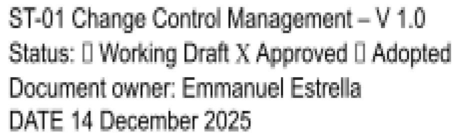
SNOWBE ONLINE
ST-01 CHANGE CONTROL MANAGEMENT

Author: Emmanuel Estrella

Version 1.0

DATE: 14 December 2025



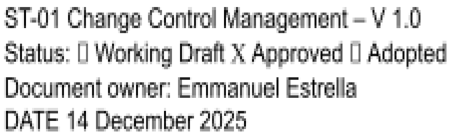
ST-01 Change Control Management – V 1.0

Status: □ Working Draft X Approved □ Adopted

Document owner: Emmanuel Estrella

DATE 14 December 2025

Table of Contents


ST-01 Change Control Management – V 1.0
Status: □ Working Draft X Approved □ Adopted
Document owner: Emmanuel Estrella
DATE 14 December 2025

Purpose

The primary purpose of this Change Control Management Policy is to provide a structured, standardized, and auditable framework for managing all modifications to SnowBe Online's critical IT infrastructure and applications. This policy enforces a mandatory process of request, review, testing, and approval for every change, from core network configurations and database schema updates (including AWS-hosted systems) to application code deployments on the front-end shopping website. Adoption of this policy is required to prevent unauthorized or untested changes that could lead to system outages, introduce security vulnerabilities, or cause data corruption, thereby protecting customer trust, ensuring continuous adherence to PCI DSS and NIST standards, and establishing the stable, reliable operational environment essential for the company's planned public offering.

Scope

This Change Control Management Policy applies to everyone (employees, contractors) and everything (automated computer programs) that makes a modification. It covers every piece of technology we use, including our entire setup in the AWS Cloud (where our website and databases live), all the physical servers we have in our offices, the code and design of our online shopping website, all our security and internet gear (like firewalls and routers), and any updates to the software and settings on our company computers. Nothing gets changed in our live, working environment until it has been properly reviewed and approved by the Change Control Board (CCB).

Definitions

Application Code
The specific set of instructions written by programmers that tell a piece of software (like the shopping website) exactly how to function.

Auditable Framework
A set of rules and documents that creates a clear record, allowing someone to easily check and verify every step of a process.

Automated Computer Programs
Tasks or programs that run by themselves on a computer without needing a person to manually control them every time.

AWS-hosted Systems
Computer services, like the website or data storage, that are running on **Amazon Web Services**, which is a remote computing service (the "Cloud").

CDE (Cardholder Data Environment)
The entire part of the company's network that stores, processes, or transmits credit card information.

CCB (Change Control Board)
The official committee of managers and experts who must review and approve all major changes before

they can be implemented.

Change Control Management
A formal process used to make sure that every change to the company's computers or programs is planned, checked, and approved safely.

CIO (Chief Information Officer)
The senior manager responsible for overseeing all of the company's technology systems.

CISO (Chief Information Security Officer)
The executive responsible for the entire security program and risk management for the company's data and systems.

Compensating Controls
Alternative security measures or protections put in place when a standard policy requirement cannot be met.

Data Corruption
The accidental damage or altering of data, which makes the original information incorrect or unusable.

Database Schema
The basic, organized plan or structure for how information is set up and stored in a computer database.

Disciplinary Action
The formal steps taken by the company to correct or punish an employee who has broken a rule or policy.

E-commerce
Business transactions, like buying and selling, that are conducted over the internet.

Endpoint
Any device that connects to the company's network, such as a desktop computer, a laptop, or a phone.

Executive Management Team
The highest-level group of leaders (like the CEO and CFO) who make the major decisions for the company.

Firmware
The basic, low-level software permanently programmed into a piece of hardware (like a router) that tells it how to start up and function.

Framework
A basic structure or set of rules that guides how a plan, like this policy, should be put together and followed.

Granular Access Management Controls
The detailed rules and tools used to decide *exactly* which specific users are allowed to see or use specific

files and systems.

Hardening
Making a computer system or network more secure by removing unnecessary functions and tightening security settings.

IT Infrastructure
The entire collection of all the hardware and software (like servers, computers, networks, and applications) that SnowBe Online uses to run its business.

Logical Position Where a system sits or connects within the larger network structure, as opposed to its physical location.

NIST Standards
A highly respected set of detailed security guidelines from a U.S. government agency that helps organizations like SnowBe Online manage their risks and protect their data.

Non-Production Environment
A safe, separate testing area (like "Development" or "Staging") used to check changes before they are allowed to go live.

Patching
The process of applying small updates to software to fix problems, improve security, or correct flaws.

PCI DSS
A strict set of security rules that any company must follow if it handles, processes, or stores credit card information.

Production Environment
The live system that customers and employees use every day, such as the active online store or the live customer service software.

Production Resource
Any part of the computer system that is actively being used by customers or employees to do real work.

Security Posture
The overall health and readiness of the company's defenses against potential cyber threats.

Security Vulnerabilities
Weaknesses or flaws in a system's security that could potentially be exploited by a malicious person or program.

