IT Security Plan

Table of Contents

Purpose

The purpose of this document is to serve as high level security guideline for securing network and endpoint devices at Florida International University (FIU). This document provides an overview of the security requirements and describes some of the controls in place, roles, and responsibilities.

Scope

This document describes the security controls, guidelines, and tools required to secure the FIU network and the managed devices connected to the FIU network. These are set forth in order to support the confidentiality, integrity, and availability of the systems FIU owns and manages. It also provides information regarding some of the services offered to our users. This document references the controls and tools which the Division of IT either uses or provides to FIU users for their manage devices. Each individual department must have their own internal process and procedures as to how they follow the FIU security polices and guidelines.

Security Controls

Network:

FIU operates an enterprise and a dedicated research network which connects to Internet 2 and Florida Lamda Rail (FLR). All network devices are connected on a private management network VLAN where Access Control Lists (ACL's) and restrictions are applied. Configurations are tested and vetted prior to being deployed into production. Standard configuration policies which are reviewed on an annual basis are applied based on pre-configured templates using network configuration tools. TACACS is used for user access and authentication. Virtual Local Area Networks (VLANs) are configured throughout the network for network segmentation. VLANs are used to segment various types of network devices such as voice, facilities, IoT, data centers, management, etc.

Wireless LAN Security:

FIU users should use the FIU Secure Wireless which is configured to use WPA2 with 802.1x for authentication. We also offer the EDUROAM SSID for EDUROAM members, this SSID is also configured to use WPA2 with 802.1x. Mac Filtering is utilized for devices which don't support 802.1x. Guest access is on a separate restricted vlan with limited ports and bandwidth.

Security:

Remote VPN access is allowed using the enterprise VPN. Two factor authentication is required for all VPN users. VPN access is managed by Active Directory Groups.

Next generation firewalls and IPS are configured and deployed in strategic/critical parts of the network. These devices are centrally managed and configurations are reviewed periodically. Perimeter anti-malware and anti-spam tools are in place and configured. URL filters are also in place but only configured to filter malicious URLs.

Two Factor Authentication:

Two factor authentication is available for all faculty, staff, and students at FIU. For more information regarding two factor visit https://fiu.service-now.com/sp?id=kb_article&sys_id=81f1943edb0c3200ff70785e0f9619cc

Identity Management:

Accounts are provisioned for faculty, staff, and students through a centralized process. Role based access is granted depending on the system being accessed. Passwords must meet the minimum requirements which are documented. Password Information can be found at https://fiu.service-now.com/sp?id=kb_article&sys_id=0e57be03db53e600ff70785e0f961917.

Host Security:

Managed hosts joined to the Active Directory Domain are required to have the host security tools which include, anti-virus, host data loss prevention, whole disk encryption, and host intrusion prevention. These tools are pushed to the hosts via GPO polices once they are joined to the active directory domain. Host firewalls are configured via GPOs. Hosts are patched using SCCM.

Vulnerability Management:

Vulnerability scans are performed on a regular basis to all endpoints connected to the FIU network. Vulnerability reports are shared with the various IT administrators for corrective action. Follow-ups and rescan are performed.

Patch Management:

SCCM is used for all managed windows workstations. JAMF and patch my PC are used to patch mac and third party applications. Notification of missing patches is done via the vulnerability reports, notifications, or assessments.

Log Management:

Central log management servers are used to collect logs from network and security devices. These logs can be correlated using a SIEM. Logs are kept for period of 6 months. Logs at a minimum must include: time stamp, source IP, destination IP, source port, and destination port.

Media Sanitation:

Media Sanitation guideline https://security.fiu.edu/uploads/docs/Media-Sanitation-Guideline.pdf

User Training and Awareness:

All faculty and staff are required to take the annual cyber security awareness training. For more information visit https://security.fiu.edu/awareness_training

The IT Security Office offers in person cyber security sessions during the month of October as part of the National Cyber Security Awareness month.

Other trainings for compliance or regulatory requirements such as HIPAA, PCI, CUI, GDPR, and FERPA are also offered to faculty and staff.

