Encryption

Standard number: DS-15
Date issued: 7/1/2018
Date last updated: 2/18/2022
Date last reviewed: 3/11/2025
Date of next review: 3/11/2027
Version: 1.1
Approval authority: Vice President for Information Technology and CIO
Responsible office: Information Assurance

This Standard supports and supplements the Information Security (SPG 601.27) policy. The Standard is mandatory and enforced in the same manner as the policy. It will be periodically reviewed and updated as necessary to meet emerging threats, changes in legal and regulatory requirements, and technological advances.

I. Overview

Encryption is the process of encoding information in order to protect the data, and can be applied to data that is stored (at-rest) or transmitted (in-transit) over networks. It reduces the risk of unauthorized access or disclosure, and may help mitigate financial, regulatory, reputational, and institutional risks to U-M related to loss or breach of unencrypted data.

Encryption should be used in conjunction with other data protection controls, such as access control, strong passwords, authentication, and authorization.

Federal or state regulations or contractual agreements may require additional actions that exceed those included in this Standard.

II. Scope

This standard applies to the Ann Arbor campus, Michigan Medicine, UM-Dearborn, UM-Flint, all affiliates, and all faculty, staff, workforce members, and sponsored affiliates. It further applies to:

- All units, faculty, principal investigators, and staff that process, maintain, transmit, or store data classified as **Restricted**, **High**, or **Moderate** on any university owned device, whether or not it is connected to the campus network and whether or not it is university or self-managed;
- Personally owned devices that have stored the above categories of data, in accordance with provisions of Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33);
- Any storage media that has been used to store **Restricted**, **High**, or **Moderate** digital or electronic university information or data;
- Any third-party provider with a contractual relationship with the university that maintains the same data types.

III. Standard

Where technically feasible, the university requires data classified as **Restricted** or **High** to be encrypted at rest or in transit, depending on storage location, type of device, or whether it is inside or outside the U-M network. See Tables 1 and 2 below. If data is unable to be encrypted for technical reasons, an appropriate set of compensating controls must be implemented.

Specifically, U-M requires the use of encryption technologies that meet NIST FIPS minimum requirements:

- Cryptographic modules validated under the Cryptographic Module Validation Program (CMVP) in accordance with NIST FIPS Publication 140-3 are approved for use by this Standard. When selecting a storage encryption technology, the university and its units should prioritize solutions that use existing system features (such as operating system features) and infrastructure.

Encrypting Data-at-Rest

Encryption at rest involves encrypting data when it is stored on a server or hard drive. There are two recognized methods for encrypting data-at-rest:

- **Full disk encryption, also called whole disk encryption,** encrypts the entire device or disk partitions at once; it provides good protection against data loss due to theft or other loss and requires less attention to how one handles files.
- **File-Level Encryption** encrypts individual files; There are two methods of file-level encryption:
  - When the file is decrypted only when it is in use, typically the case with application-based encryption.
  - When the file is not automatically re-encrypted when one is done viewing or editing it, as it the case with standalone encryption utilities.

Table 1. Encryption Requirements for Data-at-Rest by Location or Type of Device

Location or Device Type	Restricted	High	Moderate	Low
Data Centers	Recommended	Recommended	Recommended	Recommended
Machine Rooms	Required	Required	Recommended	Recommended
Portable and Removable Storage Media	Required	Required	Recommended	Recommended
Laptops (U-M owned)	Required	Required	Recommended	Recommended
Desktops (U-M owned)	Required	Recommended	Recommended	Recommended
Cloud Providers	Required	Required	Recommended	Recommended
Personally Owned Devices	Not Permitted	Required	Recommended	Recommended

1. **Data Centers:** Data stored on devices within U-M data centers is presumed to be protected from unauthorized access because of the physical security and physical access control provided within the data center.
2. **Portable and Removable Storage Media:** In general because of the risk of their being lost or stolen, portable media should only be used to store or backup Restricted, High, or Moderate

data when it is absolutely necessary to achieve a work-related purpose.

3. **Desktops:** Encrypting desktop devices is of lower priority than portable and removable storage devices because they are less likely to be lost or stolen.
4. **Personally Owned Devices:** Personally owned devices have a similar risk to portable devices and media with respect to being lost or stolen. All personally owned devices that process, maintain, transmit, or store U-M data must be in compliance with Security of Personally Owned Devices That Maintain Sensitive Institutional Data (SPG 601.33) in addition to any specific encryption requirements as identified in Table 1.
5. **Data Backups:** Backups that store Restricted and High data, including external hard drives and media, must be encrypted if not maintained in a protected U-M data center.

