1. Information Security Logging and Monitoring Policy

Issued: May 3, 2019
Last Revised: July 1, 2021
Last Reviewed: November 11, 2022

2. Policy Purpose

This Information Security Logging and Monitoring Policy establishes the security requirements for logging and monitoring of information security-related events on University of Southern California (USC) information systems.

3. Scope and Application

This policy applies to all:

- University faculty members (including part-time and visiting faculty)
- Staff and other employees (such as postdoctoral scholars, postdoctoral fellows, and student workers)
- iVIP (guests with electronic access), as well as any other users of the network infrastructure, including independent contractors or others (e.g., temporary agency employees) who may be given access on a temporary basis to university systems
- Third parties, including vendors, affiliates, consultants, and contractors

4. Definitions

Term	Definition
Confidential	Data that typically includes regulated data requiring compliance efforts if exposed to unauthorized parties, or would cause legal, financial, reputational, operational harm if disclosed
Confidential-Controlled Data	Data that is a sub-category of Confidential and is to be used only for Covered Defense Information, which includes Controlled Technical Information (CTI), Controlled Unclassified Information (CUI), or any other information that has military or space application where the data provider (e.g. research sponsor) has imposed safeguarding or dissemination controls for reasons of national security
High Value Asset (HVA)	USC information systems that create, process, transmit or store High Value Information (HVI)
High Value Information (HVI)	Data that if inappropriately disclosed, accessed, used, disrupted, modified or destroyed, could cause significant impact, as defined by the Information Risk Standard, to USC's reputation and public confidence. High Value Information (HVI) could be Confidential, Internal Use, or Public data
Information Security Governance, Risk, Compliance (IS GRC)	A combination of three approaches that organizations use to demonstrate compliance with international standards, global rules, laws, and state regulations. Governance, risk management, compliance (GRC)

	is often implemented by companies that are growing globally to maintain consistent policies, processes, and procedures across all parts of the organization
ITS	Information Technology Services
OCISO	Office of the Chief Information Security Officer
System Owner	The individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The System Owner is a key contributor in developing system design specifications to ensure the security and user operational needs are documented, tested, and implemented

For more definitions and terms: USC Information Security Policies Terms and Glossary

5. Policy Details

Objective

The objective of this policy is to define information security logging and monitoring requirements for USC Confidential data and High Value Information (HVI), as defined in the Data Protection Policy.

5.1 In collaboration with OCISO, System Owners will help define information security events to be logged (e.g., user activity, system failure and logon errors) for any systems handling Confidential data, Confidential-Controlled data and High Value Information (HVI) as defined in the Data Protection Policy.

5.2 System Owners will, as defined in section 2.1, log all identified information security events, user activities, and other identified logging requirements related to systems that process, store, or transmit Confidential data, Confidential-Controlled data and High Value Information (HVI) data, as defined in the Data Protection Policy (e.g., network devices, servers, databases, faults or failures, errors). System Owners will use OCISO services, as it relates to Confidential data, Confidential-Controlled data and High Value Information (HVI) data as defined in the Data Protection Policy, to maintain and monitor security logs for data stored in cloud platforms and Software-as-a-Service (SaaS) solutions.

5.3 When technically feasible, System Owners will use OCISO services to ensure information security event logs are aggregated and correlated using an automated and centralized security event monitoring system.

5.4 System Owners will ensure information security event logs do not contain any Confidential data, as defined in the Data Protection Policy. If event logs are required to be shared, they must be sanitized in a manner consistent with industry standards, prior to disclosure.

5.5 System Owners will ensure information security event logs are retained for a predefined time period in accordance with legal and regulatory requirements and USC's Record Management Policy.

5.6 System Owners will ensure information security event logs are protected from unauthorized access, as defined in the Access Management Policy.

5.7 System Owners will use OCISO services to ensure information security event logs are reviewed and analyzed on a periodic basis through the use of log harvesting, parsing, alerting tools or a manual process.

6. Procedures

None

7. Forms

None

8. Responsibilities

All Faculty and Staff are required to comply with this policy.

9. Related Information

Compliance Measurement

The Office of the CISO and the Office of Audit Services will collectively monitor compliance with this policy, USC's information security policies and standards, and applicable federal and state laws and regulations using various methods, including but not limited to periodic policy attestations. Compliance with information security policies will be monitored regularly in conjunction with USC's monitoring of its information security program. Audit Services will conduct periodic internal audits to ensure compliance.

Exceptions

Any exceptions to the policy will be submitted and approved in accordance with the Information Risk Committee decision criteria by the OCISO Governance, Risk Management, and Compliance. Exceptions will be requested via email to the OCISO Governance, Risk Management, and Compliance team at infosecgrc@usc.edu.

Non-Compliance

Violation of this policy may lead to this being classified as a serious misconduct, which is grounds for discipline in accordance with the Faculty Handbook, staff employment policies, and the Student Handbook, as appropriate. Any disciplinary action under this policy will consider the severity of the offense and the individual's intent and could include termination of access to the USC network, USC systems and/or applications, as well as employment actions up to and including termination, and student disciplinary actions up to and including expulsion.

10. Contacts

Please direct any questions regarding this policy to:

OFFICE	PHONE	EMAIL
Office of the Chief Information Security Officer		trojansecure@usc.edu