# Network Security Policy

<table>
<thead>
<tr>
<th>Policy Contents</th>
<th>Effective Date: 03-01-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. POLICY STATEMENT</td>
<td>Last Updated: 02-27-2015</td>
</tr>
<tr>
<td>II. REASON FOR POLICY</td>
<td>Responsible University Officer:</td>
</tr>
<tr>
<td>III. SCOPE</td>
<td>Opinder Bawa</td>
</tr>
<tr>
<td>IV. AUDIENCE</td>
<td>Vice President, Chief Information Officer</td>
</tr>
<tr>
<td>V. POLICY TEXT</td>
<td>Policy Owner:</td>
</tr>
<tr>
<td>VI. PROCEDURES</td>
<td>Director, IT Infrastructure</td>
</tr>
<tr>
<td>VII. RELATED INFORMATION</td>
<td>Policy Contact:</td>
</tr>
<tr>
<td>VIII. DEFINITIONS</td>
<td>ITS Help Desk</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>

Effective Date: 03-01-2015
Last Updated: 02-27-2015

Responsible University Officer:
Opinder Bawa
Vice President, Chief Information Officer

Policy Owner:
Director, IT Infrastructure

Policy Contact:
ITS Help Desk
I. POLICY STATEMENT
A. USF network resources shall preserve the integrity of the data stored on USF computing systems and prevent unauthorized access to confidential information. Unauthorized access and unlawful uses of USF network resources is prohibited. Network security will include firewalls, access control lists, and intrusion detection mechanisms for detecting unauthorized network activity.

II. REASON FOR POLICY
A. This policy is intended to ensure the secure configuration and use of the USF network.

III. SCOPE
A. This policy covers the USF network, including equipment, servers and user systems connected to the USF network.

IV. AUDIENCE
A. This policy is intended for the entire USF community, including students, faculty, staff, alumni, trustees, temporary employees, contractors, volunteers and guests who have access to the USF network.

V. POLICY TEXT
A. Policy Goals
   1. Ensure availability of and reliable access to USF network resources and network-based services, especially mission-critical applications.
   2. Preserve integrity of the data stored on USF computing systems, and prevent unauthorized access to confidential information.
   3. Preserve the privacy of users to the greatest extent possible.
   4. Promote an efficient, standards-based approach to providing and managing network-based services, servers, and user systems.
   5. Foster awareness of security issues among the members of the USF community who access network resources and services.
   6. Protect University computing systems from unauthorized access and unlawful uses.
   7. Facilitate prompt, effective, and consistent institutional responses to security threats, attacks, and violations.
8. Identify authority and responsibilities associated with enforcing security policies and procedures, responding to security threats, attacks, and violations.
9. Establish processes evaluating exception requests and periodic assessment and revision of policies and standards to ensure timely adaptation to changing network security requirements.

B. Network Management
1. Only authorized network equipment may reside on the USF network. See Standards for Network Equipment.
2. Access to USF network equipment and network equipment rooms is restricted to authorized USF personnel. See Standards for Network Management.
3. USF policy is not to police content, but to monitor resource usage and authenticate users. USF may log and trace basic identifying information (such as Mac address) for all desktops, servers, and other devices connected to the USF network.
4. Individual users should* be required to authenticate to access the USF network.
5. Entry points into the USF network must¹ be configured in accordance with Standards for Network Access.
6. USF personnel with network management responsibilities must adhere to Standards for Network Management.

C. Server Management
1. Servers connected to the USF network should meet Standards for Server Equipment, be authorized and registered, and be supported in compliance with Standards for System Administration.
2. Unauthorized servers or non-compliant servers connected to the network may be disconnected upon discovery.
3. Compromised systems or systems interfering with the functioning of the network will be immediately disconnected and will remain disconnected until the system has been appropriately secured or the problem resolved.
4. A server must not be used as a user system.

