Network Security High Level Process

Parent Policy: Information Security

Associated Policies: Technology Resource Appropriate Use

Associated High Level Process: Information Security

Contents

1. Scope and Purpose.................................................................................................................................1
2. Process and Procedure..........................................................................................................................1
   2.1 Network Access ..............................................................................................................................2
   2.2 Network Management ....................................................................................................................3
   2.3 Server Management ........................................................................................................................4
   2.4 User System Management .............................................................................................................4
3. Applicable Roles, Responsibilities, and Skills .....................................................................................4
4. Measurement and Metrics ....................................................................................................................5
5. Continual Improvement .........................................................................................................................5
6. Resources ................................................................................................................................................5

1. Scope and Purpose

This high level process primarily supports and enables the Information Security Policy and the Technology Resource Appropriate Use Policy. The network assets and resources work to preserve the integrity and availability of the data stored on the University's computing systems, prevent unauthorized access to confidential or private information to the greatest extent possible, and deliver services and information.

The network assets and resources include network devices, wired and wireless networks and equipment, intrusion detection servers, User systems connecting to the network, and the management of User and account authentication, and network access control. (See the glossary (in the knowledge base) for the definition of terms used in this document).

2. Process and Procedure

• The University (USF) Information Technology and Services Department (ITS) will implement and apply reasonable security safeguards practices and procedures to protect the network and infrastructure asset as well as the data and information the network accesses, processes, or transmits. The practices will be aligned to an authoritative information security standard framework, (e.g. ISO, NIST, PCI, SANS-CIS, etc.) to comply with Federal, State, and local laws and regulations. ITS will collaborate with designated information stewards, asset owners, Schools, Colleges, and Departments, to implement the safeguards using a risk-based approach.
The following process requirements apply to all three asset categories - infrastructure, applications, and endpoints. (The italicized text indicates the active response that USF ITS utilizes to satisfy the requirements. The internal Standard Operating Procedures (SOP) are ITS access only.)

2.1 Network Access

1. Access to both the wired and wireless network is restricted to authorized Users whose access is managed via an authentication process.
   a. Access to the Campus wired network is authenticated by checking for a valid username and password.

   

   **ITS follows an internal SOP to authenticate Users before granting access.**

   b. Access to the Campus wireless network is authenticated the same way as wired access but with the addition of requiring the computer or wireless device to be registered with ITS first before full network access is provided. See [How Do I?](#) article to register a wireless devices.

   

   **ITS follows an internal SOP to register a User's computers and other wireless devices requesting access, and then authenticate the device and User when accessing the network.**

   c. Access to the visitor or guest wireless network requires a User to register using an (non-USF) email address. It does not require the creation of a password in the USF access management system. The guest network provides limited functionality and connectivity. See [How Do I?](#) article on how to access the guest wireless network.

   

   **ITS follows an internal SOP to first register and then allow guests and visitors to only access the guest network. Access to Campus network resources is denied.**

2. All access to the USF network, i.e. wired, wireless, campus, or guest, must be done from an approved ITS-managed access point, such as USF provided wired Ethernet ports, wireless access points (WAP), and other approved connection points. Other means of wired or wireless access are prohibited.

   

   **ITS follows an internal SOP to search for and disable rogue, non-ITS approved and unauthorized wireless access points, and unsecured fax/inward-dial telephone lines.**

3. The wireless network supplements the wired network for use by portable electronic devices. It is not intended to be a User's sole connection means to the USF network or IT resources, nor does it provide the same bandwidth capacity. Inappropriate use of the wireless network is prohibited. See [Technology Resource Appropriate Use Policy](#).

4. The University will monitor network usage, and retain, and protect log files for analysis.

   

   **ITS follows an internal SOP to monitor network traffic, usage, and manage and protect the log files recording access and network events. The log files are provided for internal analysis.**
5. When network access is no longer needed it will be revoked or removed. Access may also be temporarily revoked or suspended for violations of policy.

   **ITS follows an internal SOP to suspend or revoke network access for a User when informed of and in response to policy violations, and fully remove access when it is no longer needed.**

6. Login accounts to network assets must be limited to only authorized ITS personnel whose actions are logged and tracked.

