1. Information Risk Management Policy

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

2. Policy Purpose

This Information Risk Management Policy establishes requirements to achieve consistent identification, evaluation, response and monitoring of information risks facing 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

<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>Confidential</td>
<td>Data that typically includes regulated data requiring compliance efforts if exposed to unauthorized parties, or would cause legal, financial, reputational, operational harm if disclosed</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Data, objects and resources are protected from unauthorized viewing and other access</td>
</tr>
<tr>
<td>High Value Asset (HVA)</td>
<td>USC information systems that create, process, transmit or store High Value Information (HVI)</td>
</tr>
<tr>
<td>High Value Information (HVI)</td>
<td>Data that if inappropriately disclosed, accessed, used, disrupted, modified or destroyed, could cause significant impact, as defined by the Information Risk Standard, to USC’s reputation and public confidence. High Value Information (HVI) could be Confidential, Internal Use, or Public data</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>
</tbody>
</table>
5. Policy Details

Objective

The objective of this policy is to define requirements for the management for information risks at USC.

Policy Requirements

5.1 System Owners will utilize Office of the CISO (OCISO) to identify and/or report information security risks on High Value Assets (HVA) or assets with Confidential data, as defined in the Data Protection Policy, at defined intervals and upon request to OCISO.

5.2 System Owners will utilize OCISO services to monitor the effectiveness of security measures designed to reduce information security risks to a reasonable level, that may be subject to review of OCISO, Office of Compliance or USC Audit Services.

5.3 OCISO and USC Information Risk Governing Bodies will manage known information risks at a Reasonable Level as required by the USC Board of Trustees.

5.4 OCISO will conduct Information Security Risk Assessments of the potential risks and vulnerabilities to the Confidentiality, Integrity and Availability of High Value Assets (HVA) or assets with Confidential data, as defined in the Data Protection 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 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 Security Officer</td>
<td></td>
<td><a href="mailto:trojansecure@usc.edu">trojansecure@usc.edu</a></td>
</tr>
</tbody>
</table>