SNOWBE ONLINE Policy# CCM1

Change Control Management Policy

Your name: Jedson Jerume

Change Control Management

Policy- Version 1.3

DATE: April 28th 2025

Table of Contents

Purpose

The purpose of the SnowBe Online Change Management / Change Control Policy is to ensure that all changes to SnowBe Online's information resources are appropriately documented, reviewed, approved, and implemented in a controlled manner. This procedure protects the integrity, availability, and security of systems and data, minimizes the risk of disruptions, and ensures compliance with regulatory, contractual, and internal requirements.

Scope

The SnowBe Online Change Management/Change Control Policy applies to any individual, entity, or process that creates, evaluates, and/or implements changes to SnowBe Online's Information Resources. This procedure applies to all SnowBe Online remote workers, permanent and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to SnowBe Online's electronic systems, information, software, and/or hardware.
The terms set out in this procedure work in conjunction with, and do not replace, amend, or supplement any terms or conditions of employment stated in any collective bargaining agreements and/or employment contracts.
This procedure is not intended to restrict communications or actions protected or required by regional/local laws and regulations.

Definitions

Change Advisory Board:
A group of designated individuals responsible for evaluating, approving, or rejecting proposed changes based on their potential impact, urgency, and necessity.
Change Control:
A systematic approach to managing all changes made to SnowBe Online's information resources to ensure minimal disruption to services and accountability for each modification.
Emergency Change:
A change that must be implemented immediately to prevent an ongoing incident, significant risk, or major disruption, with retroactive completion of the change control process.
Information Resource Owner:
The individual or department responsible for the management, oversight, and protection of specific SnowBe Online information systems, data, or technology assets.

Roles & Responsibilities

The Director of Governance, Risk, and Compliance (GRC) and the Chief Technology Officer (CTO) are responsible for the SnowBe Online Security Framework and its associated procedures.
This procedure is reviewed annually by members of the GRC team. Any changes to this procedure must be approved by SnowBe Online's Chief Technology Officer and Director of Governance, Risk, and Compliance prior to its release.
Suggestions for changes to this procedure should be reported to snowbeonline
The Information Technology (IT) department is responsible for managing change management activities for SnowBe Online.
Technology owners are responsible for defining and maintaining technical standards applicable to their operating environments and domains.
All employees, contractors, and third parties who access SnowBe Online's information must abide by this and associated procedures.
Line managers have day-to-day responsibility for enforcing this procedure, and employees should refer any questions about this procedure to their line managers first.
In alignment with their applicable solution groups, SnowBe Online's business units shall develop, disseminate, and maintain formal, documented processes and/or procedures to facilitate the implementation of this procedure and, where applicable, any local or regional access management procedures.
All processes and procedures must remain consistent with applicable laws, executive orders, directives, regulations, and standards.

Policy

Procedure

1. Changes to production SnowBe Online Information Resources must be documented and classified according to their:
    - a. Importance,
    - b. Urgency,
    - c. Impact, and
    - d. Complexity.
2. Change documentation must include, at a minimum:
    - a. Date of submission and date of change,
    - b. Owner and custodian contact information,
    - c. Nature of the change,
    - d. Change requestor,

- e. Change classification(s),
- f. Roll-back plan,
- g. Change approver,
- h. Change implementer, and
- i. An indication of success or failure.

3. Changes with a significant potential impact to SnowBe Online Information Resources must be scheduled.
4. SnowBe Online Information Resource owners must be notified of changes that affect the systems they are responsible for.
5. Authorized change windows must be established for changes with a high potential impact.
6. Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing, along with back-out plans, included in the change documentation.
7. Change control documentation must be maintained in accordance with SnowBe Online's data retention schedules.
8. Changes made to SnowBe Online customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.
9. All changes must be approved by the Information Resource owner, an Information Technology (IT) manager (or delegate), or a Change Advisory Board (if one is established).
10. Emergency changes (i.e., break/fix, incident response, etc.) may be implemented immediately with written senior management and IT management approval and must complete the change control process retroactively.

5. Compliance, Monitoring, and Enforcement

This procedure applies to all SnowBe Online business units, in all countries where operations are conducted.

