1. Cloud Security Policy

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

2. Policy Purpose

The purpose of this Cloud Security policy is to establish information security requirements for Cloud Service usage at the 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
Cloud Services	A paradigm for enabling on-demand network access to a shared pool of physical and virtual computing resources (e.g. networks, servers, storage, applications, and services) that support self-service provisioning and management. Division of management responsibilities between the customer and provider vary by service model
Cloud Service Provider (CSP)	A third party that provides on-demand network access to a shared pool of physical and virtual computing resources (e.g. networks, servers, storage, applications, and services) that support self-service provisioning and management. Division of management responsibilities between the customer and provider vary by deployment model
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
Infrastructure as a Service (IaaS)	On-demand access to cloud-hosted physical and virtual servers, storage, and networking – the backend IT infrastructure for running applications and workloads in the cloud
ITS	Information Technology Services

Platform as a Service (PaaS)	On-demand access to a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining, and managing applications
Service Level Agreement (SLA)	A service level agreement (SLA) is a contract between a service provider and the customer that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive. SLAs do not define how the service itself is provided or delivered. Though each SLA may vary depending on the service provider, the areas covered are consistent across SLAs, including responsiveness, work volume, quality, precision, accuracy, and speed
Software as a Service (SaaS)	On-demand access to ready-to-use, cloud-hosted application software
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 information security responsibilities with respect to the use of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) cloud services at USC.

Policy Requirements

5.1 System Owners will adhere to the Information Security Policies and Standards when utilizing cloud services.

5.2 System Owners should maintain a current inventory of assets hosted in cloud environments in accordance with the Asset Management Policy. The inventory should contain information such as organization criticality, data classification as defined in the Data Protection Policy, Service Level Agreements (SLAs) and business continuity requirements.

5.3 USC data in cloud environments will be classified and protected as outlined in the Data Protection Policy.

5.4 System Owners will comply with geographic restrictions on data storage, processing, and transmission, including but not limited to regulatory requirements governing the flow of data across borders, international commerce and trade laws, and location-based restrictions on physical and logical access to USC data.

5.5 USC information and applications residing in multi-tenant hosting environments will have access restricted appropriately.

5.6 System Owners will confirm Cloud Service Providers (CSPs) will have audit plans in place requiring at least annual assessment of the effectiveness of information security measures.

Upon request, cloud providers will be able to show evidence of audit results and proof of compliance with industry and regulatory standards as defined in the Third-Party Security Risk Management Policy.

5.7 Access to USC information stored in external cloud environments will be subject to the same access controls as internally hosted applications and infrastructure as defined in the Access Management Policy and Third-Party Security Risk Management Policy.

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 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