Information Security Policy High Level Process

Parent Policy: Information Security

Associated High Level Processes: Encryption and Protection of Media, and Network Security

Contents

1. Scope and Purpose...........................................................................................................................................1
2. Process and Procedures....................................................................................................................................1
   2.1 Process Requirements..................................................................................................................................1
      2.1.1 Protect Information..............................................................................................................................2
      2.1.2 Protect Access to Information Assets..................................................................................................4
      2.1.3 Protect Technical Equipment and Systems........................................................................................5
   2.2 Training and Awareness.............................................................................................................................5
3. Applicable Roles, Responsibilities, and Skills .................................................................................................6
4. Measurement and Metrics..................................................................................................................................7
5. Continual Improvement.....................................................................................................................................7
6. Resources..........................................................................................................................................................7

1. Scope and Purpose
This high level process supports the implementation of the Information Security Policy. The policy applies to all University (USF) information assets, resources, and Users in all locations. (See the glossary (in the knowledge base) for the definition of terms used in this document).

2. Process and Procedures
USF’s Information Technology and Services Department (ITS) will implement reasonable security practices and procedures to safeguard USF’s information assets, align to authoritative information security standard frameworks and controls (e.g. ISO, NIST, PCI, CSC-CIS, etc.), and comply with Federal, State, and local laws and regulations. ITS will work in conjunction with designated Information Stewards and asset owners from the Schools, Colleges, and Departments to implement the safeguards using a risk-based approach. The more valuable the asset, or the more it is viewed to be at risk, the higher the level of safeguards and standards (see knowledge base for the description of security standards) that will be employed.

2.1 Process Requirements
Every User and information asset must comply with the 3 key aspects of the Information Security Policy:

- Protect the University’s information and data.
- Manage access to the information assets.
- Protect the technical equipment and IT systems.
The following process requirements apply to all three asset categories - infrastructure, applications, and endpoints - unless otherwise indicated as being category specific. (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.)

### 2.1.1 Protect Information

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Applications</th>
<th>Endpoint Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. All <a href="#">information assets</a> (hardware, software, applications, information, and data) must be <a href="#">inventoried</a> and the inventory maintained to provide an up-to-date record for each asset. This includes both approved, authorized assets, and unapproved, unauthorized assets (i.e. those systems discovered on the network or found to be in use but not centrally acquired or managed by ITS). The inventory forms the foundational record of what needs to be safeguarded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITS follows an internal SOP to discover, add, update, remove, and retire hardware and software assets in the ITS inventory-asset management systems. This include managing both technical and end-user software licenses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. An <a href="#">Information Steward</a> is required to <a href="#">classify</a> information according to the USF <a href="#">Information Classification scheme</a> and assert that the appropriate reasonable <a href="#">security controls</a> are in place to protect the information and data. This may be done with ITS. This assertion applies to IT system data, like audit log files, business applications and databases, and to end-user data files. This <a href="#">FAQ</a> describes how to classify information, and how to grant or revoke User access to applications, data stores and audit logs. It also lists the named, designated information stewards for each asset.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITS follows an internal SOP to identify and maintain an up-to-date inventory of the Information Stewards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITS follows an internal SOP to record that assets are classified, that reasonable security controls are present, or if missing, that they will be established. If missing then approved non-standard mitigations must be added and the risk status of the asset updated in the inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. An information assets’ <a href="#">value</a> to USF, and the <a href="#">risks</a> to USF if the asset was compromised (e.g. lost, damaged, subjected to unauthorized use, changed, deleted, etc.), must be determined and documented by the Information Steward. This may be done with ITS. The information (data) classification of an asset indicates the value and level of risk USF will tolerate in the event of a compromise. Typically the higher the classification level the lower the tolerance for loss, and the more safeguards are needed. This <a href="#">FAQ/How Do I?</a> describes how to assess the value of the asset and where the result of a risk assessment will be stored for future use, and the cadence on when to re-assess.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITS follows an internal SOP to record that USF’s information assets have a risk assessment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Users are required to follow the classification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

1 See Applicable Roles, Responsibilities, and Skills
2 There are 4 [classification levels](#): public, internal, confidential, and highly confidential.
|   |   | established by the Information Steward and to apply and follow the recommended safeguarding measures. This FAQ/How Do I? describes how to use recommended safeguards based on the Information (Data) Classification standard, e.g. how to encrypt data at rest, how to encrypt data in transit via email or file transfer, and what not to do when using or accessing data internally or externally (i.e. not to print a highly confidential document and leave it on the printer).

