## Contents

<table>
<thead>
<tr>
<th>Role</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>1. Vice President-Chief Information Officer (VP-CIO)</td>
<td>2</td>
</tr>
<tr>
<td>2. Board of Trustees (BoT) Committee for Information Technology Strategy (CITS)</td>
<td>2</td>
</tr>
<tr>
<td>3. University Leadership Team (ULT)</td>
<td>2</td>
</tr>
<tr>
<td>4. Information Steward</td>
<td>2</td>
</tr>
<tr>
<td>5. Information User</td>
<td>3</td>
</tr>
<tr>
<td>6. Information Security Officer (ISO)</td>
<td>4</td>
</tr>
<tr>
<td>7. Public Safety</td>
<td>4</td>
</tr>
<tr>
<td>8. Internal Auditor</td>
<td>4</td>
</tr>
<tr>
<td>9. Office of the General Counsel (OGC)</td>
<td>4</td>
</tr>
<tr>
<td>10. Third-Party</td>
<td>4</td>
</tr>
<tr>
<td>11. Asset Responsible Owner (ARO)</td>
<td>5</td>
</tr>
<tr>
<td>12. Primary Client</td>
<td>5</td>
</tr>
<tr>
<td>13. Computer Refresh (CR) Coordinator</td>
<td>5</td>
</tr>
<tr>
<td>14. Technical Liaison</td>
<td>5</td>
</tr>
<tr>
<td>15. Budget Approver</td>
<td>5</td>
</tr>
</tbody>
</table>

## Scope

This document describes the set of roles used to govern, manage, and safeguard the security of the University’s information assets used to deliver and support its mission. These assets include hardware (e.g. computers, servers, network devices, etc), software (e.g. MS-Office, locally installed applications), and applications (e.g. Banner, Google Mail, other cloud-based services). The roles have differing levels of responsibility, accountability, and involvement in terms of managing and safeguarding the assets, and are filled by individuals in the Schools, Colleges, Divisions, and Departments, including ITS. The University relies on the roles working together to be effective.

The majority of the roles described in this document were taken from the 2015 edition of the Information Security Policy, unless otherwise indicated. Additional roles come from those described in the 2015 editions of the Technology Asset Management Policy and Computer Refresh (CR) Policy.

The list reflects the set of roles defined for the University and these are still referenced in most of the current 2015 set of ITS policies and also appear on a number of web pages which will be updated over time. It should be noted that use of the role labels does not necessarily indicate that the roles are being actively performed as described.
1. Vice President-Chief Information Officer (VP-CIO)

The VP-CIO is responsible for approving and ensuring ongoing compliance with this policy with oversight from the Board of Trustees (BoT) Committee on Information Technology Strategy (CITS). The Vice-President, Chief Information Officer (VP-CIO) designates the Information Security Officer (ISO) to be responsible for the development and maintenance of information security policy with consultation from the Office of the General Counsel (OGC).

2. Board of Trustees (BoT) Committee for Information Technology Strategy (CITS)

This Committee, under the Board of Trustees (BoT), focuses on IT strategy which includes information security. They ensure ongoing compliance with security policy as they review new and continuing ITS-ISC initiatives. Per their charter, "The Committee on Information Technology Strategy shall consist of not less than eight [8] members of whom at least half will be trustees of the University. The Chief Information Officer (CIO) will provide administrative support for this committee."

3. University Leadership Team (ULT)

The University Leadership Team are responsible for championing information security policies and information security practices in their respective Divisions, Schools, and Colleges, and any substantive revisions as recommended by the VP-CIO.

4. Information Steward

Information Stewards are Users who have primary responsibility for particular information. Stewards are either designated by the ULT, or by virtue of having acquired, developed, or created information resources for which no other party has stewardship. For example, the Registrars (Law and University) are the Stewards of student data; Human Resources are the Stewards of employee data; Development Services are the Stewards of donor and alumni data; Faculty are the Stewards of their research and course materials; Students are the Stewards of their own work.

The use of the term 'Steward' does not imply ownership in any legal sense, for example, as holder of a copyright or patent, but rather the person designated to make decisions about the data on behalf of the University. Stewards have all the responsibilities of Users (see next section). In addition, they are responsible for the following:

a. Establishing the risk profile (value and tolerance) for the information and data they are designated as owners of,

b. Establishing supplemental security policies and procedures. Stewards may establish specific information security policies and procedures for their information where appropriate. Stewards are responsible for the procedures related to the creation, retention, distribution and disposal of information. These procedures must be consistent with the Information Security Policy, as well as with other University policies, contractual relationships, and laws. Stewards may impose additional requirements that enhance security, working with ITS-Information Security & Compliance (ISC) to document these,
c. Assigning classifications and marking information. Stewards are responsible for determining the classification of their information and any specific information handling requirements particularly those as may be imposed by confidentiality agreements with third parties. Information that is Confidential or Highly Confidential shall be marked as such when it is presented or distributed to Users. Additional markings specifying handling and distribution requirements may be added,

d. Authorizations access. Stewards determine who is authorized to have access to their information. Steward shall keep records of all users who are granted access and make these records available for audit upon request. ITS-ISC can provide access control lists and groups of users,

