Purpose

Network security monitoring is an essential tool in detecting network traffic that violates existing laws, regulations, policies, and/or is malicious in nature. This document describes the monitoring, logging, and retention of network traffic at UCSF for the purposes of ensuring the confidentiality, integrity, and availability of UCSF IT Resources and Institutional Information.

Definitions

Authorized User

Any UCSF faculty, staff, student, or other individual affiliated with UCSF who has been granted authorization to access or invoke Institutional Information for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with UCSF. The authorization granted is for a specific level of access to the Institutional Information in accordance with University policy. An example of an Authorized User is someone who handles business transactions and performs data entry into a business application or someone who gathers information from an application or data source for the purposes of analysis and management reporting.

Unit Information Security Lead

A term for the Workforce Member(s) assigned responsibility for tactical execution of information security activities including, but not limited to, implementing security controls; reviewing and updating Risk Assessment and Risk Treatment plans; devising procedures for the proper handling, storage and disposal of electronic media within the Unit; and reviewing access rights.

Technology Support Provider

Technology Support Providers are those individuals who design, manage, and operate enterprise Institutional Information.

Institutional Information

A term that broadly describes all data and information created, received and/or collected by UC.

Exceptions to Policy
Any deviations from this Policy, as to the business need or operational requirement must be documented and reviewed by Enterprise Information Security to assess the appropriateness and impact of the exception. Documentation must include requestor, policy exception, reason for exception, and length of time. Documentation can be in the form of email, paper document, or electronic document.

Resource Proprietor

The individual designated responsible for the information and the processes supporting the University function. Resource Proprietors are responsible for ensuring compliance with federal or state statutory regulation or University policy regarding the release of information according to procedures established by the University, the campus, or the department as applicable to the situation. Examples of responsibilities of Resource Proprietors include: specifying the uses for a departmentally owned server; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which individuals may have access to an application or to data accessible via an application. All Instructional Information and IT Resources are University resources, and Resource Proprietors are responsible for ensuring that these Resources are used in ways consistent with the mission of the University as a whole.

Restricted Data

The term restricted data describes any confidential or personal information that is required by federal or state law or regulation, or contractual obligation, and may be subject to data breach notification requirements and requires the highest level of security protection whether in storage or in transit. See BFB IS-2 for further discussion on restricted data. Examples of restricted data include:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Research Health Information (RHI)
- Payment Card Industry (PCI) Data
- Confidential Security Information
- Licensed Proprietary IP and Product Development Information

Policy

A. Scope

This policy applies to all users of UCSF Institutional Information and to all IT Resources used to conduct business for UCSF. This includes personal and third party systems that are used for UCSF business purposes and extends from the networking peering points between UCSF-controlled networks to the end-user system.

B. Privacy

The University of California respects the privacy of the members of the University community and has established policies and procedures consistent with federal and California law to guide the conduct of University activities relating to personal information. The monitoring of network traffic and the use, storage, disclosure, handling, and disposal of this information shall be done within applicable laws and policies.

C. Associated Policies and Procedures
Collection and monitoring of network traffic is addressed in the University of California Electronic
Communications Policy (ECP). Privacy and Confidentiality is addressed in ECP Section IV. Monitoring and
analysis of network traffic for security related matters are covered in ECP Section IV.C (b) and in ECP
Section V.B.

UCSF definitions of information types and roles and responsibilities are found in UCSF Policy 650-16:
Information Security and Confidentiality.

D. Access With and Without Consent

The ECP allows for routine monitoring and analysis of network traffic without user consent (ECP Section
IV.C (b)). Analysis and monitoring that extends beyond routine practices requires user consent. Access
without consent may be granted if the conditions detailed in ECP Section IV.B (Access without Consent) are
met. Each instance of access without consent must be documented.

E. Requirements

· UCSF employees who operate and support Institutional Information may observe network traffic during
regular business practices. Systems personnel shall not intentionally search the contents of electronic
communications or transactional information for violations of law or policy.

· If system personnel inadvertently discover or suspect improper activity that violates policy or law they
must notify the UCSF Information Technology Department or report violations consistent with the Policy on
Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the
?Whistleblower Policy?).

