a

SNOWBE ONLINE #017
Change Control Management Policy

Sean Redding

Change Control Management

Policy- Version # 1.0

10-18-25

Table of Contents

Purpose

The purpose of this policy is to ensure that all changes to SnowBe Online's IT Resources minimize any potential negative impact on services and Users.

Scope

This IT policy, and all policies referenced herein, shall apply to all employees of SnowBe Online, including authorized guests, vendors, and third parties who use, access, or otherwise employ, locally or remotely, SnowBe Online's IT Resources, whether individually controlled, shared, stand-alone, or networked.

Definitions

Change Control - A systematic approach to managing all changes to SnowBe Online's IT Resources. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted, and that resources are used efficiently.

IT Resources - Include computing, networking, communications, applications, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and related materials and services.

Roles & Responsibilities

IT Director:
Responsible for the execution of the Change Management process. This includes operating the defined and agreed process, ensuring it interfaces with all other relevant processes, setting targets and reviewing the effectiveness and efficiency of the process, performing process audits, and managing the process improvement cycle.

Responsibilities:

- Manages and coordinates all activities necessary to control, track, and audit Changes in the environment.
- Leads the Change Management function and is responsible for the adequate skill levels and performance of the assigned staff members.
- Ensures Change status, progress, and issues are communicated to the appropriate groups.
- Audits and manages the process lifecycle and reports to upper management
- Schedule Urgent relevant meetings when necessary
- Evaluates performance metrics against the defined critical success factors and institutes actions to correct shortcomings or further streamline the process as necessary
- Responsible for reviewing the Change Schedule (CS) for conflicts
- Report Change Management activities to upper management.
- Produce management reports
- Responsible for the education of the Change Management process
- Initial Approval of Change Requests
- Review Change Request for technical accuracy and feasibility

- Provide input to the IT Manager for the ongoing maintenance and improvement of the Change Management process.

IT Manager:
Responsible for the overall planning, initiation, and execution of the change and thus, assigns the work for the change.

Responsibilities:
- Gathers Change-Related information
- Creates Change Request
- Assess, evaluate, and set the Risk for the Change
- Create a Change implementation plan
- Propose Change schedule
- Identify resources to implement the change and, in some cases, implements the change themselves
- Communicate the Change status and results
- Attend meetings when necessary
- Provide input to the Change Manager for the ongoing maintenance and improvement of the Change Management process

IT Team:
Responsible for implementing the change submitted by the Change Submitter.

Responsibilities:
- Provide change-related information to the IT manager when necessary
- Review Change Request for technical accuracy and feasibility
- Attend meetings when necessary
- Perform Change-related activities documented in the Change Request to ensure the Change is implemented according to plan
- Document closure activities in the Change record and complete the Change record
- Escalate any deviations from plans to appropriate management (direct manager and change manager)
- Provide input to the IT Manager for the ongoing maintenance and improvement of the Change Management process

Employees:

- Provide input to the IT team/manager for the ongoing maintenance and improvement of the Change Management process

Policy

- All changes to SnowBe Online's IT resources must be documented.

- Change requests may not be required for non-production (e.g., DEV, Test, QA) environments unless there is a significant upgrade or an impact.

- Production change requests must note that the change has been successfully applied, tested, and verified in a non-production environment when a suitable environment(s) exists.

- Changes to production environments undergo impact examination before submitting the change request. This information will be used to determine the impact of the change by considering:

  1) The impact the proposed change will have on business services, if it is expected to cause a widespread outage, a loss of connectivity, or functionality to a specific group or groups.

  2) The risk involved in not making the change;

  3) The risk if the change does not go as planned, and

  4) Predictability of the success of the change.

- Changes must be vetted for security implications through Information Security and IT participation.

- Significant User experience changes must be conveyed to the Change Control Board and communicated to the affected audience and IT.

- A lessons learned session should occur in the event of an incident during a change request.

Exceptions/Exemptions

Requests for an exception must be submitted in writing to consult with the IT Director or IT Manager.

The request must be detailed with information, including:

- Length of time
- Policy or standard
- Reason

Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.

If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.

The IT Director and the Commissioner must maintain constant communication during the exception. If approved, the Commissioner's office will send the letter of approval to the requester with details. In the event of denial, a letter of explanation will be sent to the requester with the reason the IT Director denied the request and an explanation.

Exemptions:

Access Control – Access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies, are not to be paused or discontinued.

Enforcement

- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director.

- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.

- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from SnowBe.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-18-25	IT Director	IT Director	Initial draft of policy.

Citations

https://it.emory.edu/smcc/itsm_process/change/roles-responsibilities.html

https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/change-control-policy/