1. Security Incident Response Policy

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

2. Policy Purpose

This Security Incident Response Policy describes University of Southern California (USC) expectations for management of an information security incident and the related minimum-security requirements.

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Authorized users have access to the systems and the resources they need</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Data, objects and resources are protected from unauthorized viewing and other access</td>
</tr>
<tr>
<td>Covered Individuals</td>
<td>People or entities specified by the scope of a policy</td>
</tr>
<tr>
<td>Incident Response Plan</td>
<td>A systematic and documented method of approaching and managing situations resulting from IT security incidents or breaches</td>
</tr>
<tr>
<td>Integrity</td>
<td>Data is protected from unauthorized changes to ensure that it is reliable and correct</td>
</tr>
<tr>
<td>Information Security Governance, Risk, Compliance (IS GRC)</td>
<td>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</td>
</tr>
<tr>
<td>ITS</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>Local Technology Support</td>
<td>Information technology support dedicated within a local school or unit</td>
</tr>
<tr>
<td>OCISO</td>
<td>Office of the Chief Information Security Officer</td>
</tr>
</tbody>
</table>
Personnel Identifiable Information (PII) | Any data that could potentially identify a specific individual
---|---
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
Security Incident | Any information security event which has the potential to or has already resulted in unauthorized access, acquisition, manipulation, or destruction of data which compromises the Confidentiality, Integrity or Availability of university information assets, including those which may be handled, stored, or accessed by third party services, products or related processes
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 ensure all employees, iVIP guests, and third parties know what to do in the event of an information security incident. A “security incident” is defined as any information security event which has the potential to or has already resulted in unauthorized access, acquisition, manipulation, or destruction of data which compromises the Confidentiality, Integrity or Availability of university information assets, including those which may be handled, stored, or accessed by third party services, products or related processes.

Policy Requirements

5.1 Incident Reporting

5.1.1 Covered Individuals must immediately report both potential and suspected security incidents. Covered Individuals will:

5.1.1.1 Contact the System Owner and Local Technology Support immediately.

5.1.2 Local Technology Support will report major security incidents to OCISO, as defined in the Incident Response Plan, to initiate incident investigations. Local units will not conduct independent investigations.

5.2 Incident Response Plan

5.2.1 Relevant System Owners will work with Office of the CISO to establish an Incident Response Plan, which will include a report and response plan on the Confidentiality, Integrity and Availability of the data that may be breached, including but not limited to
Personally Identifiable Information (PII), Protected Health Information (PHI), privacy data, and student records.

5.2.2 The Incident Response Plan will be maintained, updated, and tested at least annually for timely and effective handling of all security incidents. OCISO may request evidence of the plan periodically.

5.3 Incident Response
5.3.1 Affected schools and units, in coordination with the Office of Culture, Ethics & Compliance, Office of General Counsel and OCISO as required, will follow established procedures for the identification, collection, acquisition and preservation of information related to security incidents.
5.3.2 Affected schools and units will adhere to the expected notification and response timelines, as outlined in the Incident Response Plan (IRP).
5.3.3 System Owners will work with OCISO on measures to contain and resolve security incidents.
5.3.4 System Owners and Local Technology Support will comply with evidence requests from OCISO, General Counsel and other OCISO authorized partners in a timely manner. At no time will Covered Individuals impede an investigation, as defined by the Acceptable Use Policy.
5.3.5 All information pertaining to an information security incident investigation must be handled with discretion and disclosed to internal and external parties only on a need-to-know basis.
5.3.6 Document initial local response procedure using OCISO template.
5.3.7 All people supporting your systems to complete "TrojanSecure: Information Security Incident Response" training module in TrojanLearn.usc.edu.

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:

<table>
<thead>
<tr>
<th>OFFICE</th>
<th>PHONE</th>
<th>EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Chief Information</td>
<td></td>
<td><a href="mailto:trojansecure@usc.edu">trojansecure@usc.edu</a></td>
</tr>
<tr>
<td>Security Officer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>