Sensitive Data Classification

INFORMATION ASSURANCE
UNIVERSITY OF MICHIGAN

Agenda

- Sensitive Data Classification
- Sensitive Data and U-M IT Standards
- Third Party Vendor Security Review Process

https://safecomputing.umich.edu

IA Mantras

- IT security and compliance are shared responsibilities
- IT security and compliance are never-ending journeys
- Do the right thing to the best of your ability
- Use common sense
- Think alignment, not compliance
- Ask for IA support

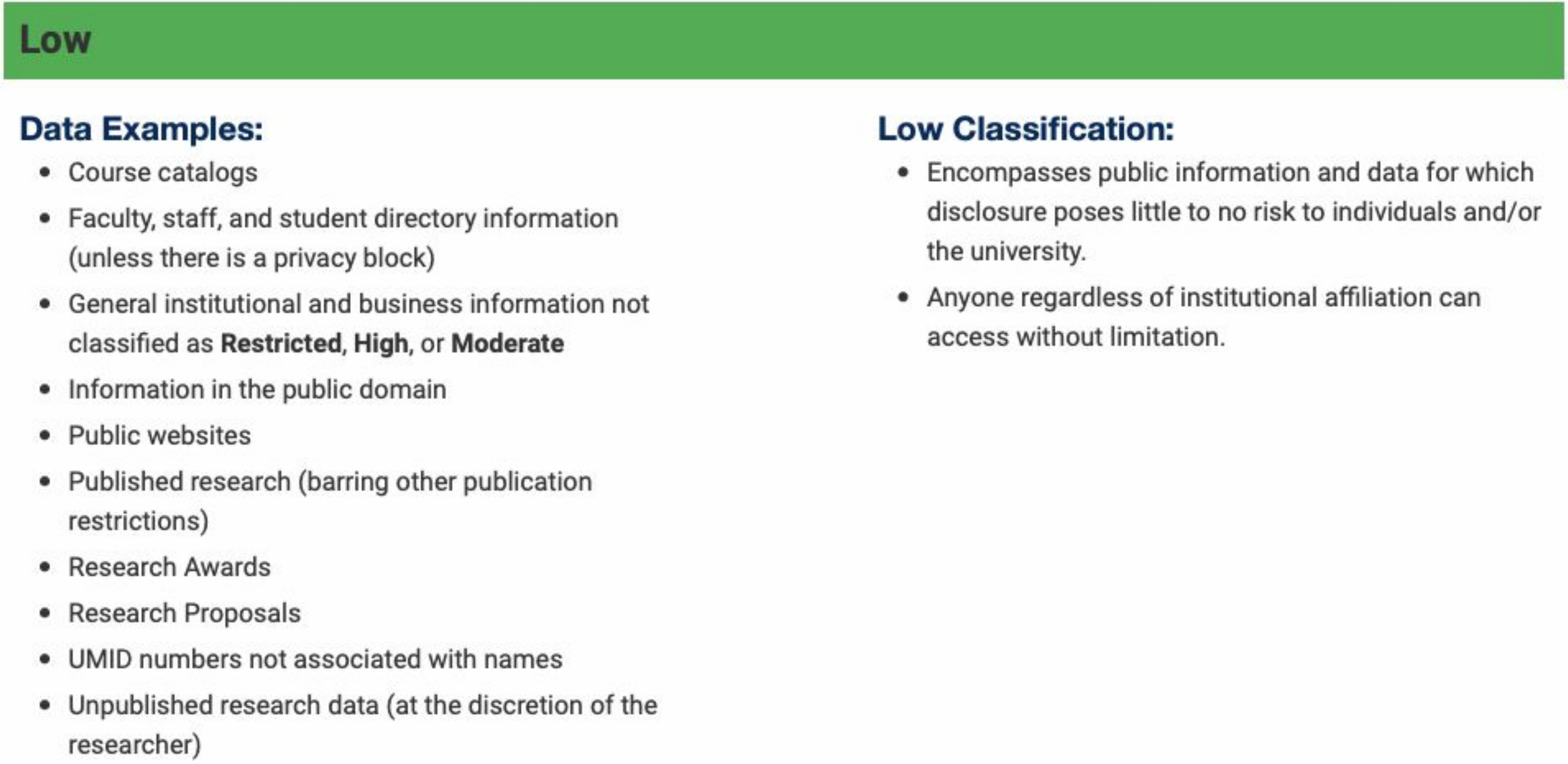
Incremental improvement is still improvement

Sensitive Data Classification

Sensitive Data must be protected to prevent theft, unauthorized access, compromise, and inappropriate use.

