1. Network Security Policy

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

2. Policy Purpose

This Network Security Policy establishes security requirements for network infrastructure and connectivity at University of Southern California (USC).

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
Data Security Addendum (DSA)	A legal document used during the procurement process that is designed to protect and limit the unauthorized disclosure and use of personal information and proprietary technical data between a vendor and USC
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
Intrusion Prevention System (IPS)	A network security/threat prevention technology that examines network traffic flows to detect and prevent malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine
ITS	Information Technology Services
Network Owner	The person or entity responsible for the overall procurement, development, integration, modification, operation, maintenance, and

	retirement of a network
OCISO	Office of the Chief Information Security Officer

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 resources, and to ensure that members of the USC community have access to reliable and robust IT resources that are protected from unauthorized or malicious use.

Policy Requirements

5.1 Network Owners will map and document network connections and identify key components during network analysis, operations and investigations.

5.2 Access to USC's secured wireless network is permitted so long as the following security measures have been implemented on that network:

- 5.2.1 Encryption is enabled on wireless network traffic;
- 5.2.2 Media Access Control (MAC) based, certificate based, or username/password authentication is required before connecting to USC secured wireless network; and
- 5.2.3 All wireless infrastructure consoles and other management interfaces have been secured or disabled.

5.3 The confidentiality of transmitted information will be protected using encryption and device authentication as defined in the Data Protection Policy.

5.4 Networks, along with related endpoint devices (e.g., department workstations, security cameras, point of sale systems), will be logically or physically segregated into separate logical domains due to regulations and security requirements. Public-facing devices will reside within an OCISO approved network, based on the security requirements of the System Owners and in accordance with the data classification scheme in the Data Protection Policy.

5.5 Network and endpoint devices that store Confidential data, in accordance with the Data Protection Policy, will have information security event logging enabled, as defined in the Information Security Logging and Monitoring Policy.

5.6 System Owners should utilize OCISO services to perform a timely analysis or System Owners will ensure a timely analysis is performed of identified vulnerabilities on all network devices as defined by the Vulnerability and Patch Management Policy.

5.7 System Owners will perform remediation activities within a reasonable time frame by implementing appropriate risk mitigation procedures (e.g., deploying security controls, applying patches, making configuration changes, and implementing compensating controls) on all network and endpoint devices as defined by the Vulnerability and Patch Management Policy.

5.8 External connections (e.g., third-party connections, remote access) will be approved by System Owners and secured with network protection mechanisms, such as firewalls, and/or an Intrusion Prevention System (IPS), to adequately prevent external entities from accessing the internal USC network.

5.9 Physical and remote connections will be logically or physically segregated into separate logical domains within an OCISO approved network.

5.10 System Owners will maintain and periodically review all remote access connections into USC's internal network and will require all connections be established through approved methods in accordance with the Third-Party Security Risk Management Policy.

5.11 System Owners will require all third-party access permissions for Confidential data, as defined in the Data Protection Policy, to be documented in a signed Data Security Addendum (DSA); otherwise access to the USC infrastructure will not be granted.

5.12 Create a network map with basic components for supporting containment and investigation strategies.

5.13 Implement and require Multifactor Authentication (MFA) on all Virtual Private Networks (VPN).

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