## Information Security Policy

<table>
<thead>
<tr>
<th>Policy Contents</th>
<th>Effective Date: 12-01-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. POLICY STATEMENT</td>
<td>Last Updated: 11-13-2015</td>
</tr>
<tr>
<td>II. REASON FOR POLICY</td>
<td><strong>Responsible University Officer:</strong></td>
</tr>
<tr>
<td>III. SCOPE</td>
<td>Vice President, Chief Information Officer</td>
</tr>
<tr>
<td>IV. AUDIENCE</td>
<td><strong>Policy Owner:</strong></td>
</tr>
<tr>
<td>V. POLICY TEXT</td>
<td>Director, Application Services</td>
</tr>
<tr>
<td>VI. PROCEDURES</td>
<td><strong>Policy Contact:</strong></td>
</tr>
<tr>
<td>VII. RELATED INFORMATION</td>
<td>ITS Help Desk</td>
</tr>
<tr>
<td>VIII. DEFINITIONS</td>
<td></td>
</tr>
<tr>
<td>IX. FREQUENTLY ASKED QUESTIONS</td>
<td></td>
</tr>
<tr>
<td>X. REVISION HISTORY</td>
<td></td>
</tr>
<tr>
<td>XI. COMPLIANCE</td>
<td></td>
</tr>
<tr>
<td>XII. POLICY EXCEPTION PROCESS</td>
<td></td>
</tr>
<tr>
<td>XIII. APPENDICIES</td>
<td></td>
</tr>
</tbody>
</table>
I. POLICY STATEMENT
A. All members of the University community are responsible for protecting information resources to which they have access. See ‘V. Policy Text’ (below) for details of the policy.

II. REASON FOR POLICY
A. The purpose of this policy is to ensure the confidentiality and integrity of USF information assets. The policy reflects USF’s commitment to stewardship of sensitive personal information and critical business information, in acknowledgement of the many threats to information security and the importance of protecting the privacy of University constituents, safeguarding vital business information, and fulfilling legal obligations.
B. This policy serves as a companion to the USF Network Security Policy, which speaks to the secure configuration of systems and use of the USF network, and the Technology Resources Appropriate Use Policy.

III. SCOPE
A. This policy applies to the entire USF community, including students, faculty, staff, alumni, trustees, temporary employees, contractors, volunteers and guests who have access to USF information assets. Information assets are information in any form, recorded on any media. Such assets include data, images, text, software, and voice recordings, in digital or analog form, stored on hardware, paper or other storage media.

IV. AUDIENCE
A. This policy applies to the entire USF community, including students, faculty, staff, alumni, trustees, temporary employees, contractors, volunteers and guests who have access to USF information assets.

V. POLICY TEXT
A. Policy Development and Maintenance
   1. This policy was drafted by the Information Security Policy Task Force for review and revision by the Communication Infrastructure and Security (CIS) subcommittee of the University Information Technology Committee (UITC). The resulting version was reviewed and revised by the full UITC, and forwarded to the University Leadership Team for final review and approval.
2. This policy shall be reviewed by the CIS subcommittee on an annual basis and any substantive changes forwarded to the UITC and the University Leadership Team for approval.

B. Policy Implementation and Evaluation
1. Implementation of this policy shall be overseen by the Vice President for Information Technology, in consultation with the University Leadership Team. Implementation activities, including information security review, remediation, and training development, shall be carried out by the ITS Information Security Coordinator in collaboration with Information Stewards, as defined in this policy.
2. An evaluation of policy implementation shall be conducted on an annual basis in the form of a third-party information security audit.

C. Information Classifications
1. Public
This classification covers information that may be disclosed to any person inside or outside the University. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and/or destruction of information.

2. Internal
This classification covers information that requires protection against unauthorized disclosure, modification, destruction, and use, but the sensitivity of the information is less than that for Confidential information. Examples of Internal-use-only information are internal memos, correspondence, and other documents whose distribution is limited as intended by the steward.

3. Confidential
This classification covers sensitive information about individuals and sensitive information about the University. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include personally identifiable information about:
   a. Current and former students (whose education records are protected under the Family Educational Rights and Privacy Act (FERPA) of 1974), including student academic, disciplinary, and financial records.
   b. Current, former, and prospective employees, including employment, pay, benefits data, and other personnel information.
   c. Donors, potential donors, Law Clinic and other University clinic clients, library patrons.
d. Human subjects in USF research.

Other categories of confidential information include:

e. Research information related to a forthcoming or pending patent application.
f. Certain University business operations, finances, legal matters, or other operations of a particularly sensitive nature.
g. Information security data, including passwords. Information about security-related incidents.

