BOISE STATE UNIVERSITY

University Policy 8180

Information Technology Change Management

Effective Date

February 06, 2023

Responsible Party

Office of Information Technology, (208) 426-4357
Executive Director, Development & Business Intelligence Reporting Services, (208) 426-2635
Chief Information Security Officer, (208) 426-4127

Scope and Audience

This policy applies to all colleges, departments, and units, including all computing devices located at or controlled by Boise State University.

Additional Authority

- Gramm-Leach-Bliley Act

1. Policy Purpose

To protect University data, provide reliable enterprise tools, and reduce the risk of data loss or loss of service information productivity loss through negligence or intentional harm.

2. Policy Statement

Boise State University is committed to maintaining effective, efficient, reliable, and secure management of its enterprise systems consistent with the mission and goals of the university. All users of the University's Information Technology (IT) resources are expected to follow the guidelines outlined in this policy.

3. Definitions

3.1 Information Technology Change Management

Information Technology Change Management seeks to minimize the risk associated with the additions, modifications, or removal of anything that could have an effect on IT services, including changes to the IT infrastructure, processes, documents, interfaces, etc.

3.2 Best Practices

Change management procedures generally recognized by the industry for assuring secure, reliable, scalable, and efficient system management.

3.3 Tier 0 and 1 Systems

Tier 1 systems are the mission critical applications used by the University and are required for operation. Tiers are assigned to services and documented internally in the Office of Information Technology (OIT) Service Catalog. Tier 0 Systems are the infrastructure services necessary to operate Tier 1 systems.

4. Review of Changes

4.1 Standard Changes

Standard Changes are pre-authorized for Tier 0 and 1 Systems. They are low-risk changes associated with well-documented projects and or department procedures. They are documented in a system of record appropriate to the Tier system (for example, all standard changes to PeopleSoft are to be documented in the university's change management software, Stat).

4.2 Emergency Changes

Changes that must be implemented immediately, for example, to resolve a major incident. These changes must be approved by a member of OIT leadership, normally the director over the affected Tier 0 or 1 System.

4.3 Normal Changes

All other Changes that are not Standard Changes or Emergency Changes are reviewed, calendared, and discussed by the Cross Team Coordination subcommittee (CTC).

4.4 Blackout Periods

OIT leadership will define blackout periods at the first of the semester in which all standard and normal changes will follow the emergency change process and must be reviewed and approved by two (2) members of the OIT leadership team.

5. Separation of Duties

The University will maintain a separation of duties and responsibilities. This will be enforced by user and groups rights management within the given enterprise system. Group rights will be reviewed by managers every sixty (60) days.

6. Best Practices

Managers of University IT resources must seek and adopt, whenever possible, Best Practices with regards to change management. The CTC will review and adopt appropriate standards and procedures that represent Best Practices for calendaring, documenting, and testing normal changes.

7. Responsibilities

The OIT Executive Director of Development & Business Intelligence Reporting Services is responsible for administering this policy, including its maintenance and compliance. CTC will consist of representatives across OIT, and Campus Departments will review this policy and supporting documents and make recommendations to the OIT Executive Director of Development & Business Intelligence Reporting Services regarding additions, deletions, and/or modifications.

8. Exceptions to Policy

A request for exception, along with a plan for risk assessment and management, can be submitted for review by the OIT Executive Director of Development & Business Intelligence Reporting Services by completing a Self-Service Support Request. Non-compliance with these standards may result in revocation of access, notification to the supervisor, and reporting to the individual's manager, Human Resources and Workforce Strategy, Internal Audit and Advisory Services, and/or Institutional Compliance and Ethics.

9. Enforcement

Failure to comply with this policy may result in the suspension of the individual's access to network resources until policy standards have been met.

10.Related Information

Change Management Procedures
https://www.boisestate.edu/oit/itgrc/it-plans-procedures/change-management-procedures/

11.Forms

Self-Service Support Request
https://boisestateproduction.service-now.com/bsu_sp

Last Review Date

June 18, 2024