¹ In some policy statements within this document, the word "must" is used and in other instances, the word "should" is used. The use of "must" indicates that compliance is both feasible and expected. "Should" is used in those instances where compliance is highly desirable, but may not be technically feasible within the University's current network and technology infrastructure. In these cases, the policy statements represent goals that the University expects to achieve as its network and technology infrastructure advances.
D. User System Management

1. Each user is responsible for the network security of any device he or she connects to the network.
2. User accounts are for individual use only. Users must not share their account information.
3. User systems must not allow unauthorized access to University information, whether stored locally or gained through connection to other systems.
4. User systems must not be used to launch attacks on USF network services or systems/services outside the USF network.
5. User systems interfering with the functioning or security of the network may be immediately disconnected and remain disconnected until the system has been appropriately secured and the problem resolved.
6. USF reserves the right to ban any software or hardware, which USF deems a security threat, from user systems connected to the USF network.
7. File Sharing on the USF Network:
   a. File sharing will be disabled by default on USF-owned systems.
   b. USF recommends network file sharing through its centralized file server.
8. USF-owned and/or supported user system hardware and software should meet the standards detailed on the following web pages:
   a. Hardware Standards
   b. Software Standards
9. All user systems connected to the network must have up-to-date virus protection software with the latest virus definitions and operating system critical vulnerability updates. Subsequently, adequate protection against network-based vulnerabilities must be maintained on a regular basis.
10. Computers not conforming to this policy will be allowed limited network connectivity to the University's network for only the period required to install the necessary software and updates to conform to this policy. At the end of this time, the computer must meet these requirements or it will not be allowed to connect to the network.
11. All users accessing the USF network are expected to act in accordance with the Technology Resources Appropriate Use Policy.
E. Standards for Network Equipment
1. Network equipment must be housed in USF-approved equipment rooms, spaces, or classrooms.
2. An inventory of all network equipment must be maintained including configuration, IP address, physical location, and maintenance and warranty information.
3. Only USF-authorized network equipment may be deployed on the USF network. Authorization requests must be submitted via email to the Infrastructure Director.
4. Wireless access points not supported by ITS must meet the following requirements:
   a. Be authorized by ITS Infrastructure (send email to itshelp@usfca.edu).
   b. Be configured to require authentication for each user and device.
   c. Have DHCP disabled on LAN interface.
   d. Be configured with the default password changed.

F. Standards for Network Management
1. Access to equipment rooms must be limited to authorized personnel.
2. Distribution of keys to equipment rooms must be documented and tracked.
3. Accounts on switches, routers, and other network equipment must be limited to authorized personnel and distribution of these accounts must be documented and tracked. When staff members with accounts leave or change positions, their accounts must be deleted in a timely manner.
4. Network management tools should provide support in the following areas.
   a. Maintaining an inventory of all network equipment.
   b. Configuring network equipment from a central management console.
   c. Upload and download of network equipment configurations from a central management console.
   d. Tracking software versions on network equipment.
   e. Track changes in network equipment configuration.
   f. Monitor and log network equipment behavior.
   g. Monitor and log all access to network equipment.
5. Whenever possible, remote sessions with network equipment must be encrypted.
6. Network security should include the following mechanisms.
a. Firewall mechanisms for network access control, restriction of unencrypted data transmissions, content security (e.g., virus protection), and detecting and preventing denial of service attacks.
b. Access control lists.
c. Intrusion detection mechanisms for detecting unauthorized network activity.
d. Network Address Translation (NAT).

7. Network management should include the following network traffic and performance monitoring activities:
   a. Monitoring network configuration and connectivity.
   b. Monitoring network traffic.
   c. Monitoring network performance levels and diagnosing network performance problems.

8. Firewall protection is required at the following points in the USF network.
   a. Campus network connection to the Internet.
   b. Interface between the administrative network and the residence hall network.
   c. Entry points to campus Intranet.
   d. Connections to department networks whose research and/or instructional network activities could potentially interfere with the proper functioning of the campus network.

G. Standards for Network Access
   1. Access to USF Intranet services and resources from the outside is limited to USF-authorized entry points and facilities.
   2. All entry points into the USF network must be authorized including T1, DSL, ISDN, modems, and other types of connections.

