SNOWBE ONLINE

CCMP#1

Change Control Management

POLICY

Your name:
Chris Stevens

Change Control Management

Policy Version # 1.0

DATE: 5-26-2025

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 2

POLICY 3

EXCEPTIONS/EXEMPTIONS 5

ENFORCEMENT 6

VERSION HISTORY TABLE 7

CITATIONS 8

Purpose

The purpose of this Change Control Management Policy is to establish a structured process for managing changes to SnowBe Online's IT systems, applications, and infrastructure to ensure stability, security, and compliance. It aims to minimize risks, prevent unauthorized changes, and maintain the integrity of the AWS-hosted e-commerce platform, customer data, and PCI compliance requirements. This policy outlines procedures for proposing, reviewing, approving, implementing, and documenting changes to safeguard operations and customer trust.

Scope

This policy applies to all SnowBe Online employees, contractors, and third-party vendors who manage, operate, or interact with the company's IT systems, including the AWS platform, on-premises servers, desktops, laptops, and credit card processing systems. It covers all changes to hardware, software, firmware, configurations, and data environments that impact operations or security.

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.

Change Request
A formal proposal to modify IT systems, applications, or configurations, submitted for review and approval.

Configuration Item (CI)
A component of the IT environment (e.g., server, application, database) subject to change control.

Emergency Change
An urgent change required to address critical system failures or security incidents.

IT Resources
Everything to include computing, networking, communications, application, 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.

PCI Compliance
Adherence to Payment Card Industry Data Security Standards for protecting credit card data.

Roles & Responsibilities

Change Advisory Board (CAB)
Reviews and approves/rejects change requests, ensuring alignment with business and security objectives. Comprises IT manager, security officer, and business representatives.

Change Initiator
Any employee or contractor proposing a change, responsible for submitting a detailed change request.

Change Manager
Oversees the change control process, coordinates reviews, and maintains change records. Reports to the IT manager.

IT Manager
Ensures policy compliance, oversees implementation, and escalates emergency changes for approval.

Security Officer
Assesses change impacts on security and PCI compliance, providing recommendations to the CAB.

Policy

SnowBe Online mandates a formal change control process to manage modifications to its IT environment, ensuring stability, security, and compliance with PCI standards. The policy establishes rules, expectations, and procedures for all changes to maintain the integrity of the AWS platform, on-premises servers, and customer data systems.

Items Requiring Change Management Approval

All changes to the following require formal approval through the change control process:

- **Hardware**
  Modifications to servers, desktops, laptops, or credit card terminals (e.g., adding/removing devices, firmware updates).

- **Software**
  Updates, patches, or new installations on the AWS platform, servers, or endpoints (e.g., WordPress shopping cart updates, anti-virus software upgrades).

- **Network Configurations**
  Changes to firewalls, VPN settings, or network devices (e.g., firmware updates, access rules).

- **Applications**
  Modifications to customer relationship management, order management, accounting, or vendor applications.

- **Data Environments**
  Changes to databases storing customer or credit card data (e.g., schema updates, access controls).

- **Security Controls**
  Updates to access management systems, authentication mechanisms, or encryption settings.

- **Emergency Changes**
  Urgent changes to address critical failures or security incidents, requiring expedited approval.

Change Control Process

- **Change Request Submission**
  - Change Initiators submit a change request to the Change Manager, detailing the proposed change, purpose, impact, risks, and rollback plan.
  - Requests must include potential effects on PCI compliance, security, and system availability.

- **Review and Assessment**
  - The Change Manager logs the request and forwards it to the CAB.
  - The Security Officer evaluates security and PCI compliance impacts (e.g., encryption, data protection).
  - The CAB assesses risks, benefits, and alignment with business goals.

- **Approval or Rejection**
  - The CAB approves, rejects, or requests modifications to the change request.
  - Emergency changes follow an expedited process, with post-implementation review by the CAB.
  - Approved changes receive a scheduled implementation window.

- **Implementation**
  - The IT Manager oversees change implementation, ensuring adherence to the approved plan.
  - Changes are tested in a non-production environment (e.g., AWS staging) when feasible.
  - Emergency changes are documented and implemented promptly.

