# Third Party Vendor Security and Compliance

**Standard number:** DS-20
**Date issued:** 3/5/2018
**Date last updated:** 7/15/2025
**Date last reviewed:** 9/26/2025
**Date of next review:** 9/26/2027
**Version:** 2.2
**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. It will be periodically reviewed and updated as necessary to meet emerging threats, changes in legal and regulatory requirements, third party vendor environments, and technological advances.

## I. Overview

The use of external service providers can result in cost savings, efficiencies, greater security and compliance, stronger resiliency, and higher quality services. However, outsourcing IT services also creates risks for the university if the information assurance posture of the service providers is not adequately assessed and properly accounted for in a contract or agreement. Serious security incidents or data breaches that originate from a third party vendor still represent significant financial, regulatory, and reputational impacts on U-M.

In order to ensure that appropriate information assurance considerations are integrated into the procurement process, Information Assurance (IA), U-M Procurement Services, and the Office of the General Counsel (OGC) developed the vendor security risk management practices and processes underpinning this standard. Specifically, Procurement General Policies (SPG 507.01), Section VIII A, requires all university units engaging in acquisitions of, or contracting, for information technology or data goods and services to:

- Involve Procurement Services if the transaction includes providing access to sensitive institutional data classified as Restricted, High, or Moderate, including all data types regulated by federal or state law;
- Where mandated, include the U-M Data Security Agreement (DSA) as part of the contract;
- Where mandated, require the prospective vendor to undergo a privacy, security, and compliance assessment;
- Involve U-M Merchant Services if the transaction includes payment card information (PCI) and systems that process credit card transactions.

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. The scope encompasses all units and individuals who enter into contractual relationships on behalf of the university with third party vendors or contractors.

Specifically, this standard also applies to:

- Contracts, including research contracts or agreements, with a third party vendor that will establish a service on behalf of the university that will create, process, maintain, transmit, or store institutional data classified as **Restricted**, **High**, or **Moderate**;
- Transfers of any sensitive institutional data from a university-owned system or device to third party vendor contracted-for systems, applications, or devices (including cloud provider services and biomedical devices), where the vendor has operational control over data classified as **Restricted**, **High**, or **Moderate**.

# III. Definitions

- **Data Security Agreement (DSA)**
  The U-M data security agreement broadly defines IT security and compliance service provider roles,

responsibilities, and requirements related to the management and disclosure of U-M data.

- **Family Education Rights and Privacy Act (FERPA) Acknowledgment**
  The U-M FERPA Acknowledgement outlines the vendor's responsibilities under the Family Educational Rights and Privacy Act and confirms that the vendor agrees to act as a "School Official" when processing educational records.
- **Vendor Security Questionnaire**
  The Vendor Security Questionnaire is a standard set of questions used to assess a prospective service provider's IT security and compliance posture and its ability to satisfactorily protect institutional data throughout the lifecycle of its product or service. Additional or alternative vendor security risk questionnaires or security assessment tools may be used if vetted and approved by IA.
- **Business Associate Agreement (BAA) (PDF)**
  The U-M business associate agreement documents assurances from the service provider that it will not use or disclose Protected Health Information (PHI), except as permitted by law. To the extent the service provider maintains PHI in the Designated Record Set as defined by the Health Insurance Portability and Accountability Act (HIPAA), it will cooperate with Michigan Medicine to honor patient rights as mandated by the Privacy Rule.

# IV. Roles and Responsibilities

## Information Assurance (IA)

- Coordinate periodic review and update of DSA and vendor security and compliance assessment tools;
- Periodically review assessment process and maintain documentation related to it;
- Support and consult with units on data classification, vendor assessments and security reviews.

## U-M Procurement Services

- Maintain up-to-date versions of DSA, BAA, Vendor Security Questionnaire and other equivalent and approved vendor security assessment tools;
- Incorporate DSA into contracts/agreements;
- Provide Vendor Security Questionnaire or other vendor security assessment tool to vendor as required; serve as interface with vendor during assessment process;
- Coordinate document reviews with IA and OGC as needed.

## U-M Merchant Services

- Approve all contracts or purchases of credit card transaction services, software and/or equipment;

- Ensure that third party vendors maintain compliance with the PCI Data Security Standard for the life of the agreement.

## Office of the General Counsel

- Periodically participate in review and update of BAA and DSA documents;
- Review contracts, DSAs, and redlined or alternatives to DSAs on an as-needed basis.

### University Units

*Includes schools, colleges, institutes, departments, research centers, research projects, clinical environments*

- Determine data classification (with consultation from IA if needed) which in turn determines which components of the third party vendor assessment process are recommended or required.
- Abide by provisions of this standard and appropriately monitor third party vendors for compliance with DSA. The Security Unit Liaison (SUL) or an IT manager/director should primarily coordinate the service provider security and compliance review process on behalf of their unit.

# V. Standard

As part of its ongoing due diligence, U-M conducts risk management assessments of its third party relationships commensurate with the level of risk and complexity, including compliance and regulatory risks. Prior to establishing a contractual relationship with a vendor, U-M units must identify the data that will be shared with or accessed by the vendor and the appropriate data classification.

Vendors that have access to data classified as **Restricted** or **High,** or are providing higher-risk services, should receive the greatest scrutiny prior to formalizing a contractual relationship.

Vendors with access to data classified as **Moderate** are generally expected to agree to a DSA or its equivalent but are not required to complete the Vendor Security Questionnaire.

