SNOWBE ONLINE SP17

Change Control Management Policy

Danielle Williams

SP17 - Version # 1

DATE: August 26, 2024

SP17 – V 1.0
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Danielle Williams
DATE 8/26/2024

Table of Contents

Purpose

This policy's objective is to ensure that standardized methods and procedures are used to enable beneficial changes while ensuring efficient and prompt handling of all changes to services. This policy aims to minimize the disruption of services, reduce back-out activities, and ensure clear communication across SnowBe, its employees, and when applicable its customers.

Scope

The SnowBe Change Control Management Policy applies to any individual, entity, or process that create, evaluate, and/or implement changes to and SnowBe Information Resource.

Definitions

Change
A Change is defined by an addition, modification, or removal of configuration item that could have an effect on SnowBe operations and which is approved by management, enhances business process changes (fixes) and minimize risk to IT Services. The scope of this definition includes changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.

Change Management
Change Management refers to the process used to control the lifecycle of all changes.

Change Proposal
A Change Proposal describes a proposed major Change, like the introduction of a new service or a substantial change to an existing service. The purpose of Change Proposals is to communicate a proposed major Change and assess its risk, impact and feasibility before design activities begin.

Change Record
A Change Record contains all the details of a Change, documenting the lifecycle of a single Change. It is usually created on the basis of a preceding Request For Change.

Configuration Item (CI)
A Configuration item is any component or service that is managed in order to deliver an IT service. These include IT services, hardware, software, process documentation, and service level management.

Department Change
Any change that will only affect one department at SnowBe.

Emergency Change
An Emergency Change is a change that must be deployed as soon as possible in order to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs) and state regulations.

Maintenance Window
A Maintenance Window is a period of time designated in advance by the technical staff, during which preventive maintenance that could cause disruption of service may be performed.

Normal Change
A Normal Change is a change that does not have a pre-approved SOP and is not classified as an Emergency Change; it follows the full Change Management Process and has a predefined maintenance window.

Organizational Change
Any change that if implemented will affect either multiple SnowBe departments OR SnowBe customers is considered an organizational change.

Release
A set of new, changed and/or unchanged Configuration Items that are tested and introduced into IT environments together to implement one or multiple approved Changes.

Remediation Plan
Remediation Plans are actions taken to recover after a failed change into production. These plans are required as part of the Release Management process and clearly defines the steps necessary to restore services to its previous level.

Request for Change Form (RFC)
The Request For Change (RFC) is a formal request for the implementation of a Change. An RFC records the details of a proposed Change and must be submitted to Change Management process by the requestor for every non-Standard Change. The document will provide details of the change for approval and prioritization, and a mechanism for ECCG to govern the Change Management process.

Standard Change
A Standard Change is a pre-authorized change that is low-risk, predictable in its outcome and repeatable through defined work instructions in a standard operating procedure (SOP).

Roles & Responsibilities

Compliance (Change) Managers
A Compliance Manager/Change Manager is the person that is responsible for ensuring that changes within their scope are managed from inception through presentation and into implementation. The scope of a compliance manager is either Organizational or Departmental focused. If there are no compliance managers, the Compliance officer will take on these responsibilities.

Departmental Change Control Group (DCCG)
The Departmental Change Control Group is responsible for the oversight of changes to any changes environments that are not organizational changes.

Organizational Change Control Group (OCCG)
The Organizational Change Control Group is charged with overseeing the Change Management

process for each Change and executing enterprise level change decisions. The Compliance Officer will chair with IT department Head as co-chair with a unanimous decision voting method.

Service Owner (SO)
The role that is accountable for the delivery of a specific IT Service. IT managers are the Service Owners for all IT services. Service Owners can delegate decision making for services to leaders within their departments as needed.

Policy

The following guidelines and processes shall be used to both manage and approve any and all changes to any SnowBe provided service, regardless of source or type.
The decision to authorize or reject a proposed change is based on the completed Change Control Management Process, to include proper understanding of the risks associated with either implementing or not implementing the change.
Each type of change [Standard, Normal, and Emergency] (regardless if organizational or departmental) will have specific submission, approval and execution requirements within this policy, including the specific levels of authorization and communication required for each type of change and all rules for assessing and executing Changes.

The objective of the Change Control Management process subsequently outlined is to govern the introduction of standard, normal, and emergency changes into production by insuring that the correct procedures are being followed, proper documentation has been completed, proper testing has been performed, and proper approval is in place.

Standard Changes
All Standard Releases are governed by the pre-approved Standard Operating Procedure (SOP). This SOP must be reviewed by the Service Owner and appropriate compliance managers.

