1. Endpoint Security Policy

Issued: May 3, 2019
Last Revised: October 24, 2022
Last Reviewed: October 24, 2022

2. Policy Purpose

This Endpoint Security policy establishes minimum security requirements for protecting University of Southern California (USC) systems, including operating systems and endpoint computing 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
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
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 protect and preserve an environment that encourages academic and research collaboration through the responsible use of Information Technology (IT) resources, and to ensure that members of the USC community have access to reliable and robust IT resources that are safe from unauthorized or malicious use. This policy applies to USC-Owned Technology Resources, this includes, but is not limited to, desktops, workstations, laptops, and mobile storage devices purchased from all sources of USC funds, including sponsored project accounts. This policy also applies to personally purchased devices used for USC business purposes.

Policy Requirements

5.1 System Owners will configure information systems (e.g., email, application, web, database, network devices, and file servers) to protect against unauthorized or malicious use in accordance with industry-accepted system hardening standards and ensure systems are inventoried per the Asset Management Policy.

5.2 System Owners will apply the latest vendor supplied security patches or upgrade to system components and software to currently supported versions to mitigate known vulnerabilities. All patching and updates should be done at regular intervals not to exceed 60 days from vendor release and in compliance with the Vulnerability and Patch Management Policy.

5.3 When configuring the system, system owners will remove or disable default accounts as per the Access Management Policy and unnecessary services, applications, and network protocols.

5.4 System Owners will review endpoint security configurations periodically to protect against vulnerabilities.

5.5 System Owners will implement USC's approved endpoint detection and response (EDR) security software to protect against malicious software, including viruses and malware. This is required on all University High Value Asset, as defined in Data Protection Policy, systems and devices accessing High Value Assets or Confidential data, as defined in Data Protection Policy. Endpoint security controls will be implemented for all USC-Owned technology resources. (e.g., workstations, laptops, servers).

5.6 Personal devices accessing or handling USC data will implement an industry-accepted endpoint security software.

5.7 System Owners will implement industry-accepted procedures for the protection of removable media.

5.8 System Owners will encrypt all USC-Owned Technology Resources, specifically laptops and mobile storage devices. All encryption solutions will be installed before the device may be used to store or access USC data.

5.9 Install SentinelOne on all USC-owned endpoints (e.g., servers, desktops, laptops).

5.10 Confirm that all USC-owned endpoints are on at least the following versions of SentinelOne MacOS –v22.2.3.6268, Linux, K8s –v22.2.2.2, Windows -v22.1.4.10010

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 SCampus, 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