Encrypting Data-in-Transit

Malicious users may intercept or monitor unencrypted data when transmitted on untrusted networks, and gain unauthorized access that jeopardizes the confidentiality of sensitive institutional data.

Transmission	Restricted	High	Moderate	Low
Data transmitted within: • Ann Arbor campus (including Michigan Medicine) • Dearborn campus • Flint campus	Recommended	Recommended	Recommended	Recommended
Data transmitted between U-M campuses (not including between Ann Arbor campus and Michigan Medicine)	Required	Required	Recommended	Recommended

Transmission	Restricted	High	Moderate	Low
Data transmitted external to the Ann Arbor (including Michigan Medicine), Dearborn or Flint campuses (including cloud providers)	Required	Required	Recommended	Recommended

The following are examples of the most commonly employed technologies that provide encryption of data in transit.

1. **Virtual Private Network (VPN):** Users traveling on university business or who need to access the U-M network and any sensitive university data from a non-university or public network must use the U-M VPN (Virtual Private Network) which meets this standard. It also permits access to applications or data that require an on-campus connection.
2. **Secure Web Traffic:** HTTPS is a protocol that encrypts traffic between a web browser and a web based application.

Key Management

Units and individuals processing, maintaining, storing, or transmitting encrypted high and restricted data are required to ensure that a cryptographic key management plan is in place that protects the creation, use, distribution, storage, and recovery of cryptographic keys. Effective key management is critical to prevent unauthorized disclosure and to ensure access to data when needed. If a key is lost, it is likely that the data on the device cannot be recovered, particularly if there are no other copies of the data available.

The key to decrypt the file should be shared separately from the file via a different method of transmission.

Cryptographic keys are a type of IT security information classified as **High** data, and must themselves be encrypted while stored. Keys should be stored separately from encrypted data.

Data Encryption and Export Controls

Any export or import of encryption products must comply with the applicable laws and regulations of the countries involved, including those countries represented by foreign nationals affiliated with U-M. Faculty that conduct research that incorporates, develops, or uses data encryption software—

both mass market and custom-developed—must comply with two federal laws, International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). It is important to consult with the U-M export control officer prior to any international travel to confirm country-specific regulations.

IV. Violations and Sanctions

Violations of this Standard may result in disciplinary action up to and including suspension or revocation of computer accounts and access to networks, non-reappointment, discharge, dismissal, and/or legal action. In addition, the connectivity of machines and servers to the U-M network that do not comply with this Standard may be limited or disconnected.

Discipline (SPG 201.12) provides for staff member disciplinary procedures and sanctions. Violations of this policy by faculty may result in appropriate sanction or disciplinary action consistent with applicable university procedures. If dismissal or demotion of qualified faculty is proposed, the matter will be addressed in accordance with the procedures set forth in Regents Bylaw 5.09. In addition to U-M disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

Any U-M department or unit found to have violated this policy may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.

V. Implementation

Information Assurance is responsible for the implementation, maintenance, and interpretation of this Standard.

VI. References

- FIPS 140-3, Security Requirements for Cryptographic Modules, 2019
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, 2006
- NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices, 2007
- NIST Special Publication 800-57, Recommendation for Key Management, Part 1 and Part 2, 2019-2020

- NIST Special Publication 800-175b, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, 2020

VII. Related NIST Security Controls

- NIST SP 800-53 Revision 5:
  - AC-17 Remote Access
  - AC-18 (1) Wireless Access
  - AC-19 (5) Access Control for Wireless Devices
  - AU-9 (3) Protection of Audit Information
  - CM-3 (6) Configuration Change Control
  - IA-5 (1) Authenticator Management
  - IA-7 Cryptographic Module Authentication
  - MA-4 (4)(b)(2)(6) Nonlocal Maintenance
  - MP-5 (4) Media Transport
  - PE-4 Access Control for Transmission Media
  - SC-8 (1)(3)(4) Transmission Confidentiality and Integrity
  - SC-12 (1)(2)(3) Cryptographic Key Establishment and Management
  - SC-13 Cryptographic Protection
  - SC-28 (1) Protection of Information at Rest