1. **Establish a Standard Change**
    a. In order to establish a Standard Change:
        i. A Standard Operating Procedure must be drafted.
        ii. The change must have been successfully implemented in the past as outlined in the drafted Standard Operating Procedure.
        iii. The change must be repeatable, and its outcome predictable, as outlined in the drafted Standard Operating Procedure.
    b. Once drafted, the Standard Operating Procedure must be presented to Service Owner for review and then to the appropriate compliance manager for approval via email.
    c. If approved, the Standard Operating Procure is published in the approved document library and the change is labeled as “Standard”.
2. **Standard Change(s) Deployment Approval:**
    a. Standard Changes do not require approval by the Vertical Change Control Group but are required to provide notification.
        i. All Standard Changes must be completed in a time frame approved by the Service Owner.
        ii. If no approved Standard Operating Procedure exists, the change must follow the Change Management Process for a Normal or High Priority Change until requirements to “Establish a Standard Change” are completed.

b. Where possible, multiple Standard Changes should be released together and documented in a Schedule of Standard Changes.
  i. The Schedule of Standard Changes should outline all changes to be released during the same window as well as details of the timing for that window
  ii. Even if only one Standard Change is to be completed, a Schedule of Standard Change must be created and communicated.
  iii. A Change Item must be created in the official SnowBe IT service management ticket solution and the Schedule of Standard Changes must be included in the ticket entry.
  iv. The Change ticket entry must have the following fields populated:
    1. Request Type
    2. Classification
    3. Change Scope
    4. Subject
    5. Description
    6. Contact
    7. Priority
    8. Notification
  v. A Completed Request For Change (RFC) form must be attached to the ticket entry.

c. Once drafted, the Schedule of Standard Change will be sent via the service owner approved communication plan to service subscribers/consumers.

d. If no issues or concerns are raised, release of changes may proceed as outlined in the Schedule of Standard Changes. Else, all outstanding issues and concerns must be resolved prior to execution of the change.

3. Deployment to Production

a. At the start of the change window communicated via the Schedule of Standard Changes, the assigned SnowBe employee will communicate via the service owner approved communication plan to service employees/customers notifying recipients that the change window is about to begin.

b. The assigned employee will then execute the approved SOP(s) for all changes planned in the Schedule of Standard Changes.

c. The employee will test each change per the established SOP for each in order to ensure that the desired expectations are met.
  i. If the test fails, the employee will utilize techniques outlined in the SOP to correct the issue.

4. Successful Deployment

a. Upon a successful implementation of the change, the assigned employee will communicate via the service owner approved communication plan to service employees/customers notifying recipients that the changes are complete.

b. The Change Record will be updated to reflect successful completion of the Schedule of Standard Change.

5. Failed Deployment

a. If during the release, one or more of the changes results in a disruption of service or service level, an Incident must be created and the Incident Management Process must be followed.

b. Once resolved and the changes completed, a Post Implementation Review and Root

Cause Analysis must be completed and attached to the appropriate ticket item.

c. Standard Operating Procedures for any change resulting in an Incident must be updated and resubmitted for review and approval.

Normal Changes

A Normal Change does not have a pre-approved SOP, is not classified as an Emergency Change, and can be deployed during a predefined, standard maintenance window. These changes must follow the full Change Management Process as outlined below.

1. **Change Request and Review**
   - a. The Analyst will complete the Request For Change (RFC) Form and a corresponding ticket entry. This includes coordination of impact and risk analysis, test plan and coordination, and identification of affected stakeholders that must approve the RFC.
   - b. The following fields must be completed in the corresponding ticket entry:
     - i. The ticket entry must have the following fields populated:
       - 1. All items for needed for a Standard change. See Standard Changes 2.b.Iv and 2.b.v.
   - c. The completed RFC, including the corresponding ticket number, will be sent to Service Owner and compliance officers, as well as any affected department managers for review, updates and approvals.
   - d. Once approved, the RFC will be submitted to the for inclusion in the next OCCG Meeting Agenda. The Compliance officer will review the RFC to determine readiness for review, priority and timing for ECCG Meeting.
2. ECCG Review and Approval
   - a. Each RFC will be reviewed and voted on by the ECCG
   - b. ECCG will review the RFC as outlined in the section below
     - i. 2.1.2. Upon Approval, the release date / time will be confirmed and documented and a releaser assigned
     - ii. If not approved due to missing or erroneous information, a remediation period is available to correct any outstanding issues
3. **Deployment into Production**
   - a. At the start of the standard or approved change window, the assigned SnowBe employee will communicate via the service owner approved communication plan to service employees/customers notifying recipients that the change window is about to begin.
   - b. The assigned technical employee will then execute the steps as outlined in the change release notes.
   - c. Upon completion of the change implementation, employee will execute the test plan as documented in the RFC.
     - i. If the test fails, the employee will utilize approved troubleshooting techniques to correct the issue including execution of the back out plan based on the criteria and steps outlined in the RFC.
   - d. Upon verifying successful implementation of the change, the technical SME will transition to the appropriate testers for regression and/or post implementation testing as outlined in the RFC.
4. **Post Implementation Testing and Successful Deployment**
   - a. If so documented in the Request For Change, the appropriate departments will execute the test plan as documented in the RFC.