- U-M's data classification levels are designed to help Determine minimum security requirements
- U-M takes a risk-based approach to data protection
- Protection is driven by legal, regulatory, academic, Financial, and operational requirements.
- Classification seeks to balance protection of the Confidentiality, integrity, and availability of the data, While recognizing the need for collaboration and sharing of knowledge.

Data Classification Levels



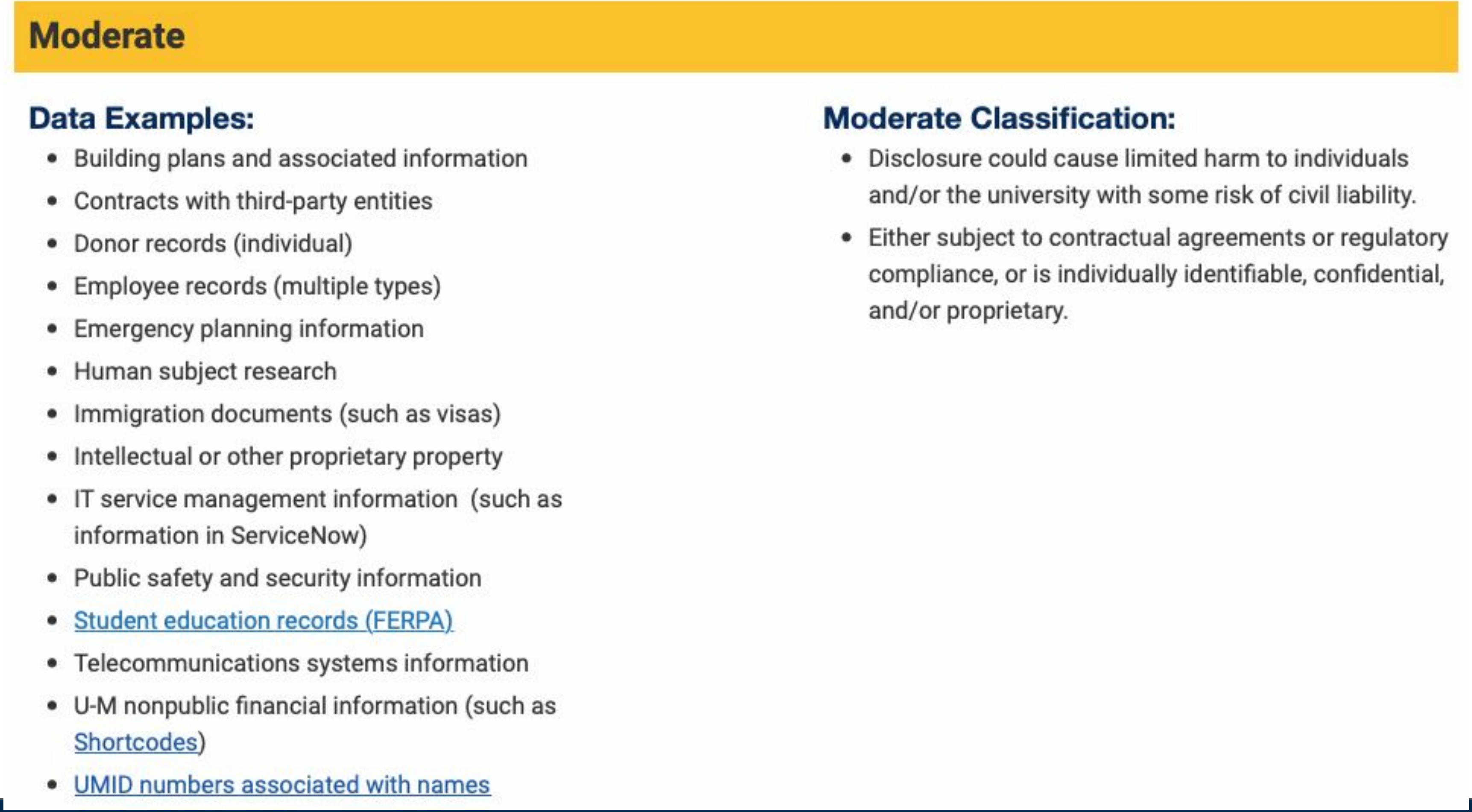
Low

Data Examples:

- Course catalogs
- Faculty, staff, and student directory information (unless there is a privacy block)
- General institutional and business information not classified as **Restricted**, **High**, or **Moderate**
- Information in the public domain
- Public websites
- Published research (barring other publication restrictions)
- Research Awards
- Research Proposals
- UMID numbers not associated with names
- Unpublished research data (at the discretion of the researcher)

Low Classification:

- Encompasses public information and data for which disclosure poses little to no risk to individuals and/or the university.
- Anyone regardless of institutional affiliation can access without limitation.



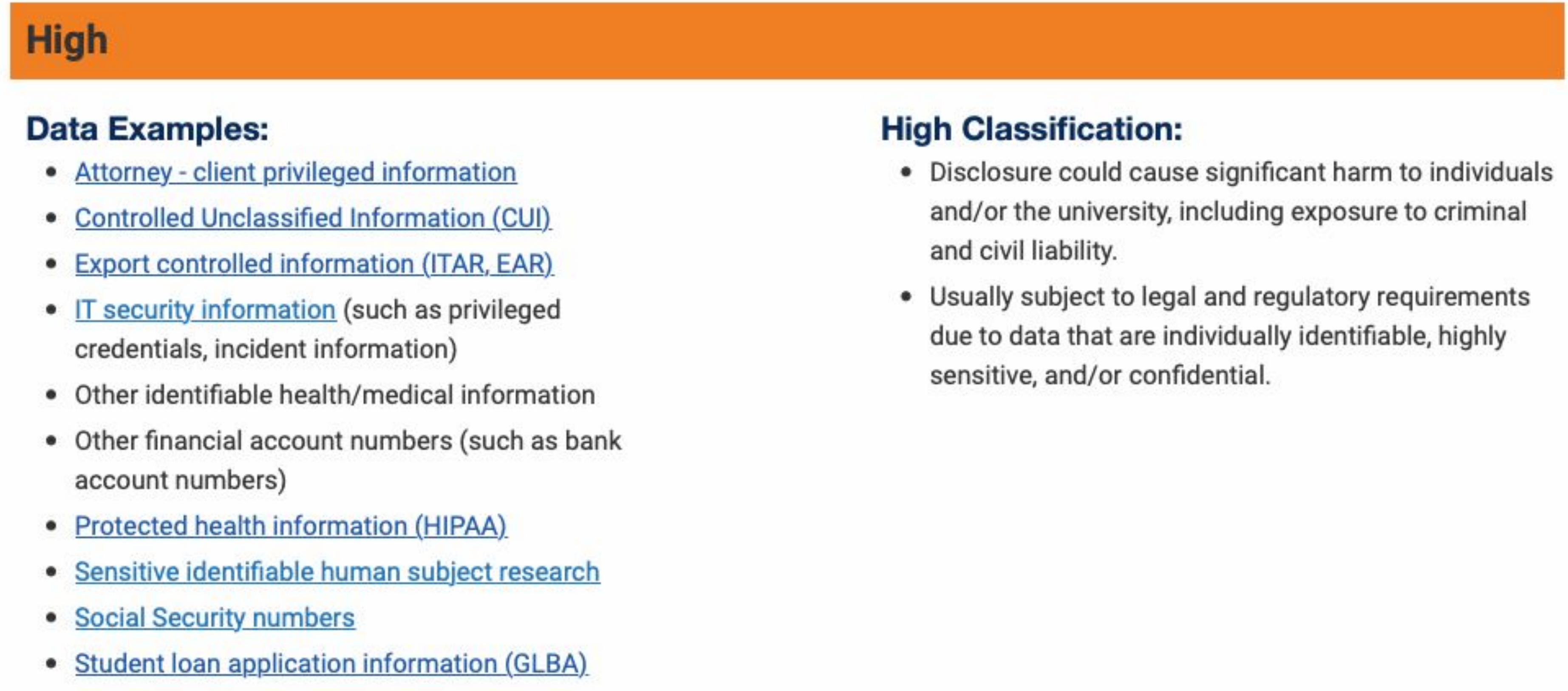
Moderate

Data Examples:

- Building plans and associated information
- Contracts with third-party entities
- Donor records (individual)
- Employee records (multiple types)
- Emergency planning information
- Human subject research
- Immigration documents (such as visas)
- Intellectual or other proprietary property
- IT service management information (such as information in ServiceNow)
- Public safety and security information
- Student education records (FERPA)
- Telecommunications systems information
- U-M nonpublic financial information (such as Shortcodes)
- UMID numbers associated with names

Moderate Classification:

- Disclosure could cause limited harm to individuals and/or the university with some risk of civil liability.
- Either subject to contractual agreements or regulatory compliance, or is individually identifiable, confidential, and/or proprietary.



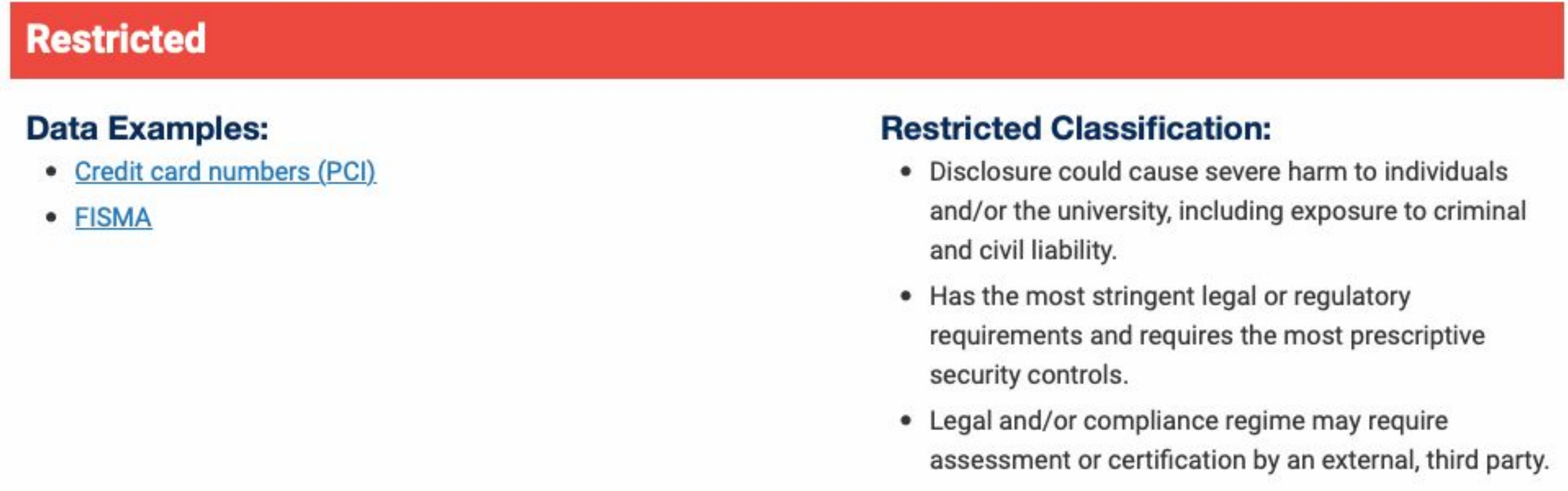
High

Data Examples:

- Attorney - client privileged information
- Controlled Unclassified Information (CUI)
- Export controlled information (ITAR, EAR)
- IT security information (such as privileged credentials, incident information)
- Other identifiable health/medical information
- Other financial account numbers (such as bank account numbers)
- Protected health information (HIPAA)
- Sensitive identifiable human subject research
- Social Security numbers
- Student loan application information (GLBA)

High Classification:

- Disclosure could cause significant harm to individuals and/or the university, including exposure to criminal and civil liability.
- Usually subject to legal and regulatory requirements due to data that are individually identifiable, highly sensitive, and/or confidential.