e. Training. Stewards of Confidential and/or Highly Confidential information shall ensure the development/compilation and delivery of appropriate training on security policies and procedures to be completed by users prior to being granted access to their information. Third-party resources and services may be used. Stewards or their designees shall keep records of required training completion by users,

f. Confidentiality Agreement. Stewards of Confidential and Highly Confidential Information shall ensure that users sign an appropriate confidentiality agreement prior to being granted access. All confidentiality agreements must be reviewed and approved by University General Counsel,

g. Periodic review of access and/or revocation of access. Stewards must revoke access to Confidential and/or Highly Confidential information resources in a timely manner when a User has changed roles or left the University. Access privileges should also be reviewed periodically to ensure they are correct. ITS-ISC can provide access control lists and groups of users.

5. Information User
All members of the University community are "Users" of the University's information assets and resources, even if they do not have responsibility for managing these. Users are responsible for protecting information resources which they have access to. They shall follow the information security practices described in the Information Security Policy, as well as any other information security practices specified by an Information Steward, and other information security related policies including but not limited to the University's FERPA compliance policy, and the Technology Resources Appropriate Use Policy.

Users are responsible for helping maintain the security and integrity of USF technology resources:

a. Security Updates. Users must keep antivirus definitions and operating system security updates current on their PCs,

b. Backups. Users are responsible for the security and integrity of the University's information stored on PC systems. Users must make regular backups of USF information to a file server, backup tape, CD, DVD, or other storage medium and also follow encryption policy when using such portable media,

b. Access Control. Users are responsible for reasonably controlling the physical and network access to their information technology and communications equipment.
6. **Information Security Officer (ISO)**
As designated by the VP-CIO, the Information Security Officer (ISO) coordinates the efforts of ITS-ISC and other University personnel to improve the state of information security across the University.

The ISO is responsible for establishing and maintaining an information security program aligned to the information asset's risk and value which includes developing, deploying, and maintaining reasonable security policies, processes, practices, procedures, guidelines, and technologies to protect the assets. The ISO will ensure the information security program complies with applicable laws, regulations, and University policies, and that this program and policy, and other related IT security policies, are reviewed and updated as necessary. The ISO will assist with training to support this policy, and ensure that this policy is reviewed and updated as necessary.

The ISO coordinates the ITS-ISC response to information security incidents, directs and coordinates the University-wide information security program to comply with applicable laws and regulations, and ensures the information security policy and other related policies are regularly reviewed and updated as necessary.

7. **Public Safety**
The Department of Public Safety is responsible for working with ITS-ISC in response to information security incidents in which a policy violation or crime may have been committed. Public Safety, working with ITS-ISC, shall conduct an investigation and prepare a report for the appropriate authorities, or provide support to authorities conducting their own investigations.

8. **Internal Auditor**
The University's Internal Auditor reviews ITS-ISC's information security practices and recommends appropriate controls to mitigate the risk of inappropriate information access or use. The Internal Auditor also receives and processes reports to the 'whistleblower hotline', which may alert the University to information security incidents.

9. **Office of the General Counsel (OGC)**
The University Office of the General Counsel provides guidance regarding laws applicable to the information security policies and procedures. The OGC also reviews confidentiality agreements, contracts, and information security policy and proposed revisions for clarity and conformity with best practice.

10. **Third-Party**
Third-Parties who the University exchanges or entrusts Confidential and/or Highly Confidential information with must provide the University with documentation of sound information security practices prior to any release of Confidential or Highly Confidential information. This documentation must be kept on file in the office of ITS Business and Finance.
11. Asset Responsible Owner (ARO)
All University-owned or managed technology hardware, software, and application assets, including those in the cloud, must be assigned to an University employee with full-time, permanent employment status. This person is referred to as the Asset Responsibility Owner. They may also be an Information Stewards.

12. Primary Client
Personal computers (desktops and laptops), tablets or smart phones used by temporary or part-time (non-employee) staff and faculty must first be assigned to an appropriate full-time permanent employee, the Asset Responsibility Owner (ARO). The ARO must indicate if the asset will be used by a non-employee temporary staff or faculty member. The temporary staff or faculty member will be identified as the "Primary Client" for the asset assigned by the ARO.

13. Computer Refresh (CR) Coordinator
The CR Coordinator assists in scheduling the installation of replacement PCs and other logistics (such as access to locked offices, or designating and acting as a proxy if the recipient of the new computer cannot be present).

14. Technical Liaison
The Technical Liaison, as a member of the School, College or Division, participates in selection of computer replacement standards, assists clients with matching their needs to available computers in inventory, or to appropriate standard models and configurations for new purchases. The Technical Liaison also reviews and advises the Budget Approver regarding new use, failure, and theft replacements and requests for exceptions to standards.

15. Budget Approver
The Budget Approver is tasked to exercise judgment in assessing and approving computer purchases for their organizational unit including:

a. Review and approval of new use, failure, and theft replacement requests in consultation with the Technical Liaison,
b. Review and approval of exceptions to standards in consultation with the Technical Liaison,
c. Review and approve sharing cost to exception requests and working with ITS Finance for budget transferring details.