4. **Highly Confidential**
This classification covers sensitive information which, if it becomes available to unauthorized users, creates risk for identity theft and therefore requires notification of affected individuals. This information includes Social Security Numbers, bank account numbers, credit card numbers, and drivers’ license numbers.

5. **Default Classification**
Information that is not classified explicitly is classified by default as follows: Information falling into one of the Confidentiality categories listed above is treated as Confidential or Highly Confidential. Other information is treated as Public unless it is labeled as Internal-use-only by the Steward.

6. **Summary Table**

<table>
<thead>
<tr>
<th>Example</th>
<th>Public</th>
<th>Internal</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule of Classes</td>
<td>Access</td>
<td>Memos and minutes</td>
<td>Academic records</td>
<td>SSN</td>
</tr>
<tr>
<td>Minimal controls to prevent unauthorized modification/deletion</td>
<td>Determined by steward</td>
<td>Limited based upon need to know, named users only, training and confidentiality agreement required</td>
<td>Provide access only when no alternative exists. Treat as toxic. Named users only, training and confidentiality agreement required</td>
<td></td>
</tr>
</tbody>
</table>

| Access | Minimal controls to prevent unauthorized modification/deletion | Determined by steward | Limited based upon need to know, named users only, training and confidentiality agreement required | Provide access only when no alternative exists. Treat as toxic. Named users only, training and confidentiality agreement required |
### Use

<table>
<thead>
<tr>
<th>Public</th>
<th>Internal</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use</td>
<td>Post as needed</td>
<td>Determined by steward</td>
<td>No posting, limited reporting and copying</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use only when no alternative exist. Treat as toxic. No posting, limited reporting and copying</td>
</tr>
</tbody>
</table>

### Transmission

<table>
<thead>
<tr>
<th>Public</th>
<th>Internal</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission</td>
<td>Minimal controls to prevent unauthorized modification</td>
<td>Determined by steward</td>
<td>Confidential envelope; encrypted transmission</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hand deliver; encrypted transmission</td>
</tr>
</tbody>
</table>

### Storage

<table>
<thead>
<tr>
<th>Public</th>
<th>Internal</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Minimal controls to prevent unauthorized modification</td>
<td>Determined by steward</td>
<td>Locked private office or cabinets; secure server room; should encrypt on desktops, laptops, media</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Locked private office or cabinets; secure server room; should encrypt on desktops, laptops, media</td>
</tr>
</tbody>
</table>

### Destruction

<table>
<thead>
<tr>
<th>Public</th>
<th>Internal</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destruction</td>
<td>No controls</td>
<td>Determined by steward</td>
<td>Shred paper; securely delete files, wipe media</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Shred paper; securely delete files, wipe media</td>
</tr>
</tbody>
</table>

### D. Roles & Responsibilities

1. Information Stewards

Stewards are members of the University community who have primary responsibility for particular information. One becomes a Steward either by designation 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; Advancement Services are the Stewards of donor data. Faculty are the Stewards of their research and course materials; students are the Stewards of their own work.

The term Steward as used here does not imply ownership in any legal sense, for example, as holder of a copyright or patent. Stewards have all responsibilities of Users (see next section). In addition, they are responsible for the following:

a. 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 this Policy, as well as with other University policies, contractual relationships, and laws. Stewards may impose additional requirements that enhance security.

b. Assigning classifications and marking information. Stewards are responsible for determining the classification of their information and any specific information handling requirements that go beyond this Policy, particularly 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.

c. Determining authorizations. 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.

d. 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 the information. Third-party resources and services may be used. Stewards or their designees shall keep records of required training completion by users.

e. Confidentiality Agreement. Stewards of Confidential and/or 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.

f. Periodic review of access and/or Termination of access. Stewards must terminate 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 currency.

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

3. ITS Security Coordinator
The ITS Security Coordinator coordinates the efforts of ITS and other University personnel to maintain and improve information security at USF. On behalf of the Vice President for Information Technology, the Security Coordinator is charged with taking steps to ensure compliance with this policy across the University, including assisting with training and development of technical and procedural solutions. The Security Coordinator also coordinates the ITS response to information security incidents.

4. University Information Technology Committee and Subcommittees

5. Leadership Team
The Leadership Team approves this policy and any substantive revisions, as recommended by the UITC. Leadership Team members are also responsible for championing good information security practices in their respective divisions, schools, and colleges.