Restricted

Data Examples:

- Credit card numbers (PCI)
- FISMA

Restricted Classification:

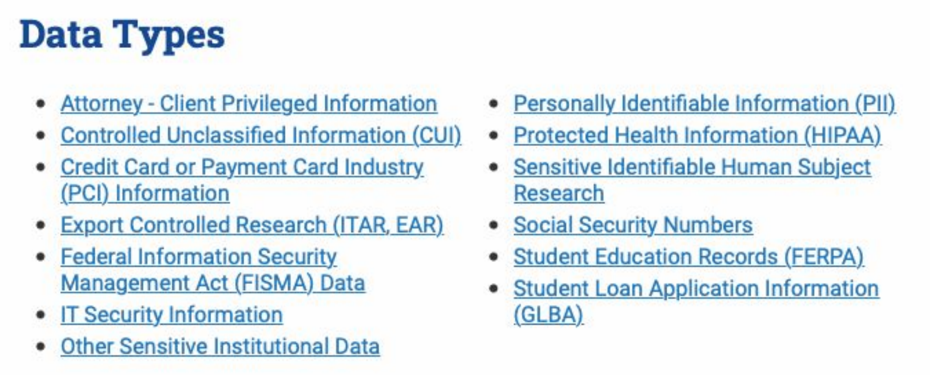
- Disclosure could cause severe harm to individuals and/or the university, including exposure to criminal and civil liability.
- Has the most stringent legal or regulatory requirements and requires the most prescriptive security controls.
- Legal and/or compliance regime may require assessment or certification by an external, third party.

Sensitive Data and IT Standards

HOW TO PROTECT YOUR SENSITIVE DATA

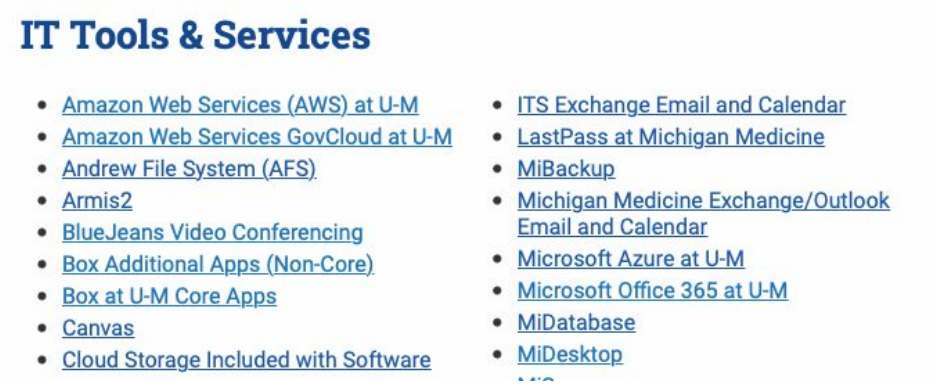
Sensitive Data Guide

- https://safecomputing.umich.edu/dataguide/
- Provide guidance to help make informed decisions about where to safely store and share university data. It is not intended to be a complete or comprehensive catalog of services available at U-M



Data Types

- Attorney - Client Privileged Information
- Controlled Unclassified Information (CUI)
- Credit Card or Payment Card Industry (PCI) Information
- Export Controlled Research (ITAR, EAR)
- Federal Information Security Management Act (FISMA) Data
- IT Security Information
- Other Sensitive Institutional Data
- Personally Identifiable Information (PII)
- Protected Health Information (HIPAA)
- Sensitive Identifiable Human Subject Research
- Social Security Numbers
- Student Education Records (FERPA)
- Student Loan Application Information (GLBA)

