FAU™
FLORIDA
ATLANTIC
UNIVERSITY

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.

IS-POL-1 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 reviewed and approved by the CISO or designee prior to entering into any agreement or contract under University Policy 12.9 – Cloud Service Providers.

IS-POL-2 Patching and Vulnerability Management

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 or firmware. 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 regardless of the data stored or accessed by the device. 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.

Systems accessible from the Internet

Systems with Critical or High (CVSS Score of 7.0 or higher) must be patched within 24 hours of the availability of applicable patches. This policy supersedes any policy allowing a longer patch cycle.

Systems with Moderate or Low (CVSS Score below 7.0) must have patches applied within 14 days of release.

Server and Client Operating System Patches

Microsoft regularly releases patches on the second Tuesday of every month for Windows Operating Systems. Other vendors have varying patch cycles.

FAU administrators 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 to resolve these issues in a timely manner.

Updates for Windows-based operating systems must come from OIT-managed update solutions unless an exception has been approved. If a critical update is not readily available through OIT-managed update services, users may 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 OIT-managed update services.

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.

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.

Server Applications

Server applications with high or critical vulnerabilities (CVSS Score 7.0 or higher) must be patched within 14 days if the server is not accessible from the Internet. Server applications with critical or high vulnerabilities must be patched within 24 hours if the server is accessible from the Internet.

Server applications with moderate vulnerabilities (CVSS score between 4.0 and 7.0) must be patched within 30 days.

Desktop Applications

Desktop applications with critical vulnerabilities (CVSS 7.0 and higher) must be patched within 30 days.

Desktop applications with moderate vulnerabilities (CVSS between 4.0 and 7.0) must be patched within 90 days.

Unsupported Operating Systems and Firmware

Unsupported operating systems and applications may not be used on the FAU network.

Exceptions

Written exceptions to these policies may be made at the discretion of the CISO or designee.

At the discretion of the CISO or designee, some patches may be required to be deployed sooner than specified in these policies.

Maximum Remediation Time

At no time can remediation of Critical and High vulnerabilities in operating systems or server applications exceed 90 days.

Removal from the Network

The Information Security team may remove any system from the network that is running an unsupported operating system or firmware without notice.

The Information Security team may remove any system from the network that is in violation of other policies after consultation with the CISO or designee.

Notification by the Information Security team is not required prior to removal from the network.

In cases where removal is not due to an unsupported operating system or firmware, Information Security staff will make reasonable effort to notify the responsible administrators or managers of a system prior to disconnection provided the system is not accessible from the Internet and the system is not believed to be at high risk for compromise.

In all cases where a system is disconnected from the network for policy violations, the Information Security team will make reasonable efforts to notify the manager or administrator, if known, for a system in addition to the Network team.

IS-POL-3 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 resides in an off-campus location (such as a cloud service provider), and those devices need access to internal FAU resources.

Remote Monitoring and Management Tools (RMM)

RMM tools are used to allow a user to remotely connect to an on-campus system for remote management purposes.

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 and adjunct faculty may be granted basic access to the University VPN. However, such access needs to include a commitment from the user's management to promptly inform the Information Security team when access is no longer required.
- Students, 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.

Remote Monitoring and Management Tools (RMM Tools)

While RMM tools may be useful from a remote support or access standpoint, such tools allow the circumvention of University security policies and controls and are highly restricted on campus. RMM tools that connect to cloud services are not permitted for use in any network segment that contains servers or sensitive data storage.

Some tools may be permitted on desktop and wireless networks for the sole purposes of providing remote support for end user devices by the IT staff in colleges or the University Help Desk, or for providing monitored desktop sharing with vendors subject to the approval of the Information Security team.

RMM tools that connect to the cloud are subject to normal review processes including security reviews required for cloud service providers. Information Security may prohibit the use of certain tools.

The Information Security team will apply appropriate technical controls to prevent or limit the use of RMM tools on University networks.

IS-POL-4 IT Asset Inventory

Applicability and Scope

This policy applies to all University departments and units.

Definitions

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.

IS-POL-5 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.

IS-POL-6 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 be configured to 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.