Backup Strategy:

Server backups take place daily for incremental and weekly, monthly, quarterly and annually for full backups. Backups are maintained for 30 days.
Network device backups take place daily for incremental and weekly, monthly, quarterly and annually for full backups.
The Division of IT offers an online storage tool designed to backup files. All FIU faculty and staff have the ability to install this tool on their FIU owned computers. https://fiu.service-now.com/sp?id=kb_article&sys_id=ba098260dbd3ee4019f173921f961912

Disaster Recovery and Business Continuity:

FIU has a disaster recovery site where critical services are replicated and maintained in an active configuration. The Division of IT performs disaster recovery tests twice a year for critical systems. These tests are documented. Some applications and services are hosted in online cloud environments such as AWS and AZURE which are part of our disaster recovery plan. The Department of Emergency Management offers a tool to assist every department create a plan; https://dem.fiu.edu/resources/fiu-ready/. All units within the university are required to have disaster recovery and business continuity plan. Table top exercises are performed on a regular basis to test the disaster recovery plans. Along with the process and procedures, the Division of IT has a fulltime resource dedicated to business continuity.

Change Management:

The Division of IT has established a change management board where all changes affecting users such as outages and upgrades must be submitted and approved prior to taking place. The board meets once a week to review the submitted change request at which time it can question the changes, deny, or approve the change. All board meetings are documented. The board is made up of individuals from all of the various Division of IT units.

Incident Response:

FIU has an enterprise Incident Response Plan (https://security.fiu.edu/uploads/docs/Incident-Response-Plan.pdf) which will be activated in the event of a major incident or breach. The Division of IT has performed a table top exercise using this plan. The Incident Response plan is reviewed annually.

Risk Assessments:

Internal Security Risk Assessments are performed by the IT Security Office for various departments at the University. External risk assessments are performed as well by third party vendors which are hired to perform these assessments for compliance or regulatory requirements.

Policies and Procedures:

FIU's IT Security policies and procedures are posted online in the Policies repository site. New policies are deiminated to users using a tool managed by the Office of Compliance. All University policies are located at https://policies.fiu.edu/.

Policies

1110.002 Address Validation in Connection w/Covered Accounts Offered or Maintained by FIU
1930.005 Applications Software Resources: Purchasing, Licensing & Use
175.150 Digital Communications Standards Policy
1930.015 Gramm-Leach-Bliley Act: Safeguards to Protect Confidential Financial Information
2370.521 HIPAA & RESEARCH: CERTIFICATION FOR RESEARCH USING DECEDENT PROTECTED HEALTH INFORMATION
2370.510 HIPAA & RESEARCH: CERTIFICATION OF REVIEW PREPARATORY TO RESEARCH
1640.010 HIPAA PRIVACY AND SECURITY: REQUIRED EDUCATION OF COVERED WORKFORCE
1610.010 HIPAA PRIVACY AND SECURITY: RESPONSIBILITIES OF UNIVERSITY IT SECURITY OFFICER AND HIPAA SECURITY ADMINISTRATORS
1670.005 HIPAA SECURITY: ACCESS CONTROLS TO SYSTEMS CONTAINING ELECTRONIC PROTECTED HEALTH INFORMATION
1670.010 HIPAA SECURITY: ACCESS TO FACILITIES HOUSING ELECTRONIC PROTECTED HEALTH INFORMATION
1670.015 HIPAA SECURITY: AUTHENTICATION AND AUDIT CONTROLS FOR ELECTRONIC PROTECTED HEALTH INFORMATION
1670.020 HIPAA SECURITY: DUTY TO REPORT SECURITY INCIDENTS INVOLVING PROTECTED HEALTH INFORMATION
1670.025 HIPAA SECURITY: INFORMATION ACCESS MANAGEMENT FOR ELECTRONIC PROTECTED HEALTH INFORMATION
1670.030 HIPAA SECURITY: INVENTORY OF HARDWARE AND SOFTWARE CONTAINING ELECTRONIC PROTECTED HEALTH INFORMATION
1670.055 HIPAA SECURITY: WORKFORCE SECURITY REGARDING PROTECTED HEALTH INFORMATION
1930.021 Incident Response Plan

1930.020 Information Technology Security
1760.127 Information Technology Security (SEIU)
1110.025 Payment Card Processing
1110.032 Preventing Identity Theft on Covered Accounts Offered or Maintained by FIU
1910.005 Responsibilities for FIU Network and/or System Administrators
1610.010 Responsibilities of University IT Security Officer and HIPAA Security Administrators
1670.045 Technical Security Measures for the Transmission of Electronic Protected Health Information
1910.010 University Wireless Network Infrastructure
1670.050 Use and Security of Workstations with Access to Electronic Protected Health Information

Procedures

- 1930.020a Data Stewardship
- 1640.005(a) HIPAA PRIVACY AND SECURITY: FAXING PROTECTED HEALTH INFORMATION: STEPS TO MINIMIZE PRIVACY RISKS
- 1930.020b IT Security Procedure: Sharing Access To IT Resources; Password Management
- 1930.020c IT Security Procedure: System and Application Management