific guidelines set by the Technology Department.
    - Recommended Use of Virtual Desktop Interface (VDI):
        - Users are encouraged to access Restricted Institutional Data through a Fitchburg State-provisioned Virtual Desktop Interface (VDI) when using personal devices. This should be done to comply with data protection standards.
4. **Off-Site Security Measures:**
    - Removal of hardcopy or electronic media containing Restricted Information from secure storage for off-site use is only permissible for legitimate university business purposes, and the information must be protected at all times.
    - It is unacceptable to leave Restricted Information, such as employee files, in an unsecured and unoccupied vehicle or at an employee's home.
    - In situations where electronic Restricted Information must be transported from its secure location, it must be carried on an encrypted laptop or equivalent secure media.
    - For hardcopy Restricted Information, a meticulous record should be maintained, documenting the individual in possession of the information, the date of removal, and the date of return.

Disposal of Restricted Information

The disposal of Restricted Information at Fitchburg State University is handled with the highest level of diligence to ensure confidentiality and compliance with all pertinent obligations, adhering to the following prescribed protocols.

1. **Disposal of Hardcopy Restricted Information:**
    - Once it is determined that there is no longer a legitimate business need for hardcopy Restricted Information, these documents must be destroyed securely. This can be achieved through the use of an office-grade cross-cut shredder or by placing the documents in marked, contracted document shredding receptacles provided by a professional shredding service.
    - Under no circumstances should Restricted Information be discarded in regular trash, recycling bins, or any other public disposal methods.
2. **Disposal of Electronic Restricted Information:**

- The disposal of electronic records, including those on hard drives or other media, must adhere strictly to all Confidentiality Obligations, specifically including Massachusetts General Law 93I
- The Technology Department is responsible for managing the disposal of all electronic format Restricted Information, including printers, computers, mobile devices, network equipment, removable media or other technology that contains digital storage of media.
- Additionally, the Technology Department is available to consult with other departments on the secure disposal of hardcopy Restricted Information to ensure compliance with confidentiality requirements. One method is to use a cross-cut shredder or similar appropriate technology for paper media before recycling and discarding.

Transmission Restrictions

- Employees must only transmit Restricted Information using Fitchburg State University-issued laptops and desktop computers. Transmission via non-company devices is prohibited due to increased security risks.
- Restricted Information must not be transmitted through unapproved channels such as personal email, instant messaging, social media sites, or unencrypted internet channels. All transmissions must adhere to protocols approved by the Technology Department, ensuring encrypted and secure data transfer.

Campus Network Access

- While on the Fitchburg State University campus, employees and any other individuals authorized to access Restricted Institutional Data must strictly use one of the following secure connection options:
  1. Ethernet Connection: A direct Ethernet connection to the Fitchburg State University network.
  2. Encrypted Wireless Service: The FSUwifi encrypted wireless service is specifically designed for secure access.
- It is expressly prohibited for those handling Restricted Institutional Data to connect via unencrypted wireless networks, such as IOT or Public Wi-Fi options. These networks do not offer the necessary encryption to ensure the security and confidentiality of Restricted Institutional Data.

Email

Authorized Email System:

- In accordance with the Electronic Mail Services policy, Employees and others with access to Restricted Institutional Data are only permitted to use the Fitchburg State email system for communicating such data. The term "Fitchburg State email" specifically refers to the @fitchburgstate.edu system and does not include other email systems with addresses like @[abc].fitchburgstate.edu or similar variants.

Alternative Communication Tools Recommendation:

- Due to the risks associated with email, such as accidental misaddressing and vulnerability to hacking, it is strongly advised to use alternative communication tools for Restricted Institutional Data wherever possible.

Guidelines for Necessary Email Use:

- If Fitchburg State email must be used for Restricted Institutional Data, adhere to one of the following methods:
    - Send the message from one @fitchburgstate.edu address to another.
    - Transmit the information in an encrypted, password-protected document, with the password communicated securely by means other than email.

Prohibition on Email Forwarding:

- Automatic forwarding of Fitchburg State employee email accounts to non-Fitchburg State email systems is strictly prohibited.

Handling Email with Restricted Institutional Data:

- Fitchburg State email should not be used for long-term storage of Restricted Institutional Data. Any such data received or sent via email must be promptly moved to secure storage and the email message deleted, including emptying the email trash bin.

Remote Access and Transmission Protocols:

- When necessary for legitimate business purposes, remote transmission of Restricted Information should be conducted solely through Fitchburg State University's secure private network or VPN connections, which require two-factor authentication and encrypted internet protocols.