Lower risk relationships that involve data classified as **Low** do not require a security review or a DSA. The vendor assessment process based on data classification levels is summarized in Table 1.

## Table 1. Third Party Vendor Assessment Process Based on Data Classification Level

| Data Classification | DSA or equivalent required? | Vendor Security Questionnaire or equivalent required? | BAA required? | IA review required? | Can unit accept risk? |
|---|---|---|---|---|---|
| **Low** | Recommended | No | No | No | Yes |
| **Moderate** (excluding FERPA) | Yes* | No | No | Optional | Yes (with unit senior leadership signature) |
| **FERPA** | Yes (FERPA Acknowledgment) | No | No | Yes | No |
| **High** (excluding PHI) | Yes | Yes | No | Yes | No |
| **PHI** | Yes | Yes | Yes | Yes | No |
| **Restricted** | Yes | Yes | No | Yes | No |

* For Moderate data (excluding FERPA), U-M units and individuals should make every effort to obtain a signed DSA (or equivalent) by the vendor. If the vendor refuses to agree to a DSA, the unit can proceed with entering a contractual relationship only with unit senior leadership approval. For this purpose, senior leadership is defined as Dean, Associate Dean (or equivalent), or their designate. See more guidance at IT Security and Privacy in Vendor Contracts.

U-M units and individuals must adhere to the Third Party Vendor Security & Compliance process in all situations where U-M data is to be accessed by, or shared with, a third party vendor. Prospective vendors or U-M units are required to submit and/or agree to the documentation listed in Table 2.

## Table 2. Third Party Vendor Assessment and Contract Documentation

| Data Security Document | U-M Unit with Primary Responsibility | Description of Third Party Vendor Requirement |
|---|---|---|
| **Request for Third Party Vendor Data Protection** | U-M units | Required at the start of third party contracting process and when requesting IA data |

| Data Security Document | U-M Unit with Primary Responsibility | Description of Third Party Vendor Requirement |
|---|---|---|
| **Review** | | classification determination; or evaluation of alternative documentation from vendors |
| **Data Security Agreement** (or its equivalent) | Procurement Services | Required for all agreements and contracts where a vendor accesses, processes, or maintains any type of institutional data classified as **Restricted** or **High**; Recommended for data classified as **Moderate** (or unit can accept risk); not required for data classified as **Low** |
| **FERPA Acknowledgment** (or its equivalent) | Procurement Services | Required for all agreements and contracts that involve processing, maintaining, or storing FERPA data, unless a Data Security Agreement is already in place |
| **Vendor Security Questionnaire** (or its equivalent) | Procurement Services | Required to be completed prior to contract award or agreements with prospective vendors that will access, process, or maintain data classified as **Restricted** or **High** |
| **Business Associate Agreement** | Procurement Services and Michigan Medicine Corporate Compliance | Required for all agreements and contracts that involve processing, maintaining, or storing Protected Health Information (PHI) |
| **Payment Card Information Attestation of Compliance** | Merchant Services | Required annually from a Qualified Security Assessor (QSA) (or be listed as a Level 1 provider on VISA website) |

Software Procurement and Licensing Compliance (SPG 601.03-3) is the authoritative source for information assurance protections related to software purchased from third parties. This includes downloading of online tools (including plug-ins), SaaS subscriptions, and other software purchases made by accepting a click-through end user license agreement (EULA) and paid for with a U-M PCard. Although SPG 601.03-3 allows for limited delegated authority of faculty, staff, and U-M units to agree to EULAs, that authority does not extend to any software acquisition (freeware, open source, purchase) that will be used to access, process, or maintain data classified as **Restricted**, **High**, or **Moderate**.

Section IV.B.3 requires that software that will be used to access or maintain such data must be procured by a U-M IT service provider or through a school, college, or departmental purchase coordinated with U-M Procurement Services.

Units are encouraged to develop internal processes for reassessing third party vendors when there are significant changes to an existing vendor relationship, such as change in the type of data accessed by the vendor (e.g., data classifies as **Moderate** or **High**) or the type of services provided. Primary attention should be directed to vendors accessing data classified as **Restricted** or **High** or providing higher risk services.

The following U-M information security standards have additional third party vendor provisions that are incorporated by reference into this standard:

- Disaster Recovery Planning and Data Backup for Information Systems and Services (DS-12)
- Electronic Data Disposal and Media Sanitization (DS-11)
- Encryption (DS-15)
- Network Security (DS-14)
- Secure Coding and Application Security (DS-18)

### Incident Reporting

Third party vendors are required to report suspected security incidents to U-M, as well as meet all incident-related regulatory requirements based on the type of data involved. They must notify the university of a breach that potentially affects U-M data by following the timetable in Information Security Incident Reporting (SPG 601.25).

## VI. 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 devices 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.

# VII. Implementation

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

# VIII. References

- Procurement General Policies and Procedures (SPG 507.01)
- Software Procurement and Licensing Compliance (SPG 601.03-3)
- Third Party Vendor Security & Compliance
- Data Security Agreement (DSA)
- Business Associate Agreement (BAA)

# IX. Related NIST Security Controls

- NIST Risk Management Framework
  - PS-07 Third Party Personnel Security
  - SA-04 Acquisition Process
  - SA-09 External Information System Services
  - AC-20 Use of External Information Systems
  - IA-08 Identification and Authentication (Non-organizational users)