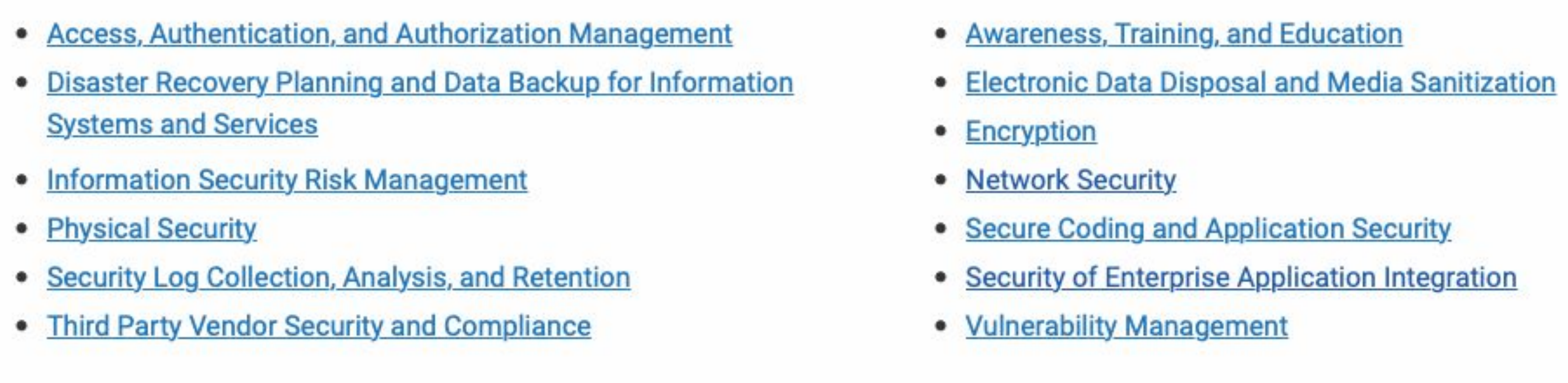


IT Tools & Services

- Amazon Web Services (AWS) at U-M
- Amazon Web Services GovCloud at U-M
- Andrew File System (AFS)
- Armis2
- BlueJeans Video Conferencing
- Box Additional Apps (Non-Core)
- Box at U-M Core Apps
- Canvas
- Cloud Storage Included with Software
- ITS Exchange Email and Calendar
- LastPass at Michigan Medicine
- MiBackup
- Michigan Medicine Exchange/Outlook Email and Calendar
- Microsoft Azure at U-M
- Microsoft Office 365 at U-M
- MiDatabase
- MiDesktop

Policies and Standards

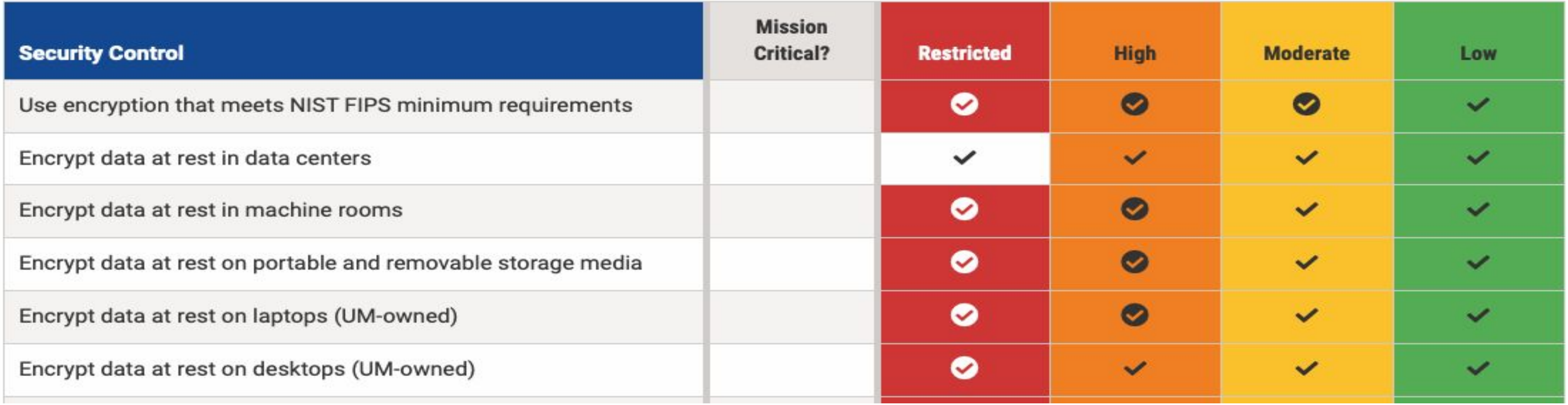
- U-M Information Security Policy (SPG 601.27)
- UM IT Security Standards
  - 13 Requirements organized by Standards



