Office of Information Technology
777 Glades Road
Boca Raton, FL 33431
Tel: 561.297.3440
Fax: 561.297.3945
http://*www.fau.edu/oit*

Information Security Policies

These policies supplement IT policies defined under Section 12 of the University Policies and Procedures Manual. Authority for the development of these policies is granted by Policy 12.10 – Information Security Policies. Additional policies covering technology devices and data maintained by HIPAA-covered components at FAU are located at the University HIPAA Policies site.

IT-0001 Protecting Electronic University Data

Applicability and Scope

This policy applies to all electronic data maintained by the University or on University-owned or University-maintained equipment as defined in University Policy 12.7 – System and Data Classifications.

Policies

University-owned portable storage devices including portable hard drives and USB thumb drives may not be connected to personally owned devices if they contain Level 1 or Level 2 data.

Level 1 and Level 2 data may not be stored on publicly accessible systems including, but not limited to, third-party email systems, DMZ-protected servers, cloud services, or public file-sharing services without the review and approval of the Chief Information Security Officer (CISO).

Personally owned or unidentified portable storage devices including, but not limited to, USB thumb drives and portable hard drives may not be used on University-owned or University-maintained devices that house Level 1 or Level 2 information with the exception of limited instruction-related Level 2 information covered by FERPA.

Transmission of Level 1 or Level 2 information must be encrypted across the network utilizing high-strength encryption technologies as approved by the CISO.

Storage of Level 1 information on a desktop or portable device requires a full-disk encryption product approved by the CISO.

Transmission of Level 1 information through email communications is prohibited unless a specific exception exists that has been approved by the CISO. HIPAA-specific policies define exceptions covering HIPAA data in HIPAA-covered components of the University.

Storage of Level 1 or Level 2 information at cloud service providers must be approved and reviewed by the CISO prior to entering into any agreement or contract following University Policy 12.9 – Cloud Service Providers and approved by the respective data owners.

IT-0002 Patching Operating Systems and Firmware

Applicability and Scope

This policy applies to all University-owned systems. All administrators in charge of any University systems need to adhere to this policy.

Policies

General Policy

University-owned networked devices must be kept up to date on applicable security patches and must be running a supported operating system. These devices include, but are not limited to, computers, servers, phones, tablets, printers, network infrastructure equipment, building controllers, DVRs, networked lab equipment, and networked cameras.

Devices that are not up to date on relevant security patches and/or not running a supported operating system place sensitive University data and systems at risk even when the device in question is not sensitive or does not contain sensitive information. Devices that are out of data on relevant security patches or running unsupported operating systems are subject to immediate removal from the network.

Specific information and requirements for patching user devices and servers are provided below.

Windows Servers and Clients

Microsoft releases patches on the second Tuesday of every month, and sometimes more frequently, depending on the severity of the vulnerability that needs a patch.

FAU administrators will stay up to date on these latest issued patches and will actively **apply these**

patches within 7 to 10 days of the patches' initial release date. An administrator who encounters an issue with applying any patch will reach out to the Information Security department, Systems department, or appropriate support to resolve these issues in a timely manner.

These updates must come from our internal Systems Center Configuration Manager (SCCM) server that is maintained by the OIT systems group unless an exception has been approved. If a critical update is not readily available through SCCM, contact the OIT Systems group regarding the issue or enter a support ticket with the University Help Desk. A standalone installer may be used as an alternative if an update is not available through SCCM.

If multiple systems need patching, systems need to be prioritized based on the criticality of the system or sensitivity of information on the server.

If systems are not patched within the time frame listed above, these systems will be subject to immediate removal from the network until they are brought up to date with the latest patches or rebuilt.

Other Server and Client Operating Systems (e.g., Linux, Unix, macOS)

Vendors of operating systems other than Windows release security patches on an ongoing basis as they become available or on a specific schedule determined by the vendor.

FAU administrators who manage these systems must stay up to date on these latest issued patches and actively **apply these patches within 7 to 14 days of the patches' initial release date.** An administrator who encounters an issue with applying any patch will reach out to the Information Security department, Systems department, or appropriate support for assistance.

If multiple systems require patching, it is necessary to patch your systems containing the most sensitive information first.

If systems are not patched within the time frame listed above, these systems will be subject to immediate removal from the network until they are brought up to date with the latest patches.

Mobile Devices (e.g., Phones and Tablets)

Modern mobile devices will prompt users to install patches at regular intervals.

Phone and tablet operating systems must be kept up to date on any security patches released by the manufacturer, and users must update their devices within 7 to 14 days of patch availability.

Network Infrastructure Devices (Networking Equipment) (e.g., Switches, Routers, and Firewalls)

Networking equipment requires the application of firmware releases to address security vulnerabilities applicable to the device within 7 to 14 days of release. Due to the nature of network device configuration and deployment topologies, not all security patches are applicable. Security patch exemption will be evaluated by the CISO in coordination with the Director of Communication Infrastructure based on the applicability of the security patches, provided such devices are configured according to applicable published OIT configuration standards. Patch exemptions will be documented, including the patch release exempted, and the reason for the exemption.