SnowBe Online seeks to proactively prevent and mitigate instances of non-compliance with this procedure. Compliance will be measured through methods including, but not limited to, risk assessments, business tool reports, and internal and external audits.

Any breaches, concerns, including ethical concerns or potential breaches of information and data protection standards, should be reported as soon as possible through SnowBe Online's Whistleblowing Procedure.

Any need for improvements will be addressed as soon as possible. Employees are encouraged to offer feedback on this procedure if they have suggestions for improvements. Feedback should be directed to GRC@snowbeonline.com.

Any exception to this procedure must be approved in advance by SnowBe Online's Chief Technology Officer (CTO), or their delegate, and/or the Director of Governance, Risk, and Compliance.

Personnel found to have intentionally violated this procedure may be subject to disciplinary action, up to and including termination of employment and other applicable penalties. SnowBe Online reserves the right to pursue any and all legal or civil action in connection with any such violation.

Any vendor, consultant, or contractor found to have violated this procedure may face sanctions up to and including removal of access rights, termination of contracts, and any related civil or criminal

penalties.

6. Acknowledgement

Those who receive this procedure acknowledge its receipt and understanding of its contents; and recognize that SnowBe Online expressly reserves the right to change, modify, or delete its provisions without notice.

Exceptions/Exemptions

Any request for an exception/exemption to any policy, standard, or procedure must:

- Be submitted in writing to the Director of IT or OIS
- Include a clear justification for the request and any compensating controls in place.
- Be reviewed and approved by the Director.
- Include a defined expiration date (no longer than 12 months) after which the exception must be re-evaluated or retired.
- Exceptions do not guarantee approval and may be denied if deemed a critical risk.
- All requests for an Exception/Exemption in policy will be archived even if the request is denied.

Enforcement

Violation of this policy can result in action taken against the employee; this can lead to termination of employment for full-time employees and temporary employees, termination of contracts, and termination of interns and volunteers. Any employee who violates this policy will be subject to a review of their actions, and the severity of the consequences will depend on the nature and frequency of the violation. SnowBe reserves the right to take further action against employees, including legal action, if necessary to protect its interests. The following outlines the actions that will be taken for violating policies here at SnowBe:

- **Level 1 – Verbal Warning and Education**
  Trigger: Minor, first-time policy violations without malicious intent
  Action: The employee receives a verbal reminder and is re-educated on the relevant policy. The incident is documented for record-keeping purposes.
- **Level 2 – Written Warning**
  Trigger: Repeated minor infractions or more serious single incidents
  Action: A formal written warning is issued, detailing the violation, its risks, and expected corrective actions. Additional training may be required.

- **Level 3 – Access Restrictions or Temporary Suspension**
  Trigger: Continued non-compliance or more significant security breaches
  Action: Access to specific systems may be temporarily suspended or restricted. The employee is subject to review and required to complete remedial training.
- **Level 4 – Disciplinary Action and Final Warning**
  Trigger: Serious or repeated violations that pose risks to the organization's systems or data integrity.
  Action: Final written warning issued with clear notice that further violations will result in termination. It may involve HR consultation and a performance improvement plan.
- **Level 5 – Termination and Possible Legal Action**
  Trigger: Egregious or malicious violations such as data theft, sabotage, or deliberate compromise of security systems.
  Action: Immediate termination of employment. Legal action may be pursued if company data, finances, or reputation are harmed.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	April 10th 2025	Jedson Jerume	Group #4	Template Creation
1.1	April 14th 2025	Jedson Jerume	Group #4	Formatting edits
1.2	April 21st 2025	Jedson Jerume	Group #4	More formatting edits
1.3	April 28th 2025	Jedson Jerume	Group #4	Change of version and date.

Citations

Bootlabstech.com – used for Enforcement
https://www.bootlabstech.com/security-policy-enforcement/
Davidson College – used to help with Exceptions/Exemptions
https://www.davidson.edu/offices-and-services/technology-innovation/it-guidelines-policies/information-systems-security-policy
Justia.com - used for Enforcement
https://contracts.justia.com/contract-clauses/enforcement/
Neweratech.com – used for policy template.
https://www.neweratech.com/us/wp-content/uploads/sites/5/2024/11/Change-Management-Change-Control-Policy.pdf