*ITS follows an internal SOP to provide a variety of encryption tools for Users.*

| e. | Users must **not move** information from one classification level to another level unless authorized by the Information Steward. New safeguards may need to be added to support the re-classification. This is particularly important in the downward classification of previously higher classified data since new safeguards may not be present. This may lead to a higher risk of exposure or compromise. This *How Do I?* describes how to ask the information steward to re-classify information and the steps to do this.

| f. | Users must follow ITS standards on data **encryption** depending on the classification of the information. This extends to all asset categories. This FAQ/How Do I? describes when and how to encrypt data at rest, encrypt data in transit (via email or file transfer), and best practices when sharing data and information internally and externally.

*ITS follows an internal SOP to provide a number of encryption tools for different assets, from data base encryption, to website encryption, to file encryption, to encrypting stored passwords, etc.*

| g. | Users must **retain** certain types of information identified as a University record according to the USF retention schedule, or to satisfy legal hold. Once the retention period is exceeded or legal hold removed, records may be deleted with
concurrency from the respective Information Steward. This FAQ describes the role of the schedule, guidance on legal hold, and for an Information Steward, how to sign-off to delete information.

*ITS follows an internal SOP for placing and removing preservation-hold flags on data files that are subject to legal hold.*

*ITS follows an internal SOP to securely delete data files from a PC or Apple, as well as wipe a whole drive. It also describes the deletion of data from databases and data stores.*

### 2.1.2 Protect Access to Information Assets

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Applications</th>
<th>Endpoint Assets</th>
</tr>
</thead>
</table>
| a. The security principle of "least privilege" will be applied to all Users and to the information assets. Least privilege means that Users are only granted access to information and IT assets at the level that is required to perform their roles. Having more access or privileges than needed could lead to the information assets being compromised, even if inadvertently. Users who change roles may lose or gain access privileges based on their new role. The level of access will be determined by the Information Steward and implemented by ITS. This **How Do I?** article describe how an Information Steward can review and determine who should have access, for how long, and when this review is to be repeated.  

*ITS follows an internal SOP to grant, update, and revoke access to the level determined by the Information Steward.* |  |  |
| b. The security principles of confidentiality, integrity, and availability (also known as the CIA Triad) will be applied to all information assets. Each User is required to respect the confidentiality (i.e. keep information and data private, and limit inappropriate access), integrity (i.e. keep information and data trustworthy, and accurate), and availability (i.e. guarantee reliable access to authorized Users as determined by the business process) of the information assets in order to deliver USF's mission. This **FAQ** provides more on the CIA Triad and guidance on respecting this. |  |  |
| c. USF requires the use of a **username** and **password** to gain access to the main campus network and as needed onward access to Third Party systems and services. The password must follow ITS standards, and Users must protect their password against loss or misuse. This is particularly important for Users with privileged or elevated system account access to IT systems and applications. This **FAQ/How Do I?** describes how to create a good password (see **Standards** for format restrictions), reset a password, protect the password, and what to do if password, or username and password, are compromised.  

*ITS follows an internal SOP to create new usernames (when on-boarding); provide password tools; reset passwords; add single sign-on (SSO) for a User; suspend, temporarily revoke, un-revoke usernames; update User details; remove, delete username (when off-boarding); and add, remove, and manage privileged accounts.* |  |  |
2.1.3 Protect Technical Equipment and Systems

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Applications</th>
<th>Endpoint Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. A designated Asset Responsibility Owner (ARO) must be assigned to each hardware asset (desktop, laptop, tablet, server, network device, etc.). One owner may be assigned to multiple assets.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*ITS follows an internal SOP to associate an ARO with an asset(s), and maintain meta-data on the asset.*

| b. ITS will ensure that reasonable physical and logical security controls and practices are applied to the IT infrastructure systems (e.g. computers, servers, network devices, wiring closets, data center, etc.), the applications (e.g. desktop and server-based applications, databases, etc.) running on, or accessed via, the IT systems and network, the endpoints (e.g. PCs, tablets, etc.), and the data and information at-rest or in-transit on these. |