            i. If the desired expectations are met, the assigned employee will be notified.
                1. The employee will update all documentation, including the change ticket and a Post Implementation Review (if required by ECCG), and communicate via the service owner approved communication plan to service employees/customers.
            ii. If the test fails, the technical SME will utilize approved troubleshooting techniques to correct the issue.
                1. If issue resolution does not address the issue within the parameters outlined in the back out plan, the back out plan will be implemented as outlined in the RFC, including communication to appropriate affected resources
            iii. If a Normal Change is low-risk and is likely to reoccur, the applicable governing body or Service Owner will consider whether to request the creation of a SOP to handle this type of change in the future. Once an SOP is created by technical SMEs and approved by ECCG, future changes of this type will be handled as Standard Changes.

5. **Failed Deployment**
    a. If during the release, one or more of the changes results in a disruption of service or service level, an Incident must be created and the Incident Management Process must be followed. 5
    b. Once resolved and the changes completed, a Post Implementation Review and Root Cause Analysis must be completed and attached to the ticket item.

Emergency Change

An Emergency Change is a change that must be deployed as soon as possible in order to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs) and state regulations.

1. **Release Approval**
    a. Once a resolution for the outage and/or severe service disruption has been identified, communications containing details with the issue, proposed resolution, associated ticket numbers, known impact and risk, must be sent to following the Incident Management policy/plan
    b. In addition, the appropriate departments will be notified that a resolution has been identified and an Emergency Change is being planned to resolve it.
    c. The Emergency Change can be executed once the Compliance Officer has approved, verbally or via email.
        i. If no verbal or written approval is received from the Compliance Officer within 30 minutes, the Service Owner will provide approval to proceed.
    d. An email to the entire organization will be sent notifying them of any outage or service disruption that will occur as a result of the Emergency Change window. This will include the service(s) affected and the potential duration of the interruption.
    e. The assigned SnowBe employee will execute the change as outlined in the emergency change documentation.
    f. Upon completion of the change implementation, the employee will execute the test plan as documented in the emergency change documentation.
        i. If the test fails, the employee will utilize approved troubleshooting techniques to correct the issue.

   g. Once service is restored, a notification will be sent following the Incident Management policy/plan.
   h. A separate communication will be sent to the appropriate departments notifying them of resolution and service restoration.
   i. If written approval was not received prior to the emergency change release, retroactive acknowledgement of verbal approval, or acknowledgement that change qualified as an Emergency Change and was appropriate to deploy without approval, will be completed.
   j. Additionally, Change ticket and related Incident tickets in the ticketing system will be updated
   k. The following fields must be completed in the corresponding ticket entry:
      i. The ticket entry must have the following fields populated:
         1. All items for needed for a Standard change. See Standard Changes 2.b.Iv and 2.b.v.

2. **Post Implementation Review and Root Cause Analysis**
   a. All Emergency Changes will require a Post Implementation Review and Root Cause.

Exceptions/Exemptions

Any exceptions or exemptions to the security policies, standards, and procedures outlined in this plan must be documented via email and approved by the Network Administrator and the relevant department manager. Exceptions will be granted on a case-by-case basis and will be subject to periodic review and re-evaluation.

Enforcement

Any exceptions or exemptions to the security policies, standards, and procedures outlined in this plan must adhere to the following criteria;

- All requests must be documented in detail, including the specific reasons for the exception, potential risks involved, and any compensating controls implemented to mitigate those risks.
- Approval must be obtained from the Network Administrator and the relevant department manager, with final oversight and approval by the Director or Manager of Information Technology.
- All exceptions will be granted on a case-by-case basis, documented in a centralized exception tracking system, and reviewed at least quarterly by the Incident Response Team (IRT) to assess any changes in risk or compliance requirements.
- Exceptions that pose significant risks or affect regulatory compliance must be reported to the Compliance Officer for additional review.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	08/26/2024	Danielle Williams		Added policy purpose, scope, definitions, roles and responsibilities, policy, exception/exemptions, as well as enforcement policy.

Citations

Louisiana Department of Administration -

https://www.doa.la.gov/media/lhibcody/ots_change_management_policy.pdf