1. Data Protection Policy

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

2. Policy Purpose

This Data Protection policy establishes the information security expectations for University of Southern California ("USC") data.

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>Academic Need</td>
<td>An academic need accomplishes a scholarly purpose, including but not limited to grant-supported research, academic assignments, and any activities required to complete USC coursework</td>
</tr>
<tr>
<td>Business Need</td>
<td>A business need accomplishes a financial or other legitimate operational purpose, including but not limited to payroll, human resources, operations, and other business management functions</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>Confidential-Controlled Data</td>
<td>Data that is a sub-category of Confidential and is to be used only for Covered Defense Information, which includes Controlled Technical Information (CTI), Controlled Unclassified Information (CUI), or any other information that has military or space application where the data provider (e.g. research sponsor) has imposed safeguarding or dissemination controls for reasons of national security</td>
</tr>
<tr>
<td>Data Security Addendum (DSA)</td>
<td>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</td>
</tr>
<tr>
<td>Electronic Media</td>
<td>Electronic media (i.e., “soft copy”) are devices that contain memory</td>
</tr>
</tbody>
</table>

1
storage such as hard drives, random access memory (RAM), read only memory (ROM), discs, and flash memory. Equipment that contain such devices including; phones, mobile computing devices, networking devices, and any additional type of device that stores information.

<table>
<thead>
<tr>
<th>Hard Copy Media</th>
<th>Hard copy media are physical representations of information, most often associated with paper printouts</th>
</tr>
</thead>
<tbody>
<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>Internal Use Only</td>
<td>Data that includes all information used to conduct USC business, unless categorized as “Confidential” or “Public”</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>Public</td>
<td>Data that is not regulated and is generally made available through public interfaces and requires no protection mechanisms</td>
</tr>
<tr>
<td>Third Party</td>
<td>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</td>
</tr>
</tbody>
</table>

For more definitions and terms: USC Information Security Policies Terms and Glossary

5. Policy Details

Objective

The objective of this policy is to establish security requirements for all information accessed, handled, created, or captured, collected, shared, and disposed by USC; all information contained on USC owned media, which is transmitted by USC; and all information that USC has a legal or contractual obligation to protect.

Policy Requirements

5.1 All information should be classified into one of the three defined classes; "Public", "Internal Use Only", and "Confidential," unless required otherwise by regulatory agencies.

5.2 "Public" data is not regulated and is generally made available through public interfaces and requires no protection mechanisms.
5.2.1 Example information types:
5.2.1.1 USC community memos
5.2.1.2 Marketing and promotional materials
5.2.1.3 Academic calendars
5.2.1.4 Course catalogs
5.2.1.5 Advertising material
5.2.1.6 Public web content and media
5.2.1.7 Press releases
5.2.1.8 Public announcements
5.2.1.9 Public relations documents
5.2.1.10 Campaigns and outreach
5.2.1.11 Job postings

5.3 "Internal Use Only" data includes all information used to conduct USC business, unless categorized as "Confidential" or "Public."
5.3.1 System Owners will ensure "Internal Use Only" data will be masked, anonymized, or de-identified, if used outside its intended purpose.
5.3.2 "Internal Use Only" classification will be used for information not otherwise classified.
5.3.3 Example information types:
5.3.3.1 Non-regulated Personally Identifiable Information
5.3.3.2 In-process contracts and agreements
5.3.3.3 Employee performance evaluation information
5.3.3.4 Audit reports
5.3.3.5 Network diagrams
5.3.3.6 Non-public USC policies
5.3.3.7 Information involving USC strategy and implementation plans
5.3.3.8 Internal USC memos and emails
5.3.3.9 USC and employee ID numbers

5.4 "Confidential" information typically includes regulated data requiring compliance efforts if exposed to unauthorized parties, or would cause legal, financial, reputational, operational harm if disclosed.
5.4.1 System Owners will ensure "Confidential" data will be masked, anonymized, or de-identified, if used outside its intended purpose.
5.4.2 Example information types:
5.4.2.1 All information protected by Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), the Family Education Rights Privacy Act (FERPA), and California Financial Information Privacy Act (CFIPA)
5.4.2.2 Nonpublic Personal Information (NPI)
5.4.2.3 Regulated Personally Identifiable Information (PII)
5.4.2.4 Special communications indicated as Attorney-Client Privilege
5.4.2.5 Trade Secrets
5.4.2.6 USC Business Financials and Business Strategy and other data and information may be classified as Confidential if in USC's best interest

5.4.3 Confidential-Controlled" data is a sub-category of Confidential and is to be used only for Covered Defense Information, which includes Controlled Technical Information (CTI), Controlled Unclassified Information (CUI), or any other information that has military or
space application where the data provider (e.g. research sponsor) has imposed safeguarding or dissemination controls for reasons of national security.

5.5 High-Value Information" (HVI) is 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.

5.5.1 Example information types:

5.5.1.1 Confidential Student personally identifiable information combined with academic performance details
5.5.1.2 Confidential Title IX case information
5.5.1.3 Publicly available historical information that may be the only data set like it in the world

5.6 "High Value Assets" (HVAs) are USC information systems that create, process, transmit or store High Value Information (HVI).

5.7 Data Owners will review the information classification of their data on an annual basis.

5.8 Data Owners are responsible for ensuring the appropriate administrative, physical and technical safeguards are in place when using, storing, transmitting, or sharing information.

5.9 Data Owners will ensure individuals who have access to "Confidential" and "Confidential-Controlled" information have taken targeted information security training as defined in the Information Security Awareness Training Policy. This is in addition to any other education or training that may be required by the party providing the data to the Data Owner, or by USC under other policies.

5.10 Data Owners are responsible for the sanitization and disposal process of assets containing data and will document that the process is completed. Data destruction and retention will comply with USC’s Record Management Policy and the appropriate use, retention, and destruction practices of that policy.

5.11 Data Owners will verify all hard copy media are appropriately destroyed when no longer needed.

5.12 Data Owners will verify all electronic media/soft copies are securely disposed when no longer needed.

5.13 Data Owners will verify all electronic media are properly and completely removed from assets before disposal or re-deployment of the media.

5.14 All data should only be retained for as long as it is meeting an Academic or Business Need and in compliance with USC’s Record Management Policy.

5.15 Purge emails with personally identifiable data reports in the emails and do not store emails beyond 16 months per USC’s email 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 SCampus, 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>