- **Documentation and Monitoring**
  - The Change Manager records all changes, including outcomes, issues, and rollback actions, in a change log.
  - Logs are stored for at least 12 months, with records older than 3 months archived to cloud storage per SnowBe's audit requirements.
  - The Security Officer monitors changes for compliance and security impacts.

- **Post-Implementation Review**
  - The CAB reviews completed changes to verify success and identify lessons learned.
  - Emergency changes undergo a mandatory review to ensure compliance and effectiveness.

Rules and Expectations

- All changes must follow the change control process; unauthorized changes are prohibited and may result in disciplinary action.
- Changes impacting PCI compliance (e.g., credit card data storage, encryption) require Security Officer approval.
- Change requests must be submitted at least 5 business days in advance, except for emergency changes.
- The Change Manager ensures all changes are documented and auditable for PCI compliance.
- Rollback plans are mandatory to mitigate risks of failed changes.
- Employees and vendors must comply with this policy to maintain system integrity and customer trust.

This policy ensures SnowBe Online's IT environment remains secure, stable, and compliant, addressing past deficiencies in technical controls and supporting the company's growth as a public entity.

Exceptions/Exemptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of SnowBe's IT Director and/or IT Manager. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness. Please note that while requesting exceptions or exemptions has been made available to you, it does not guarantee approval.

SnowBe Online recognizes that, under certain circumstances, deviations from this Acceptable Use Policy may be necessary to support specific business needs or technical requirements. Exceptions or exemptions to this policy may be granted under the following conditions:

Risk Acceptance
In some rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and reviewed by IT Enterprise Security and IT Information Systems and approved by the IT Director and/or IT Management. Further details on the risk acceptance process can be obtained through the Enterprise IT Security Department.

Pre-Approval Required
All exceptions must be formally requested in writing and approved by the IT department and an authorized member of management. The request must clearly state the business justification, duration, and potential risks of the exception.

Documentation and Review
Approved exceptions will be documented and maintained by the IT department. All exceptions are subject to periodic review to ensure they remain valid and do not introduce unacceptable risks.

Temporary and Specific
Exceptions are granted on a temporary basis for clearly defined scopes and timeframes. They do not constitute a permanent change to the policy.

No Unauthorized Exceptions
Any deviation from this policy without documented approval is considered a violation and may result in disciplinary action, including suspension of access privileges.

Compliance Priority
Exceptions will not be approved if they compromise SnowBe Online's compliance with legal, regulatory, or security requirements.

Enforcement

Enforcement
SnowBe Online takes the enforcement of this (Policy name) seriously to protect its systems, data, and customers.

Violations of this policy, whether intentional or accidental, may result in disciplinary action, up to and including termination of employment, contract cancellation, and/or legal action.

The penalties will include the following components:

Monitoring and Auditing
SnowBe Online reserves the right to monitor, log, and audit all system and network activity to ensure compliance with this policy. Users should have no expectation of privacy when using company-owned systems or accessing company data.

Incident Investigation
Suspected policy violations will be investigated promptly by the IT department, Human Resources, and other relevant stakeholders. Users are expected to cooperate fully during any investigation.

Corrective Action
If a violation is confirmed, corrective actions will be taken based on the severity and nature of the breach. This may include revocation of access, mandatory training, written warnings, or other disciplinary measures as outlined in the employee handbook.

Legal Consequences
Activities that are illegal under local, state, or federal law may be reported to the appropriate authorities. This includes unauthorized access, data breaches, or misuse of customer financial information.

Appeals Process
Individuals who believe they were unfairly penalized for a policy violation may appeal the decision to management or HR following internal dispute resolution procedures.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	5-26-2025	Chris Stevens	IT Management	Change Control Management Policy Creation

Citations

Bowie State University
https://www.bowiestate.edu/files/resources/information-security-public.pdf
Exceptions/Exemptions

ChatGPT
https://chatgpt.com/c/681bc793-d1dc-800b-a676-cb7b3cf2678d
Exceptions/Exemptions, but as a group we revised the verbiage.

Policy Template
https://www.sans.org/information-security-policy/
Exceptions/Exemptions

NIST SP 800-53 Rev 5, CM-3: Configuration Change Control,
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
Purpose, Scope, Definitions, Role and Responsibilities

Fordham University
https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/change-control-policy/
Purpose, Scope, Definitions