6. Public Safety
The Department of Public Safety is responsible for working with Information Technology Services in response to information security incidents in which a crime may have been committed. Public Safety shall conduct an investigation and prepare a report for the appropriate authorities, or provide support to authorities conducting their own investigation(s).

7. Internal Auditor
The USF Internal Auditor reviews USF information security practices and recommends appropriate controls to mitigate the risk of inappropriate information access and/or use. The Internal Auditor also receives and processes whistleblower hotline reports, which may alert the University to information security incidents.
8. General Counsel
The University General Counsel’s office provides guidance regarding laws applicable to USF information security policies and procedures. The office also reviews confidentiality agreements, this policy and proposed revisions for clarity and conformity with best practice.

9. Third-Parties
Third-parties with whom USF exchanges or entrusts Confidential and/or Highly Confidential information 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 Business and Finance.

E. Information Access

1. Collection
Highly Confidential information should be collected only when such information is an essential element of the necessary task and not prohibited by law. Alternative business processes should be employed whenever possible to avoid collection of such data.

2. Need to know
Access to Confidential and/or Highly Confidential information should be provided only when the user must know the information in order to perform his or her job functions. Access should not be provided automatically or as an adjunct to another process; for example, if a person needs access to an information system screen which contains Confidential and/or Highly Confidential data, but does not need access to all or some of the Confidential and/or Highly Confidential data elements, only those data elements which are specifically needed should be visible.

3. Individual Accountability
Access shall be granted to users in such manner as to provide individual accountability. Generic or otherwise shared accounts should not be permitted for access to Confidential and/or Highly Confidential information.

4. Usernames and Passwords
Usernames and passwords must never be shared. Passwords that provide access to University resources must not be stored on personal computers and must not be displayed on sticky notes or scraps of paper on or by computers. Whenever possible, passwords should be 8 or more characters long, and include letters,
numbers, and punctuation characters. They should not be names, words in
dictionaries, or permutations of personal data (birth dates or anniversaries, social
security numbers, etc.). Passwords should be changed periodically.

5. Logging out. Users must log off from applications, computers, and
networks when finished. If computers are located in secure offices or laboratories,
Users must not leave unattended personal computers with open sessions without
locking office doors or locking the computer. If computers are located in the open
or in a shared computer lab, Users must complete their session and log off fully.

USF faculty and staff computers should be configured to time out and require a
new login after a period of inactivity.

6. Training
Users must complete training, as designated and recorded by the information
Steward, prior to being granted access to Confidential and/or Highly Confidential
information.

7. Confidentiality Agreement
Users with access to Confidential and/or Highly Confidential information must
sign a Confidentiality Agreement prior to being granted access.

F. Information Use
1. Reporting
Social Security Numbers must not be used in reports or other documents unless
required by law.

2. Posting
Confidential and/or Highly Confidential information must not be posted in
physical spaces or on web pages whose access is not limited to the specific
individual to whom the information belongs.

3. Copying
Copying of Confidential and/or Highly Confidential information must be kept to
an absolute minimum, and all paper copies must be shredded prior to disposal.

G. Information Transmission
Highly Confidential, Confidential and Internal information must not be distributed or
made available to users who are not authorized to access the information. This applies to
originals, copies, and new materials that contain all or part of the information, and to oral
communication of information. When such information is distributed, it must be
distributed in such manner that the restrictions on its future distribution are clear.
When distributing documents in electronic form, precautions shall be taken against distributing files and disks with viruses and other forms of malicious code. Users should not forward e-mail messages with attachments without some level of confidence that the attachments do not carry malicious code.

1. Email
   Confidential and/or Highly Confidential information sent via e-mail or as e-mail attachments must be encrypted.

2. File Sharing
   Private directories in USFfiles should be used to share Highly Confidential, Confidential and Internal information with authorized individuals. Confidential and/or Highly Confidential information must not be placed in public or WWW folders on USFfiles. Confidential and/or Highly Confidential information should only be shared on local file servers if access is appropriately limited. Desktops should not be used for file sharing.

3. Campus Mail
   Confidential information sent via campus mail must be sealed and marked Confidential. Highly Confidential information must also be sealed and marked Confidential, and should be hand-delivered.

4. To Third-Parties
   All file transfers to third-party organizations containing Confidential and/or Highly Confidential information should be encrypted. Mail should be appropriately sealed and marked.

