FLORIDA
INTERNATIONAL
UNIVERSITY

Removable Media Standard

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
2/10/2026	2/10/2026	Division of Information Technology Information Security

PURPOSE

Preventing the use of removable media (USB drives, CDs, external hard drives) is crucial for preventing data theft and malware infection. This standard will define the responsibilities and rules around USB storage devices in relation to Level 3 – Confidential Data, as defined in the FIU Data Classification Standard.

Any department, business unit, or college that store, process, or transmit Level 3 - Confidential data is prohibited from using removable media on any information system handling Level 3 data. Exceptions may be granted for a documented business justification only by receiving written approval from the assigned Data Steward and the Division of Information Technology Security Office. All approved exceptions must be time-bound and are subject to annual review. Technical controls, including but not limited to Device Media Control mechanisms, must be implemented on endpoints confidential Level 3 data.

SCOPE AND AUTHORITY

This standard applies to all departments, units, and colleges that store, process, or transmit Level 3 – Confidential Data, as defined in the FIU Data Classification Standard. It applies to all university-owned or managed information systems that handle such data. This standard applies to all faculty, staff, students, contractors, third parties, and any persons of interest granted authorized access to covered systems or Level 3 - Confidential Data.

DEFINITIONS

TERM	DEFINITIONS
Authorized Removable Media Device	A removable media device that has been formally approved, institutionally managed, and configured in accordance with this standard, including required encryption and monitoring controls.

Data Exfiltration	The unauthorized transfer, copying, or removal of data from an institutional system or controlled environment.
Data Steward	All FIU employees, students and authorized users of IT data resources.
Data Owner	Any manager, director, division head or equivalent, who has accountability and responsibility for the integrity, accurate reporting and use of computerized data. This individual typically exists within the department that generated the data and is ultimately accountable for its accuracy and proper handling.
Device Media Control	Technical controls implemented at the endpoint or system level to block, restrict, monitor, or log the use of removable storage devices.
Endpoint	Any university-owned or managed workstation, laptop, server, or other computing device capable of having removable media connected to it.
Level 3 - Confidential Data	Institutional data classified under the FIU Data Classification Policy requiring the highest level of protection due to regulatory, contractual, privacy, or operational impact.
Managed Device	Any computing device (i.e. laptop, desktop, mobile device, server, or IoT endpoint) that is university-owned, controlled, configured, and secured by Division of Information Technology.
Regulated Data	Data subject to federal, state, local laws or other contractual protection requirements, including but not limited to FERPA, HIPAA, GLBA, or any other legally mandated safeguards.
Removable Media	Any portable digital storage device that can be attached to and removed from a computing device and used to store or transfer data. Examples include USB flash drives, external hard drives, solid-state drives (SSDs), SD cards, writable optical media, and similar devices.

ROLES AND RESPONSIBILITIES

Chief Information Security Officer (CISO)

- Approves and maintains this standard
- Defines institutional risk tolerance related to removable media
- Serves as final authority for high-risk or extended exceptions
- Accepts documented residual risk where appropriate
- Reports material risk posture to executive leadership

Division of Information Technology Security Office

- Implements and maintains Device Media Control mechanisms
- Establishes encryption and configuration standards on authorized removable media devices
- Reviews and approves exception requests
- Maintains an exception registry
- Monitors removable media activity
- Investigate violations and incidents
- Provides audit evidence and compliance reporting

Loss, theft, or suspected compromise of removable media containing institutional data must be reported immediately to the Division of IT Security Office and handled in accordance with the institutional Incident Response Plan.

All removable media must be sanitized or destroyed in accordance with FIU Media Sanitization Standard.

Department IT Administrator (ITA)

- Ensures endpoints are properly configured and managed
- Implements approved exceptions
- Verifies encryption and configuration standards
- Reports suspected misuse or compromise
- Supports audit and compliance activities

Department IT Administrators may not independently authorize removable media usage.

Data Owner

- Determines data classification
- Approves or denies business justification for exceptions
- Ensures risk impact is evaluated
- Reviews approved exceptions annually

Data Owner approval does not override institutional enforcement requirements.

System Owner

- Ensures systems under their authority enforce Device Media Control requirements
- Confirms compliance during periodic reviews
- Coordinates remediation of identified gaps

Data Steward (Authorized Users)

- Comply with all removable media restrictions

- Use only approved and encrypted devices
- Do not bypass security controls
- Immediately report lost, stolen, or compromised media

Failure to comply may result in disciplinary action in accordance with university policy.

Requirements for Approved Removable Media

1. Must have a minimum of AES-256 encryption
2. Must be an Information Technology Security Office approved USB device
3. Data must be accessed from a managed device.

Examples of Approved Removable Media

- Docking stations
- Encrypted USB thumb drive approved by the Division of Information Technology Security Office
- Keyboards
- Mice
- Presentation remote

Examples of Prohibited Removable Media

- Cell phones in USB storage mode
- CD/DVD drives
- External USB hard drives
- SD/microSD cards
- USB thumb drives
- Any USB storage media that allows reading or writing of files and folders

Resources

Data Classification Standard
Data Stewardship Policy
Incident Response Plan
Media Sanitization

CONTACTS
Division of Information Technology
IT Security Office
Florida International University

Security@fiu.edu

HISTORY

Initial Effective Date: 2/10/2026
Review Dates (review performed, no updates): N/A
Revision Dates (updates made to document): N/A