1. Change and Release Management Policy

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

2. Policy Purpose

This Change and Release Management Policy establishes security requirements for System Owners to control configuration changes to university information assets and/or systems.

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>Back-Out Plan</td>
<td>The back-out plan is developed in parallel with the implementation plan and outlines the steps to be followed to back-out of a change implementation, as well as the conditions that should exist in order for the back-out to be invoked. The complexity of a back-out plan depends on the type and complexity of the change. For routine changes, a standard back-out plan may be available. However, the extent to which these are be utilized should be determined on a case-by-case basis</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>Major Configuration Changes</td>
<td>An adjustment or modification to any production hardware, system software, application software, or system component that would have a negative impact on critical or key systems and the daily operations of a school, unit or the broader USC environment (i.e. version change, software update, operation system update). This</td>
</tr>
</tbody>
</table>
would exclude those items that would fall under daily operations

| 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 responsibilities of System Owners related to configuration changes made to information assets and/or systems at USC.

Policy Requirements

5.1 System Owners will document and retain records of all Major Configuration Changes made to Confidential Data (as defined in the Data Protection Policy) in information assets and/or systems, for tracking and compliance purposes. Documentation will include a description of the change, analysis of any impact of the change, formal approval of the change, Back-out Plan, and implementation information. Any changes to how data is used, stored, transmitted, or shared will also adhere to the data protection requirements outlined in the Data Protection Policy.

5.2 System Owners will ensure changes made to information assets and/or systems will be tested in a development, staging, or other test environment prior to implementation in production, where technically feasible. Evidence of the change, test plans, test results, signoffs and approvals by testers and documented pre-implementation approval from authorized individuals will be retained for tracking and compliance purposes.

5.3 A list of authorized change approvers will be maintained by the System Owner for each information system and any modifications to this list will require approval by appropriate personnel.

5.4 Change implementations will be scheduled to minimize system disruption or outage and coordinated to avoid conflict with other proposed changes.

5.5 System Owners will communicate all changes made to information assets and/or systems to all relevant support personnel and users impacted by the change. If applicable, operating procedures and user guides will be updated to reflect the changes.

5.6 Emergency changes will be approved by appropriate personnel, including relevant ITS personnel or local IT management, based on the type of change and documented appropriately, either prior to the change or no later than 48 hours after implementation.

6. Procedures

None

7. Forms
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>