H. Information Storage
   1. Electronic
      a. On desktop computers, laptop computers, PDAs, smart phones, and other portable computing devices and media
         i. USF-owned
            (a) Confidential and/or Highly Confidential information must require a login for access.
            (b) Confidential information should be encrypted and backed up to a secure server.
            (c) Highly Confidential information must be encrypted and backed up to a secure server.
ii. Personally owned

With the exception of adjunct faculty records of student academic work in their courses, Confidential and/or Highly Confidential information must not be stored on personally owned computers, devices, or media.

b. On servers

Confidential and/or Highly Confidential information should be stored on secure servers. Servers with appropriate physical and network access controls may store Confidential and/or Highly Confidential data in unencrypted form. Access to Confidential and/or Highly Confidential information on servers must require a login. Server data should be backed up regularly. Backups should be stored in a secure, off-site location. Because electronic media can degrade, copies that may require long-term retention shall be periodically refreshed.

2. Paper

a. Internal

Confidential and/or Highly Confidential information stored in USF facilities must be stored in locked cabinets or secure storage rooms.

b. External

Confidential and/or Highly Confidential information stored off-site must be stored with a reputable storage service provider in a physically secure space. Appropriate documentation of security practices should be provided by the third-party, as specified above.

I. Information Destruction

Confidential and/or Highly Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons.

Note: Information destruction is prohibited by law if litigation is reasonably foreseeable. Consult with the University General Counsel.
1. Data Wiping
   a. Retired equipment
      When donating, selling, transferring, or disposing of computers or removable media (such as diskettes), care must be taken to ensure that Highly Confidential, Confidential and Internal information are removed or rendered unreadable. All retired computers must be processed through Information Technology Services to ensure proper data removal.

   b. Current production equipment
      To remove a file containing confidential information from a current desktop or laptop computer, follow the instructions included in Appendix A or Appendix B for secure deletion of files.

2. Shredding
   Confidential and/or Highly Confidential information stored in paper form must be shredded prior to disposal.

J. Incident Reporting and Response
   Users shall report known or suspected compromises of University information security to infosecurity@usfca.edu. The ITS Security Coordinator will inform the appropriate information steward and, if it appears that a crime may have been committed, the Department of Public Safety. In such cases, a Public Safety incident report should be created prior to the start of investigation. ITS detailed investigation reports must be shared with Public Safety and appropriate executive officers only, with only general status information reported, if appropriate, to broader community. Non-criminal incidents will be treated as Confidential unless information subject to California law has been compromised. In this case, affected individuals will be informed.

   The ITS Security Coordinator shall coordinate the efforts of all involved parties to investigate the incident. The Coordinator shall provide frequent status reports to the Vice President for Information Technology and other executive officers, as appropriate, and submit a complete incident report to the Vice President for Information Technology upon completion of the investigation.

K. Sanctions
   Members of the University community who knowingly violate this policy may be subject to disciplinary action in accordance with the Administrative Handbook, the applicable Collective Bargaining Agreement, and/or the Student Handbook
Members of the University community are responsible for familiarity with this policy.

L. Associated Policies
1. Technology Resources Appropriate Use Policy
2. Network Security Policy

M. Potentially Applicable Laws
1. Family Education Right to Privacy Act
   USF compliance with FERPA is overseen by the University Registrar.
2. Gramm Leach Bliley Act (GLB)
   The GLB requires that institutions have a comprehensive written information security program.
3. Cal. Civil Code section 1798.85
   This law prohibits the posting of SSNs.
4. Identity Theft Protection Act (California)
   This California law requires notification to affected individuals if highly confidential information is compromised.
5. Laws governing Intellectual Property

VI. PROCEDURES
A. (None)

VII. RELATED INFORMATION
A. (None)

VIII. DEFINITIONS
A. (None)

IX. FREQUENTLY ASKED QUESTIONS
A. (None)
X. REVISION HISTORY
A. 09-01-2006 – First publication
B. 03-01-2015 – Updated format
C. 11-13-2015 – Corrected links in section XIII

XI. COMPLIANCE
A. Failure to follow this policy can result in disciplinary action in accordance with Human Resources Employment Handbook and Office of General Counsel employee and labor relations. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS
A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES
A. Windows Secure File Deletion
   1. For secure deletion of a confidential file, directory, or Recycle Bin on Microsoft Windows 7, Vista, or XP (SP3) computers, you can use a free Data Removal Tool called Eraser. For details, see KB11053, “Windows Secure File Deletion SOP”.
B. Mac OS Secure File Deletion
   1. For secure deletion of a confidential file, directory, or Recycle Bin on Mac 10.5 and above operating systems, you can use the Secure Empty Trash feature. For details, see Mac OS Secure File Deletion SOP.