System Security Measures

- Fitchburg State University is committed to maintaining robust firewall protection and up-to-date operating system security patches on all systems handling Restricted Information.
- Systems are equipped with the latest security agent software, including malware protection, and are kept current with patches and virus definitions.
- Employees with company-issued laptops or desktops are required not to disable automatic updating functions on these devices.

Monitoring and Data Identification

- All computer systems are monitored for unauthorized use or access to personal information.

- End-user computers and laptops are scrutinized using data identification tools to locate any stored Restricted Information.

Password and Authentication Protocols

- Employees using company-owned desktops, laptops, mobile devices, or accounts are responsible for maintaining passwords that comply with the University Password Policy.
- The sharing of passwords is strictly forbidden.
- The system periodically prompts users to modify their passwords; compliance with these prompts is mandatory.
- Multi-factor authentication (MFA) is required wherever feasible to add a layer of security to user access to Restricted Information.

Compliance and Enforcement

Education, Training, and Awareness

Fitchburg State University is committed to ensuring that all individuals with access to Restricted Institutional Data are thoroughly informed and trained. To achieve this:

1. Availability of program Information: The University will provide all individuals with access to Restricted Institutional Data with a description or a copy of the Written Information Security Program and any related plans. This ensures that everyone is aware of the program's scope and their role within it.

2. Security Training: Ongoing training will be provided to those with access to Restricted Institutional Data. This includes personnel responsible for administering the University's computer security systems. The training aims to ensure that all relevant parties are fully conversant with their responsibilities and the importance of data security.

3. Content of Training:
   The training sessions will cover several key areas, including:
   - The significance of securing Restricted Institutional Data.
   - Detailed information on the requirements and guidelines outlined in the Information Security Program and associated plans.
   - An overview of the legal and regulatory obligations pertaining to data security.

By implementing these measures, Fitchburg State University demonstrates its commitment to upholding the highest standards of data security and ensuring that all personnel involved are well-equipped to protect and manage Restricted Institutional Data effectively.

Disciplinary Measures

Fitchburg State University enforces strict disciplinary actions for any intentional breach of the WISP. Violations may result in severe consequences, including but not limited to revocation of access rights and termination of employment, in accordance with respective collective bargaining agreements.

Reporting and Response Procedures

Reporting and response procedures are crucial for promptly addressing potential breaches in the Written Information Security Program (WISP) and maintaining the integrity of Restricted Information at Fitchburg State University. They ensure that any unauthorized access or misuse of data is swiftly identified, properly investigated, and effectively managed to comply with legal obligations and to reinforce data security protocols.

1. Employee Reporting Responsibilities:
    - Employees are mandated to report any suspicious or unauthorized use of customer information to the designated authorities.
2. Managerial Responsibilities:
    - Upon receiving information about a potential WISP violation, managers must:
      i. Immediately report the incident to the Information Security Team.
      ii. Consult with the Human Resources department.
      iii. Adhere to Fitchburg State University's disciplinary policy, ensuring that the disciplinary action is formally documented in the employee's personnel file.
3. Annual Reporting:
    - An annual report detailing the assessment, recommendations for changes, and other necessary actions to meet GLBA obligations must be submitted to the University Board of Trustees.
4. Post-Incident Review:
    - In cases of incidents necessitating notification under any Confidentiality Obligations, a mandatory post-incident review will be conducted promptly.
    - The review aims to evaluate events and actions taken and to determine if modifications in Fitchburg State University's security practices are needed to enhance the security of Restricted Information under the University's responsibility.

References

CIS Controls v8
3 Data Protection
5 Account Management
9 Email and Web Browser Protections
14 Security Awareness and Skills Training
https://www.cisecurity.org/controls

PCI DSS v4.0
Requirements 3,4: Protect Account Data
Requirements 7,8,9: Implement Strong Access Control Measures
Requirement 12: Maintain an Information Security Policy
https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf

Massachusetts General Law
MA 201 CMR 17.00
Section 17.03
Section 17.04
https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth

Security Level

Public

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.

Revision History

Date of Change	Revision	Responsible	Summary of Change
8/15/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Start of Revision Tracking, Formatting of Document
5/8/2024	2.0	Stefan Dodd, CIO Eric Boughton, CISO	Modernized WISP. Reorganized Sections for Clarity. Added Data Definitions and Links to Policies
10/5/2024	2.1	Eric Boughton, CISO	Corrected Formatting for Federal Tax Information

Approval

- University Cabinet voted to approve the Written Information Security Program on October 21st, 2024.