USC University of Southern California

1. Third Party Security Risk Management Policy

Issued: May 3, 2019
Last Revised: May 3, 2019
Last Reviewed: February 27, 2023

2. Policy Purpose

This Third-Party Security Risk Management Policy establishes university security requirements for the use of third-party services, products or related processes who:

- Handle USC information; either by accessing, storing, processing, transmitting, or receiving data, for hardware and software products, support and maintenance, service or solution providers, and Information Technology (IT) services.
- Maintain a separate, but trusted network connected, to the USC network and provide services for, on behalf of, or in conjunction with 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
Business Associates Agreement (BAA)	A legal document between a healthcare provider and a contractor, when that vendor might receive access to Protected Health Information (PHI)
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
High Value Information (HVI)	USC information systems that create, process, transmit or store High Value Information (HVI)
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
Internal Use Only	Data that includes all information used to conduct USC business, unless categorized as “Confidential” or “Public”
Protected Health Information (PHI)	Also referred to as personal health information, generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care
Third Party	Any outside individual or entity who is not a university student, faculty or staff employee who contractually interacts with or on behalf of USC. This includes but is not limited to vendors, consultants, contractors, and research and business partners
Third Party Relationship Owner (TPRO)	The individual responsible for establishing and managing the interactions between a third party and USC

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 management of third parties to ensure responsible protection and use of University of Southern California (USC) information.

Policy Requirements

5.1 The Office of the Chief Information Security Officer (OCISO) must maintain defined information security criteria for third-party services, products or related processes handling Confidential data, as defined by the Data Protection Policy.

5.2 Prior to the initial third-party service, product or related processes, handling or storing USC Confidential data, relevant purchasing or information technology authorities will request that OCISO assess security practices of the third party.

5.3 The Third-Party Relationship Owner (TPRO) will adhere to information security requirements relating to USC's Confidential information assets, as defined by the Data Protection Policy, being accessed, stored, analyzed, processed, or transmitted by third party services, products or offerings. The TPRO should also obtain a Data Security Addendum (DSA) with the third party that handles, stores or transmits Confidential data and consult with the Office of Culture, Ethics & Compliance regarding whether a Business Associates Agreement (BAA) is needed for information assets related to Protected Health Information (PHI).

5.4 If a third-party service, product or related process is handling any information before a contractual or subscription engagement, relevant purchasing or information technology authorities will require that if the information being collected or exchanged is Confidential or Internal Use Only, as defined by the Data Protection Policy, a binding Non-Disclosure Agreement or appropriate confidentiality language in the contract itself should be in place between USC and the third party.

5.5 OCISO will monitor and periodically assess third party information security practices for third party services, products or related processes handling, storing or accessing Confidential data or High Value Information (HVI).

5.6 Third Party Relationship Owners will work with OCISO to monitor and reassess third party information security practices in a timely manner.

5.7 New and existing third parties will be assessed and monitored for security vulnerabilities.

5.7.1 Third parties flagged with poor security vulnerability ratings will be escalated to Business for review.

5.8 Procurement will collect and maintain up-to-date third-party information, including the following:

- Third-party contact information
- Third-party relationship owner and represented School/Unit
- Third-party associated website(s)

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

VERSION HISTORY					
Version	**Issue Date**	**Effective Date**	**Prepared By**	**Authorized By**	**Description**
1.5	TBD	TBD	Information Security Governance, Risk and Compliance	Gus Anagnos	Call To Action revision update to include third parity data management and vulnerability monitoring
1.4	05/31/2021	06/30/2021	Information Security Governance, Risk and Compliance	Gus Anagnos	Updated third party requirements to include: services, products or related processes
1.3	12/01/2020	12/01/2020	Information Security Governance, Risk and Compliance	Gus Anagnos	Updated GRC email address and high value information definition
1.2	11/01/2019	11/01/2020	Information Security Governance, Risk and Compliance	Gus Anagnos	Updated exception wording
1.1	10/15/2019		Information Security Governance, Risk and Compliance	Gus Anagnos	• Correction to 2.3 to align with contract language • Edited compliance passage to clarify exceptions process by USC Risk Leadership
1.0	05/03/2019		Information Security Governance, Risk & Compliance	Gus Anagnos	Original Version