SNOWBE ONLINE
Policy# CM-01
Change Control Management Policy

Daphnie Bruno

Policy #CM-01 - Version # 1.0

November 14, 2024

Table of Contents

Purpose

Operational change management brings discipline and quality control to SnowBe Online. Attention to governance and formal policies and procedures will ensure its success. Adopting formalized control and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalization requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is nonexistent, it is incumbent on SnowBe Online's senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, SnowBe Online organizations can demonstrate increased agility in responding predictably and reliably to new business demands.

SnowBe Online management has recognized the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy to address the opportunities and associated risks.

Scope

This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices; information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally by the Information Technology Division.
Because the Change Management Process deals with the management of changes in the production environment, it is imperative that both customers and SnowBe Online change organization understand the events that are considered within the scope of the process. In this section, the scope is described and includes areas which are both within and outside of the change management process scope.

a. **In Scope**: The intended scope of the Change Management Process is to cover all the SnowBe Online computing systems and platforms. The primary functional components covered in the Change Management process include:

- SDLC – Changes handled through the formal software development life cycle will be included within the company's change management program.
- Hardware – Installation, modification, removal or relocation of computing equipment.
- Software – Installation, Patches to non-redundant systems, Service Packs, upgrade or removal of software products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed packages and utilities.
- Database – Changes to databases or files such as additions, reorganizations and major maintenance.
- Application – Application changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.
- Moves, Adds, Changes and Deletes – Changes to system configuration.
- Telephony – Installation, modification, de-installation, or relocation of VoIP equipment and services.

• Networking – Installation, modification, de-installation, or relocation of major network services including Firewall and Router changes.

b. **Out of Scope**: There are many Information Service tasks performed at the University, either by the IS department or by the end users that do not fall under the policies and procedures of Change Management. Tasks that require an operational process, but are outside the initial scope of the universities Change Management policy include:

- Contingency/Disaster Recovery
- Changes to non-production elements or resources
- Certain changes to redundant systems including moves, adds, deletes.
- Changes made within the daily administrative process. Examples of daily administrative tasks are:
  - o Password resets
  - o User adds/deletes
  - o User modifications
  - o Adding, deleting or revising security groups
  - o Rebooting machines when there is no change to the configuration of the system
  - o File permission changes
  - o Security Patches
  - o Switch and Wi-Fi hardware swaps

NOTE: The Change Advisory Board (CAB) may modify the scope periodically to include items in the scope of SnowBe Online overall Change Management policy.

Definitions

Authorized Change Windows:
Predetermined time periods during which approved changes can be implemented with minimal impact on operations.

Change Advisory Board (CAB):
A group responsible for reviewing, evaluating, and approving change requests, as well as overseeing their implementation.

Change Control Board:
A group responsible for reviewing and approving changes in an organization's processes or products.

Commercial Off-The-Shelf (COTS):
Software or hardware products that are ready-made and available for sale to the general public.

Data Retention Schedule:
A policy that defines how long different types of data should be kept and when they should be deleted or archived.

Emergency Changes:
Urgent modifications made to resolve critical issues or security vulnerabilities, often implemented immediately and documented retrospectively.

Operational Change Management:
A disciplined approach to making alterations to IT systems, services, or processes to maintain quality control and minimize disruption.

Roll-back Plan:
A strategy to revert a system to its previous state in case a change implementation fails or causes unexpected issues.

Software Development Life Cycle (SDLC):
The process for planning, creating, testing, and deploying an information system.

Voice over Internet Protocol (VoIP):
A technology that allows voice calls to be made using an internet connection instead of a regular phone line.

Roles & Responsibilities

Audit Team:

- Conduct regular audits of the change management process
- Verify compliance with established procedures and policies
- Report findings to management and the Change Advisory Board

Change Advisory Board (CAB)

- Review and evaluate change requests
- Assess risks and potential impacts of proposed changes
- Approve or reject change requests
- Ensure changes align with organizational goals and objectives
- Oversee the implementation of approved changes

Change Implementer

- Execute approved changes according to the implementation plan
- Coordinate with relevant teams during implementation
- Report progress and any issues to the Change Advisory Board

Change Requestor

- Submit change requests with clear justification and details
- Provide additional information as requested by the CAB
- Assist in impact assessment of proposed changes

Compliance Officer:

- Ensure change management processes comply with relevant regulations and standards
- Advise the CAB on compliance-related matters

Contractors/Vendors:

- Adhere to the organization's change management policies when working on systems or processes
- Submit change requests through appropriate channels when necessary

Employees:

- Report any weaknesses or issues in current systems that may require changes
- Comply with change management procedures
- Participate in training related to implemented changes

Human Resources:

- Manage change-related training programs for employees
- Assist in communicating changes that affect staff or organizational structure

Information Security Department:

- Assess security implications of proposed changes
- Ensure changes maintain or enhance the organization's security posture
- Provide input on security-related aspects of change requests

IT Manager:

- Evaluate the impact of changes on IT infrastructure and systems
- Ensure changes align with the broader IT strategy
- Coordinate with the CAB and implementation teams

Security Officer:

- Review change requests for potential security risks
- Provide guidance on security measures for implemented changes
- Ensure changes comply with security policies and standards

System Administrators:

- Assist in developing configuration baselines
- Implement approved changes to systems
- Monitor systems post-change for any issues
- Comply with the change management process for system modifications

Policy

All changes to IT services must follow a standard process to ensure appropriate planning, execution and delivery Changes will be categorized as a standard change, a significant change, a minor change or a major change. Appropriate processes and levels of review shall be applied to each type of change commensurate with the potential of the change to disrupt university operations.

Changes to production SnowBe Online Information Resources must be documented and classified according to their:

- Importance,
- Urgency,
- Impact,
- Complexity

Change documentation must include, at a minimum:

- Date of submission and date of change,
- Owner and custodian contact information,
- Nature of the change,
- Change requestor,
- Change classification(s),
- Roll-back plan,
- Change approver,
- Change implementer,
- An indication of success or failure.

Changes with a significant potential impact to SnowBe Online Information Resources must be scheduled. SnowBe Online Information Resource owners must be notified of changes that affect the systems they are responsible for.

Authorized change windows must be established for changes with a high potential impact.
Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.

Change control documentation must be maintained in accordance with the SnowBe Online Data Retention Schedule.

Changes made to SnowBe Online customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.

All changes must be approved by the Information Resource Owner, Director of Information Technology, or Change Control Board (if one is established).

Emergency changes (i.e. break/fix, incident response, etc.) may be implemented immediately and complete the change control process retroactively.

Exceptions/Exemptions

Exceptions to this Security Plan are only permissible in rare situations where strict adherence would significantly disrupt business operations.

- Any request for an exception must be made in writing to the IT Security Manager.
- The IT Security Manager will evaluate it in collaboration with pertinent stakeholders.
- If granted, the exception will be in place until the policy changes or the person's employment status changes.
- The IT Security Manager and the Risk Management team will perform a detailed risk assessment and put suitable compensation controls in place to reduce potential risks during the exception period.
- The approval of exceptions will depend on these mitigating measures.

Enforcement

Violations of this IT Security Plan will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	14-Nov-24	Daphnie Bruno		Created and updated Document.

Citations

- https://www.montclair.edu/policies/all-policies/account-management-policy/
- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com
    - Used to correct grammar errors and spelling errors
- https://nimonik.com/case-studies-compliance-management/change-management-and-control-policy-nimonik.pdf
- https://frsecure.com/change-management-policy-template/
- https://www.up.edu/is/files/policy-changemanagement.pdf
- https://whatfix.com/blog/change-advisory-board/