IT-0004 Virtual Private Network (VPN) and Remote Access Policy

Applicability and Scope

This policy applies to all network devices and users of FAU's network resources.

Definitions

Virtual Private Network (VPN)

A VPN is a special network created between two devices through the help of special client and server software.

Remote Access VPN

A remote access VPN is a type of VPN that allows many users or devices to connect directly to a VPN server. Remote Access VPNs utilize client software programs installed on a user device to make a connection to the VPN server.

Site-to-Site VPN

A site-to-site VPN is a type of VPN that is used to bridge an entire remote network to a local network. These VPNs may be utilized to connect a remote network to the FAU network in cases where a collection of systems or devices reside in an off-campus location (such as a cloud service provider) and those devices need access to internal FAU resources.

Policies

Remote Access VPNs

Remote access VPNs hosted at FAU allow individual users outside of the University to connect to on-campus resources, bypassing some security controls while providing access to networked resources that are generally not available to users outside of the University.

Remote access VPNs may severely compromise the University network if they are not properly maintained or if access is improperly managed.

The following policies apply to remote access VPNs hosted at FAU:

- Any remote access VPN solution deployed on the FAU network must be maintained by the Information Security team and approved by the CISO.
- Full remote access to the FAU network via OIT-provided VPN services may only be granted to full-time AMP, SP, or Faculty with active pay, approved justification for access, and approval from their supervisor if necessary.
- OPS, temporary employees, students, adjunct faculty, vendors, and third parties are not permitted to have remote access to the FAU network using a remote access VPN.
- Departments are not permitted to set up their own remote access VPN services.
- All remote access VPNs require the use of two-factor authentication.
- Personal devices may be used to connect to FAU-provided VPNs if they meet security requirements as determined by the CISO.
- Limited exceptions to these policies may be made at the discretion of the CISO.

Remote access VPNs that are used to connect to entities or organizations outside of FAU, including privacy or consumer VPNs, may be utilized subject to the following restrictions:

- Devices on the FAU network are not allowed to connect to consumer VPN services typically used for privacy purposes.
- University-owned devices may be used to connect to other organizations or companies as long as such access is required for job-related duties. Such access may require technical exceptions to be implemented by the Information Security team before the access may work.
- Limited exceptions to these policies may be made at the discretion of the CISO or designee.

Site-to-Site VPNs

Site-to-site VPNs provide a secure tunnel between two networks. These are often used to provide communication privacy to hosts or services that are too dangerous to expose directly to users on the Internet. Because of this, unrestricted use of site-to-site VPNs presents a risk to FAU systems if their deployment and use are not controlled.

The following policies apply to site-to-site VPNs at FAU:

- Vendors and other third parties are not permitted to utilize site-to-site VPNs for the purposes of monitoring or remote access to FAU systems.
- Site-to-site VPNs must be managed by the Information Security team. Third-party termination equipment may not be used on the FAU network.
- All site-to-site VPNs will be subject to security restrictions, including firewall rules to enforce the principle of least-privilege access.
- Site-to-site VPNs are only permitted at the discretion of the CISO or designee.
- Limited exceptions to these policies may be made at the discretion of the CISO or designee.

IT-0006 IT Asset Inventory

Applicability and Scope

This policy applies to all University departments and units.

Definition

Physical IT Assets

Computing devices or hardware owned or maintained by the University that have a network or storage capability including, but not limited to, network routers, network switches, servers, desktop computers, tablets, cell phones, laptop computers, printers, networked video cameras, disk storage arrays, and digital signage.

Rationale

Properly assessing risks and mitigating risks to physical IT assets requires knowledge of those assets and their general location. Such risks include theft, cyberattack, data loss, and operational loss.

Policies

University units and departments are required to maintain a list of their physical IT assets that connect to the University network. Centralized management software may be used for this purpose, provided all assets are registered or otherwise covered through a manual inventory.

IT-0007 Mobile Device Management

Applicability and Scope

This policy applies to all mobile computing devices owned by the University including, but not limited to, smartphones, tablets, and laptops.

Policies

All mobile devices storing Level-1 health information as defined in University Policy 12.7 – System and Data Classifications must utilize mobile device management software compliant with the policies and procedures on the University HIPAA Website at https://www.fau.edu/hipaa.

OIT will evaluate and deploy policies for the protection of other data as appropriate. These policies will be reflected in this document once approved.

IT-0011 Security Event Logging

Applicability and Scope

This policy applies to all OIT systems providing security for, or authentication to, Level 1 and Level 2 information.

Policies

IT systems that provide authentication functions to Level 1 or Level 2 information will maintain authentication audit logs for a minimum of 30 days.

OIT systems that store Level 1 or Level 2 information will maintain access audit logs for a minimum of 30 days.

OIT system administrators are responsible for ensuring that audit logs are stored in a central location accessible by the members of the Information Security team.

The Information Security team will routinely monitor logs to detect anomalies.

The Information Security team will develop and deploy automated alerts as necessary to act on specific log conditions.