1. Secure Systems Development Policy

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

2. Policy Purpose

The purpose of this Secure Systems Development Policy is to set University of Southern California's (USC) security requirements for System Owners in the planning, design, testing, and implementation of systems, software and applications.

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
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
Major Significance	A system is considered of major significance if it impacts the daily operations of a unit or school

Security by Design Objective	System designed from the foundation to be secure
System Development Lifecycle	A process for planning, creating, testing, and deploying an information system
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 the security activities, controls, and technical standards required during the planning, design, testing, implementation, and maintenance or upgrading of systems, software, and applications.

Policy Requirements

5.1 System Owners will consider the Security by Design Objective across all phases of system development lifecycle including planning, design, testing, implementation, and monitoring.

5.2 System Owners will use OCISO services to identify security-related requirements or will use the results of an information security risk assessment to identify security-related requirements and incorporate them into the design of the proposed system, software and/or applications as defined in the Information Risk Management Policy.

5.3 System Owners will execute test plans to validate the effectiveness of security requirements identified as part of project planning and an information security risk assessment process prior to system, software and/or application deployment.

5.4 System Owners will use OCISO services to ensure that newly acquired, developed or significantly changed High Value Assets (HVA), systems, software and/or applications are released to the production environment only after a pre-implementation security assessment, and information security issues have been addressed and documented in a change record as defined in the Change and Release Management Policy.

5.5 When a system is of Major Significance, System Owners should maintain separated development, test, and production environments.

5.6 System Owners should restrict access to source code used to compile code for systems of Major Significance.

5.7 System Owners will ensure all production systems and code repositories considered to be High Value Assets (HVA) have immutable logging enabled and logs protected as defined in the Information Security Logging and Monitoring Policy and retained as defined in USC's Record Management Policy.

5.8 System Owners will ensure applications are developed using industry standard secure coding practices to prevent common coding vulnerabilities in software development processes.

5.9 System Owners will archive old versions of production application source libraries using version control software, which includes version numbers and date of last use.

5.10 System Owners will deploy security patches/updates as defined in the Vulnerability and Patch Management Policy and Patch Management standard.

5.11 System Owners will ensure that Confidential data, High Value Information (HVI), as defined in the Data Protection Policy, and production data are not used as test data, or are adequately protected via authorization checks, data masking, anonymization, de-identification, and secure data storage and removal.

5.12 Prior to production release, System Owners will harden or secure new USC information assets and endpoints as defined in the Cloud Security Policy, Network Security Policy, and Endpoint Security Policy.

5.13 The creation of unapproved covert channels or administrative "back-doors" in a system and/or software and its release into the production environment that allow users to bypass security controls is strictly prohibited.

5.14 Prior to decommissioning a system or software, System Owners will securely remove, archive or protect any Confidential data or High Value Information (HVI), as defined in the Data Protection Policy. System owners will adhere to USC's Record Management Policy and Data Protection Policy throughout the decommissioning 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