IS-POL-7 Cloud Infrastructure

Applicability and Scope

This policy apples to the procurement and use of cloud infrastructure. Cloud infrastructure includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Policies

FAU departments, units, or colleges wishing to utilize cloud infrastructure services must obtain approval from the CIO or designee and the CISO or designee prior to the procurement or deployment of cloud infrastructure.

Cloud service providers are subject to review and approval through the processes defined in Policy 12.9 Cloud Service Providers.

Cloud infrastructure involving FAU staff or faculty maintaining their own virtual machines, virtual private servers, or other computer infrastructure must utilize a firewall approved and managed by the Information Security team to ensure appropriate controls are in place to comply with University obligations including applicable Federal, State, and Board of Governors regulations, policies, or laws.

To minimize costs to the University, it is recommended that departments maintaining their own cloud virtual machines, virtual private servers, or other computer infrastructure obtain services from cloud providers already approved by OIT that already have the necessary security controls deployed and necessary contract provisions in place.

IS-POL-8 Change Management and Approval

Applicability and Scope

This policy applies to non-routine changes made to OIT-managed systems or services.

Policies

OIT will operate a change approval board to manage non-routine changes to OIT-managed systems and services.

This board will be co-chaired by the Associate Director for User Services and the CISO.

Operations of the board, including change categories, change processes, and approval procedures, will be documented in a separate charter and regularly reviewed and updated.

IS-POL-9 Vulnerability Scanning

Applicability and Scope

This policy applies to all University departments and units.

Policies

The Information Security team is authorized to scan all devices connected to the University network for vulnerabilities as a part of their Security team responsibilities.

The Information Security team will perform routine vulnerability scans of the university network.

University-owned devices must not be configured to explicitly block automated scanning from the Information Security team.

University-owned devices must be configured appropriately upon request of the CISO to allow credentialed vulnerability scans performed by the Information Security team unless a written exception is granted by the CISO.

Users outside of the Information Security team may only scan for vulnerabilities on devices under their control or management as indicated in University Policy 12.2 – Acceptable Use of Technology Resources.

Information Security staff will take reasonable measures to ensure vulnerability scanning servers are only accessible to members of the Information Security team and their devices.

Departments may request that the Information Security team deliver automated vulnerability reports for their systems on a weekly basis if available vulnerability scanning resources allow.

Remediation of identified vulnerabilities are subject to the remediation timelines defined in IS-POL-2 Patching and Vulnerability Management.

Vulnerability scanning activities by the Information Security team is not a substitute for system administrators keeping their devices up to date on security patches.

IS-POL-10 Cyber-Threat Intelligence Review

Applicability and Scope

This policy applies to the CISO, ISSM, designee(s), and any individual tasked with overseeing the security of research projects, or University servers housing Level 1 or Level 2 information (appropriate personnel).

Policies

Appropriate personnel will regularly review basic cyber threat intelligence (CTI) as part of their daily responsibilities. Some examples of CTI sources include the following:

- Social media posts from security researchers and organizations
- Emailed vulnerability announcements from vendors and security organizations
- Website posts from vendors and security organizations

The CISO will provide guidance as needed as to sources of CTI that should be monitored.

IS-POL-11 Risk Assessments

Applicability and Scope

This policy applies to risk assessments performed to assess the security of FAU's IT security controls, processes, and procedures.

Policies

The CISO or designee will routinely perform risk assessments to determine overall risks, risk exposure, or compliance issues related to the security of FAU IT assets, data, and networks.

OIT will endeavor to contract or assist with a risk assessment, penetration test, or audit with an external vendor on an annual basis subject to availability of funds or other necessary resources.

Risk assessments will be performed using the NIST CSF as the base framework for the assessment.

University departments, units, or colleges contracting IT risk assessments from outside vendors or providers must coordinate with the CISO or designee to ensure accurate information is provided regarding the security posture of the University. This ensures that the risk assessment will provide actionable recommendations for improvements to the security posture of the University, and that sensitive University information is not improperly disclosed to the assessment team.

IS-POL-12 Incident Response

Applicability and Scope

This policy applies to the management of the University's Information Security Program.

Policies

The CISO will maintain a Security Incident Response Plan (SIRP) for the University.