*ITS follows an internal SOP to apply the CIS Top 20 security safeguards to the information assets and attest compliance.*

| c. In conjunction with the Information Steward, ITS will perform a security assessment of new on-campus and off-campus technical systems and services to determine the level of exposure that could compromise or impact USF’s mission. This How Do I? explains how the security assessment is initiated and performed. |

*ITS follows an internal SOP to assess the degree of protections present in on-campus and off-campus technology and services compared to the CIS Top 20, effectiveness of mitigations, any exceptions to ITS standard, and when these are revisited.*

| d. ITS will ensure the same or acceptable level of protections are present or reflected in any Third Party (external) services that use or process USF information and data. This How Do I? describes how to request a Third Party security assessment. |

*ITS follows an internal SOP to assess the degree of protections present in Third Party technology and services compared to USF-hosted equivalent services, gaps to the CIS Top 20, effectiveness of vendor mitigations, any exceptions to ITS standard, and when these are revisited.*

2.2 Training and Awareness

1. All Users must take training on basic security awareness and education on how information security is applied at USF, on how to recognize threats and potentially compromising situations, and on how to protect themselves and the USF information assets.

*ITS follows an internal SOP to record training completions, and report those still to take it, along with follow-up and escalation.*

---

3 See Applicable Roles, Responsibilities, and Skills section.
4 The California Attorney General’s office states that “failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security”. The 20 controls in the Center for Internet Security’s Critical Security Controls (CIS-CSC) identify a minimum level of information security that all organizations that collect or maintain personal information should meet. See [https://oag.ca.gov/breachreport2016](https://oag.ca.gov/breachreport2016)
2. Users who will manage, access, or process sensitive and highly confidential data should take the appropriate **job specific training** before being granted access. For example, Users who process personnel data, payroll data, finance data, gift and donation data, confidentiality agreements, sensitive and highly confidential data received from outside of USF, and IT system and database administrators with direct access to assets holding such data. Click [here](#) for who should take training for access to Banner INB, and here for other conditional training.

*ITS follows an internal SOP to track the completion of job specific training before data or application access is granted, list trained Users, list untrained Users with access and for these cases work with Information Stewards to suspend or revoke access until training is complete.*

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>Information Steward</td>
<td>Inventory and know the list of data, information, and application assets under their control. Assess the assets for risk, and set USF’s degree of risk tolerance. Approve who has access or not.</td>
<td>Must know what assets support the business processes under their control, and who needs access to do what. Must have knowledge of how to apply information classification scheme and perform a risk assessment.</td>
</tr>
<tr>
<td>Asset Responsibility Owner (ARO)</td>
<td>Inventory and know the list of hardware assets under their control. Assess the assets for risk, and set degree of tolerance. Approve who has authorized access or not. Assess asset life cycle for replacement / retirement.</td>
<td>Know what assets are assigned to them including those used by non-employees (known as “Primary Clients.”) Know who should have access to the assets and managed access lists. Know when the asset is reaching the end of its life and need to be replaced or retired, and with what.</td>
</tr>
<tr>
<td>User</td>
<td>Maintain the confidentiality, integrity and availability (CIA) of the assets they access, use, and interact with.</td>
<td>Must know how to maintain the CIA of the assets. Must know what threats could expose the assets they access, use, and interact with, and what they can do to protect against these.</td>
</tr>
<tr>
<td>ITS Technical Staff</td>
<td>Acquire and deploy reasonable security practices (safeguarding policies, standards, controls and procedures). Based on risk</td>
<td>Must know, and how to implement, the reasonable security practices, and provide documented assurance that they are operating</td>
</tr>
</tbody>
</table>
4. Measurement and Metrics

1. Lagging results indicators:
   a. number of unplanned security incidents,
   b. number of assets without a risk assessment or named owner,
   c. number of information assets with non-documented, non-authorized User access.

2. Leading results indicators:
   a. number of Users who have completed training and awareness in time specified,
   b. number of risk assessments completed and responded to.

5. Continual Improvement

This process will be reviewed in conjunction with the review of the Information Security Policy.

6. Resources

- Information Security Policy
- Technology Resource Appropriate Use Policy
- Information Classification standards
- 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 - follow this to request an exception related to this process.