- Access, Authentication, and Authorization Management
- Disaster Recovery Planning and Data Backup for Information Systems and Services
- Information Security Risk Management
- Physical Security
- Security Log Collection, Analysis, and Retention
- Third Party Vendor Security and Compliance
- Awareness, Training, and Education
- Electronic Data Disposal and Media Sanitization
- Encryption
- Network Security
- Secure Coding and Application Security
- Security of Enterprise Application Integration
- Vulnerability Management

Minimum Security Requirements

- Minimum Security Requirements are available on Safe Computing
- Based on data sensitivity



Security Control	Mission Critical?	Restricted	High	Moderate	Low
Use encryption that meets NIST FIPS minimum requirements		✅	✅	✅	✓
Encrypt data at rest in data centers		✓	✓	✓	✓
Encrypt data at rest in machine rooms		✅	✅	✓	✓
Encrypt data at rest on portable and removable storage media		✅	✅	✓	✓
Encrypt data at rest on laptops (UM-owned)		✅	✅	✓	✓
Encrypt data at rest on desktops (UM-owned)		✅	✓	✓	✓

Third Party Vendor Security

- Any non-UM external service provider that transmits, stores, or processes university data is considered a third party vendor.

- Follow the Third Party Vendor Security and Compliance Standard (DS-20)
- Additional Guidance is available on Safe Computing

Third Party Vendor Security Overview

1. Engage Procurement Services if possible
2. Determine Data classification (consult with IA if needed)
3. Based on data classification, the following agreements may be needed -
    a. Data Protection Agreement (DPA) or equivalent
    b. FERPA Agreement
    c. Third Party Security Questionnaire (UMSPSCQ/BTAA or equivalent)
    d. Business Associate Agreement (BAA)

Current Vendor Assessment Process

Data Classification	DPA or equivalent required?	UMSPSCQ or equivalent required?	BAA required	IA review required?	Can unit accept risk?
LOW	Yes	No	No	No	No
MODERATE	Yes	No	No	Optional	No
MODERATE (FERPA)	Yes (FERPA Agreement)	No	No	Yes	No
HIGH	Yes	Yes	No	Yes	No
HIGH (HIPAA)	Yes	Yes	Yes	Yes	No
RESTRICTED	Yes	Yes	No	Yes	No

Proposed Assessment Process

Data Classification	DPA or equivalent required?	UMSPSCQ or equivalent required?	BAA required	IA review required?	Can unit accept risk?
LOW	No	No	No	No	Yes
MODERATE	Recommended	No	No	Optional	Yes (with signature)
MODERATE (FERPA)	Yes (FERPA Agreement)	No	No	Yes	No
HIGH	Yes	Yes	No	Yes	No
HIGH (HIPAA)	Yes	Yes	Yes	Yes	No
RESTRICTED	Yes	Yes	No	Yes	No

A Quick Word about Standards

- Think alignment not “compliance”
    - Remember, this is a *never-ending journey*

- Support materials
    - Safe Computing - Minimum Security Requirements
    - Safe Computing - Protect Your Unit’s IT
    - Standards Working Sessions Presentations/Recordings
    - Standards Working Group: likely establishing a formal working group to ensure continuous consideration of Standards
    - IA remains happy to do unit-level presentations

IA - Trying to Make InfoSec “Easier”*

*All since FY19 - does not include training opportunities

Work Item	Overview	Advantage
Riskonnect	BTAA shared environment for vendor security and compliance assessments	Standardizes assessments in BTAA; creates efficiencies by using each others’ assessments
RECON automation	Web-based tool that automatically fills in certain information	Automates parts of RECON assessment based on data type
DS-20 Revision	Listened to feedback based on existing vendor review practices which were incorporated in IT Security Standard	Will reduce vendor assessment and data protection addendum negotiation time
RISC team	Expanded unit security services (in-unit IA support) to entire campus	Expands IA in-unit presence to all school and colleges

Questions