   **ITS follows an internal SOP to limit access to only authorized ITS personnel identified by their job role and function. Access events are recorded in protected log files for internal analysis.**

7. See the [Standards](#) (in the [knowledge base](#)) for the description of security standards applied at USF.

### 2.2 Network Management

1. All University facilities either owned or leased containing network assets that support and enable the network (e.g. in wiring closets, in classrooms, in the data center) must be secured and protected from unauthorized physical access, with access limited to authorized personnel using suitable keys and/or door badges.

   **ITS follows an internal SOP to secure physical assets and limit access to only authorized ITS personnel identified by their job role and function. Access events are recorded in protected log files for internal analysis. The SOP includes the process for approving ITS staff access, regular reviewing of this, and revocation as needed.**

2. ITS must be involved prior to and when network equipment is connected to the network. ITS is the primary Division allowed to connect network equipment or modify the network.

   **ITS follows an internal SOP to ensure only authorized ITS staff connect equipment to the network. Any non-ITS connected equipment will be removed as a policy violation.**

3. All network assets must be inventoried and configured to secure the asset and traffic that is transmitted and managed by it.

   **ITS follows an internal SOP to ensure all network devices and equipment are inventoried, and configured to manufacturer’s and best practice security standards.**

4. Network management tools must be configured to support the operation and security of the network.

   **ITS follows an internal SOP to configure and use a suite of network management tools.**

5. See the [Standards](#) (in the [knowledge base](#)) for the description of security standards applied at USF.
2.3 Server Management
1. Only ITS-approved servers may be connected to the network. Unauthorized or non-compliant servers will be removed upon discovery. This includes the use of any Personal Computers acting (configured) as servers in violation of policy. Any ITS-approved servers found to be compromised will be disconnected from the network until remediated.

   *ITS follows an internal SOP to find, identify, isolate, and as necessary remove unauthorized and compromised servers from the network. Owners of unauthorized systems will be contacted for policy violation.*

2. See the Standards (in the knowledge base) for the description of security standards applied at USF.

2.4 User System Management
1. Users must safeguard their personal and USF-provided systems and devices that connect to the network and not enable access for unauthorized systems or individuals. User systems must not be used as network servers.

   *ITS follows an internal SOP to find, identify, isolate, and as necessary remove unauthorized servers from the network. Owners of unauthorized systems will be contacted regarding a policy violation.*

2. See the Standards (in the knowledge base) for the description of security standards applied at USF.

3. Applicable Roles, Responsibilities, and Skills
For more expanded details see the Roles & Responsibility document.

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
<th>Skills/Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS network personnel</td>
<td>Acquire and deploy standard approved network devices that are configured (hardened) to security standards before moving into production.</td>
<td>Device specific set up and recommended security configurations (e.g. from CISCO, Huawei, Palo Alto Networks, et al). Knowledge of administrative security Standards. How to add to Asset inventory, and CMDB (Service Now).</td>
</tr>
<tr>
<td>ITS server personnel</td>
<td>Acquire and deploy standard approved servers that are configured (hardened) to security standards before going into production.</td>
<td>Device specific set up and recommended security configurations (e.g. from Microsoft, Red Hat, et al) Knowledge of administrative security Standards. How to add to Asset inventory, and CMDB (Service Now).</td>
</tr>
<tr>
<td>Student/Faculty/Staff</td>
<td>Follow guidance and standards on what can be connected to the network.</td>
<td>See FAQs on gaining network access.</td>
</tr>
</tbody>
</table>
4. Measurement and Metrics

1. Results metrics.
   a. number of unauthorized connection points identified per year.
   b. number of new network devices installed and successfully added to the CMDB.
   c. number of guest wifi connections.


5. Continual Improvement

ITS will work with the Faculty and Staff to improve the provision and reliability of the network.

6. Resources

- Information Security Policy
- Technology Acquisition Lifecycle Management Policy
- Technology Resources Appropriate Use Policy
- Roles and Responsibilities
- Information Access standards
- Standards and Glossary - use the Knowledge Base for security standards, technical controls, and glossary terms.
- ServiceNow ITS knowledge base and procedures library - use Search box to find a specific guide or article.
- ITS Help Desk - use for general IT assistance.
- Exception Process - use to request an exception related to this process.