· Network traffic traversing UCSF networks is inspected on a routine basis by the UCSF Information
Technology Department and the UCSF Information Security Team, primarily to confirm malicious or
unauthorized activity. Inspections do not require user consent.

· Network traffic traversing UCSF networks may be inspected or captured for the purposes of network and
system administration by parties other than the UCSF Information Technology Department and the UCSF
Information Security Team. The content of such traffic may not be disclosed to other parties except to assist
in network and system administration. Any such disclosure shall be conducted on a least-perusal basis: data
must be destroyed when no longer needed and access must be restricted to only those responsible for
necessary network or system administration.

· Monitoring or capturing of network traffic conducted on a routine basis outside these parameters must be
approved by the Committee on IT Security which is part of UCSF Governance.

· Routine inspection for malicious or unauthorized activity is conducted by use of information security tools
such as network intrusion detection systems, network traffic monitors, firewalls, host-based security
software and system logging. Inspection may include monitoring and logging and retention of network
packets and/or network communication metadata and must be conducted on a least-perusal basis.

· All inspections must abide by applicable laws, regulations, and guidelines.

· Analysis and inspection of network traffic for malicious or unauthorized activity must be completed by a
UCSF employee or contractor designated as having the authority of ensuring the confidentiality, integrity,
and availability of UCSF Institutional Information.

· Access to analyzed or captured network traffic used for security monitoring must be logged and shall be
restricted to the UCSF Information Technology Department and UCSF Information Security Team staff.
Access by other staff members for the purposes of determining authorized and unauthorized activity shall be
limited to a least perusal basis. Request for access by other staff beyond this scope shall be handled as an
access-with or -without consent request.

- In exigent circumstances, access to analyzed or captured network traffic for incident resolution may be
granted on a least perusal basis to other UCSF employees or non-UCSF persons as determined by the UCSF
Information Technology Department and the UCSF Information Security Team. This access must be
documented and adhere to the requirements of this policy and any other applicable regulations and
guidelines. Access must be terminated as soon as it is deemed no longer necessary by the UCSF Information
Technology Department and the UCSF Information Security Team.

- Anonymized or aggregated network traffic may be made available for the purposes of network or security
performance analysis or education.

- Analyzed or captured network traffic must be disposed of when it is determined to be no longer useful for
the purposes of information security or network or system administration.

F. Implementation

Implementation of this Policy is the responsibility of each Department and School within UCSF and all
Users. All Users are responsible for understanding this Policy and ensuring that their use falls within its
scope.

G. Violations and Sanctions

Minor or accidental violations of this Policy may be handled informally, either through electronic email,
education, or discussion.

More serious or repeated Policy violations may result in temporary or permanent loss of access privileges or
modification of these privileges.

Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion
under applicable University policies and collective bargaining agreements. They may also be subject to any
federal or state penalties for violations.

Individuals who become aware of a violation or potential violation of this Policy should inform their
supervisor, department head, or Internal Audit.

In the event of a violation of this Policy that involves possible unlawful action by an individual, the Locally
Designated Official, the employee's immediate supervisor, or other appropriate official should immediately
be notified in accordance with the Policy on Reporting and Investigating Allegations of Suspected Improper
Governmental Activities (the ?Whistleblower Policy?). Notification should be made before any action is
taken, unless prompt emergency action is required to prevent bodily harm, significant property loss or
damage, loss of significant evidence of one or more violations of law or of University policy, or significant
liability to the University or to members of the University community.

**Resources** found in violation of this Policy may be removed from the UCSF network or prohibited from
connecting to the UCSF network until the violation is mitigated. Notifications of disconnects will be
communicated to the Resource Proprietor as quickly as possible; however, Resources may be disconnected
prior to notification.

UCSF may disconnect or limit access to a **Resource**, groups of **Resources**, the UCSF network, and the
Internet without notice in order to protect **Resources**, both external and internal, under exigent
circumstances.

Responsibilities
Contact Responsible Office (above) with any questions.

Related Policies
- 650-16 - Information Security and Confidentiality [3]

References

Links
[1] https://policies.ucsf.edu/policy/650
[2] mailto:SVCPOLICIES@ucsf.edu
[3] https://policies.ucsf.edu/policy/650-16