Encryption

Issued 1/25/2024

Version 101

Purpose

This policy defines the requirements for the use of encryption algorithms to protect Confidential and Restricted Information at Salem State University (SSU). This policy is designed to ensure compliance with applicable regulations and standards, including but not limited to:

- Payment Card Industry Data Security Standard (PCI DSS)
- Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
- NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- Center for Internet Security (CIS) Controls
- General Data Protection Regulation (GDPR) (under consideration)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

Scope

This policy governs the use of encryption to protect Salem State University's confidential and restricted information. Encryption requirements are determined by prioritizing actions based on the potential impact and likelihood of negative events, considering factors such as legal and regulatory obligations, data classification, access methods, storage and transmission mechanisms, and existing security controls.

This policy applies to all SSU employees, contractors, vendors and any other individuals or entities accessing, processing or storing Confidential or Restricted Information on SSU systems or networks, including cloud-based networks. This includes, but is not limited to, data at rest, data in transit and data in use. This policy also applies to all SSU owned devices, and any personally owned device used to access, process or store SSU data.

Policy

- Encryption of Restricted Information: All Restricted Information, both at rest and in transit, must be encrypted using Approved Encryption Algorithms.
- Encryption of Confidential Information: Encryption of Confidential Information is required, especially when transmitted across untrusted networks or stored on portable devices. Encryption of confidential information on all SSU owned devices is required when available.
- Data at Rest Encryption: All storage devices containing Restricted Information must be encrypted using full-disk encryption or file-level encryption with Approved Encryption Algorithms. Where technically feasible, full disk encryption is preferred.
- Data in Transit Encryption: All communication channels transmitting Restricted Information across networks must be secured using strong encryption protocols such as TLS 1.2 or higher. TLS 1.3 is strongly recommended where possible.
- Key Management: Encryption keys must be securely generated, stored and managed in accordance with SSU's Key Management Policy. Key rotation should be performed regularly, as defined in the Key Management Policy.
- Algorithm Selection: The Information Security team will maintain a list of Approved Encryption Algorithms. Any deviation from this list requires prior written approval from the Chief Information Officer (CISO). The approved algorithm list will be reviewed and updated annually, or more frequently as needed.
- Vulnerability Management: SSU will regularly monitor for, and address vulnerabilities related to encryption algorithms and implementations. This will include regular patching of encryption software and libraries.
- Prohibition of Circumvention: The use of encryption to circumvent established security processes and controls is strictly prohibited. This includes, but is not limited to, encrypting malware to bypass antivirus software, encrypting data to conceal unauthorized access or transfer, and using encryption to obscure malicious network traffic. Any attempt to circumvent security processes using encryption may constitute a violation of this policy. Any suspected circumvention will be investigated and reported to the CISO.

Any exceptions to this policy must be documented and approved in writing by the CISO.

Definitions

Confidential Information: Information that, if disclosed without authorization, could cause moderate harm to SSU, its partners or its constituents. This may include internal business plans, student information, financial data and employee information not classified as Restricted.

Restricted Information: Information that, if disclosed without authorization, could cause significant harm to SSU, its partners or its constituents. This includes Personally Identifiable Information (PII), payment card data and other sensitive data protected by law or regulation.

Encryption: The process of converting data into an unreadable format (ciphertext) to protect its confidentiality.

Approved Encryption Algorithms: Encryption algorithms that have been vetted and approved by SSU's Information Security team. These algorithms must meet or exceed industry best practices and relevant regulatory requirements. Examples of currently approved algorithms include AES-128 or higher, TLS 1.2 or higher, and other algorithms as approved by the Information Security team.

Data at Rest: Data stored on any storage device, including hard drives, USB drives, cloud storage and databases.

Data in Transit: Data being transmitted across a network, including internal networks, the internet and wireless connections.

Data in Use: Data actively being processed by a computer system. This includes data held in memory or cache.

Role ITS Security Team: Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented. They are also responsible for periodic security audits and penetration testing related to encryption.

ITS Staff: Ensure that confidential and restricted data is appropriately protected. Implement encryption policies and procedures in accordance with SSU standards.

Role

ITS Security Team: Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.

ITS Staff: Ensure that confidential and restricted data is appropriately protected. Implement encryption policies and procedures in accordance with SSU standards.

References CIS

3.6 Encrypt Data on End-User Devices
3.9 Encrypt Data on Removable Media
3.10 Encrypt Sensitive Data in Transit
3.11 Encrypt Sensitive Data at Rest
11.3 Protect Recovery Data

References PCI

PCI
Requirement 3: Protect Stored Cardholder Data
Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Additional References:
SSU Key Management Policy
SSU Data Classification Policy
SSU Incident Response Policy
MA 201 CMR 17:00 Section 17.15

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