H. Reporting and Responding to Security Violations
   1. Detected incidences of security violations must be reported immediately to the Campus Security Team by either calling the Help Desk at x6668 or sending email to abuse@usfca.edu.
   2. If appropriate, a member of the Campus Security Team will inform Public Safety of security violations.
   3. Public Safety is responsible for involving the appropriate campus and outside law enforcement agencies as necessary.
   4. Public Safety is responsible for coordinating the University's response to security violations with outside agencies.
5. Compromised systems or systems interfering with the functioning of the network will be immediately disconnected and will remain disconnected until the system has been appropriately secured.
6. The Campus Security Team will make every effort to contact the system administrator responsible for the compromised or interfering system to inform them that the system has been disconnected and to involve them in the process of analyzing and securing the system.
7. The Campus Security Team is responsible for submitting a report describing the incident, action taken, and resolution to the CIO. The CIO is responsible for distributing the report to other members of the Leadership Team as appropriate.
8. Disciplinary actions will be conducted through existing disciplinary procedures detailed in the Fogcutter Student Handbook, the Staff Handbook, and the faculty Collective Bargaining Agreement.

VI. PROCEDURES
A. (None)

VII. RELATED INFORMATION
A. (None)

VIII. DEFINITIONS
A. Mission-Critical Network Services
   1. Mission-critical network services are services designated by the Leadership Team to be essential University services such that loss of these services or inability to restore these services in a timely fashion would severely impede the University's ability to conduct business, have negative legal or financial impact, or endanger the health and safety of faculty, students, and staff.
B. Network
   1. A network is a system of transmission media and electronic devices that supports transmission of data, audio, and video among user systems and servers. All hardware and software contributing to data, audio, and video transmission are considered part of the network. This includes the network interface hardware as well as the operating systems in user systems and servers with connections to the network.
C. Server
   1. A server is a computer with the primary function of multi-user sharing of application, data, and/or services on a network.

D. User System
   1. A user system is any computational or communication device that is primarily for the use of a single individual.

E. USF Network
   1. The USF network includes the entire main campus network, networks at remote campuses, and connections among the campus sites.

IX. FREQUENTLY ASKED QUESTIONS
A. How should I access administrative systems (SIS, HRS, FRS, ADS) from home?
   1. First, check and see if the functionality you need is included in Web for Students, Web for Faculty, Web for Employees, or Web for Alumni and accessible through USFconnect. If it is not, to connect to the administrative system, you need a Secure Shell (SSH) client. USF’s supported SSH clients are Secure CRT (Windows) and DataComet (Macintosh). You can download an SSH client at https://intraweb.usfca.edu/its/usfpublic/ssh/.

B. Does USF have a firewall?
   1. Yes, USF’s network includes multiple firewalls.

C. How do I access my files from outside USF’s network?
   1. You are able to access USF network resources using your own high-speed Internet connection and a secure Virtual Private Network (VPN) client.

D. Can I run a network-based service from my desktop, such as a web server or mail server?
   1. This network security policy does not prohibit members of the USF community from running network-based services from their desktops. However, community members should be advised that running network-based services may create vulnerabilities on their desktop machine or on the network. If your desktop system interferes with the functioning or security of the USF network, it may be immediately disconnected and remain disconnected until the system has been appropriately secured and the problem resolved. Such network-based services include, but are not limited to:
      a. Web Servers
      b. Dynamic Host Configuration Protocol (DHCP) Servers
      c. Domain Name System (DNS) Servers
      d. Simple Mail Transfer Protocol (SMTP) Servers
Network Security Policy
03-01-2015

UNIVERSITY OF SAN FRANCISCO | Information Technology Services

e. File Sharing Servers
f. Mail Servers
g. Streaming Media servers

2. Further, if the network service you are running becomes utilized to the extent that the primary purpose of your desktop machine is multi-user sharing of applications, data, and/or services, your desktop has become a server and will be subject to the policies in paragraph V.C (above).

E. Can I attach a wireless router to the USF network?
1. Only faculty or staff may attach authorized wireless routers for academic purposes as long as they do not interfere with the USF wireless network. Security settings should be configured as described in Standards for Network Equipment. To find out if your router may interfere or how to restrict access, please contact the ITS helpdesk at x6668 or itshelp@usfca.edu.

F. Can I put a wireless router in my dorm room?
1. No.

G. How should I send files to colleagues, or to my home office?
1. Non-confidential files may be sent as e-mail attachments or placed on a departmental or central file server. If you would like access to the central ITS file server, please visit http://www.usfca.edu/its/about/policies/jade to learn more.

X. REVISION HISTORY
A. 06-01-2010 – First publication
B. 03-01-2015 – Updated format

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. (None)