The SIRP will contain the following elements:

- Contact info for key personnel
- Contact info for key organizations and vendors
- Basic incident response procedures
- A process for incorporating lessons learned into improvements to the SIRP and Information Security Program

The SIRP will be treated as confidential information due to details regarding incident response procedures.

The CISO will routinely update the SIRP to address new threats to the University and updated procedures.

IS-POL-13 Network Segmentation

Applicability and Scope

This policy applies to all networks deployed at FAU.

Policy

Networks deployed at FAU will be segmented as appropriate to meet the security, regulatory, legal, and compliance requirements of the University. Specific policies governing how networks are segmented will be maintained via internal Information Security Operating Policies.

The Information Security and Networking teams will review all requests to implement new networks at FAU and will ensure that such networks meet current security and operational requirements as determined by the Information Security and Networking teams.

The Information Security team will regularly assess the current network segmentation strategy and plan any necessary changes or improvements in response to risk and risk tolerance.

IS-POL-14 Capacity Planning

Applicability and Scope

This policy applies to all users procuring or otherwise deploying security hardware on behalf of the University.

Policies

All security hardware purchased by the University must be sized appropriately to handle anticipated traffic for the expected life of the device. This sizing must cover a period of 3 years at minimum.

The Information Security team will review proposed hardware purchases to ensure that devices are sized appropriately during their regular review and approval process for such devices.

IS-POL-15 Security Fault-Tolerance

Applicability and Scope

This policy applies to all users managing security access infrastructure at the University.

Definitions

Fail-Open

Fail-open is a configuration mode where a security device or service allows access without assessing security because the device or service has failed.

Fail-Closed

Fail-closed is a configuration mode where a security device or service denies all access because security cannot be reasonably assessed due to device or service failure.

Security Access Infrastructure

Security access infrastructure is services and devices intended to authenticate users or restrict network access.

Policies

Where practical and resources allow, security access infrastructure will be designed and implemented in a fault-tolerant fashion that limits the impact of device or service failure.

When security infrastructure provides a choice between fail-closed and fail-open configurations, fail-closed will be used unless a written exception is granted by the CISO or designee.

IS-POL-16 Reporting Security Incidents

Applicability and Scope

This policy applies to all users of University technology resources.

Definitions

Security Incident

Any attempted or actual unauthorized access, use, disclosure, modification, or destruction of University information or information systems.

Serious Security Incident

An activity or occurrence that leads to the actual compromise of a University system or information. This includes accidental disclose of sensitive information.

Policies

FAU does not operate a bug bounty program.

If an incident poses immediate danger to health or safety, immediately contact the FAU Police Department at 561-297-3500.

Security incidents should be reported to the Information Security team via email at security@fau.edu or via phone at 561-297-3440.

Sensitive information must not be sent to the Information Security team via email. If sensitive information needs to be provided or discussed, the Information Security team will provide a method for receiving the information upon request.

When reporting a security incident, please provide the following information, if applicable:

- Your name
- Your department
- Your email address
- You telephone number
- Date and time the incident was noticed
- Description of the security incident
- Impact, if known

The Information Security team will triage information received and determine if the University Incident Response plan needs to be activated or if the incident may require referral to the Office of General Counsel for any appropriate notification or third-party involvement obligations.

IS-POL-17 Encryption Standards

Applicability and Scope

This policy applies to all systems and services used to transmit or store University data of any classification level.

Policies

All newly procured or deployed systems or services transmitting University data must utilize encryption standards or technologies approved by the CISO or designee. OIT will maintain a standard defining currently acceptable encryption technologies and protocols. Encryption technologies other than those defined in the standard may not be utilized unless an exception is approved in writing by the CISO or designee.

Existing services or systems utilizing encryption technologies that are not approved for use will be given a remediation timeline to bring the system or service into compliance whenever the standard is updated. Some existing services and systems may be grandfathered in for a period if the encryption technologies in use are deemed sufficient by the CISO or designee.

Systems that are required to encrypt data at rest will be required to utilize encryption standards or technologies approved by the CISO or designee. OIT will maintain a standard defining currently acceptable encryption technologies and protocols.

The current approved encryption standard will be available on the FAU OIT Security website.