Service Management Ticketing System
The official computer program used to track and manage requests for help or simple IT changes.

Staging Environment
A non-production testing area that is the final stop before a change goes live, designed to perfectly match the live system.

System Outages
Times when a computer system stops working or goes down, making it unavailable to users or customers.

VPN (Virtual Private Network)
A secure, encrypted connection that allows someone to safely access a private company network over the public internet.

Roles & Responsibilities

The security and protection of SnowBe's IT resources are a shared responsibility, mandated by the Executive Management Team and enforced throughout the organization.

Executive Management & Owners

- **SnowBe Owners/Management Team:**
  - Holds ultimate accountability for funding the security overhaul required to take the company public.
  - Must formally approve the budget necessary to address all consultant-identified fixes (e.g., software licensing, staff training).
  - Required to officially endorse and enforce new security policies to replace the previously "laid-back culture."
- **Chief Information Officer (CIO):**
  - Serves as the single point of contact responsible for the overall security posture and logical position of SnowBe's core infrastructure.
  - Must be formally notified of any significant security changes made by other entities connected to SnowBe's network (as defined in the Scope).

Technical Operations & Maintenance

- **E-commerce & AWS Team:**
  - Responsible for the security, patching, and hardening of the AWS platform hosting the website and online store.
  - Must immediately update the company's WordPress shopping cart.
  - Holds primary responsibility for the security of the website database where credit card and customer history are stored, driving immediate PCI compliance efforts.
- **Server & Network Administration:**
  - Responsible for physical security by locking the servers in a secured area of the office.
  - Must immediately update the firmware of all network devices.
  - Responsible for applying patches for all Windows servers.
  - Must correct the broad access issue by implementing granular Access Management controls on all servers (on-premise and AWS).
- **Endpoint & Systems Management Team:**
  - Responsible for applying patches for all PCs and laptops (desktops/laptops in LA office and

  - remote sales laptops).
  - Must update the Anti-Virus and backup software across all endpoints.

Users & Enforcement

- **Technical Consultant:**
  - Provides initial oversight and strategic direction for implementing the NIST 800-53 framework.
  - Responsible for guiding internal teams through the urgent steps needed to achieve system control and PCI compliance.

- **All Employees (Sales, Accounting, Customer Support):**
  - Must adhere to all new security policies, especially those related to restricted Access Management on servers and systems.
  - Must enforce the security of the devices they use for work (e.g., Laptops using the VPN connection).
  - Responsible for immediately reporting any security incidents or suspicious physical activity.

Policy

1. **Change Documentation and Tracking**
   All modifications to SnowBe Online's IT infrastructure, applications, and services (including the AWS platform, on-premise servers, and end-user devices) must be fully documented using the formal Change Control Process.
   - **Routine Work:** Simple, very low-risk changes (like adding a user account, changing a password, or updating a record) will be tracked directly within the existing service management ticketing system.
   - **Normal, Planned, and Emergency Changes:** All changes that affect the live production environment, customer experience, or core security posture must be formally tracked in the dedicated Change Management tracking system.
   - **Vendor-Driven Changes:** Significant updates or security alerts for third-party services (like major WordPress upgrades or AWS maintenance notices) should be entered into the Change Management System when SnowBe Online receives prior notice, allowing for impact assessment.

2. **Mandatory Change Process**
   Every modification to a SnowBe Online production resource must follow the Change Management process to ensure proper submission, approval, planning, testing, and implementation.
   - **Testing in Non-Production:** Before any change is submitted for production approval, it must be successfully applied, thoroughly tested, and verified in a non-production environment (e.g., Development, Test, or Staging) when one exists. This is critical for changes affecting the WordPress shopping cart, databases, and core server configurations.
   - **Non-Production Exception:** Changes to development, testing, or quality assurance (QA) environments generally do not require a change request unless the system contains sensitive customer data or involves a major upgrade that could impact future production deployment.

3. **Impact and Risk Examination**
   Before any change request for the production environment is submitted to the Change Control Board (CCB), the initiator must complete a mandatory impact examination. This information is required to help the CCB evaluate the risk and necessity of the change by considering:
   - The impact on business services, such as whether the change (e.g., a server patch or firmware update) is expected to cause an outage, connectivity loss for storefronts, or reduced functionality for sales or customer support.
   - The risk of delaying the change, especially for critical security items such as the need to update network device firmware, apply server patches, or address critical vulnerabilities in the WordPress shopping cart.
   - The risk if the change fails, including the plan to immediately revert the system to its previous, working state.
   - The predictability of the change's success, based on prior testing and proven procedures.

4. **Critical Systems and Data Requirements**
   - **CCB Composition:** The Change Control Board (CCB) must include key representatives from all functional areas, including Information Security (the Consultant), Infrastructure/Networking, and Customer Support to ensure full awareness of business impact.
   - **Sensitive Data**: Any change affecting systems that store, process, or transmit sensitive data (specifically, credit card numbers, customer purchase history, and login audit records) requires additional lead time for security review. This ensures compliance with PCI DSS and NIST standards.
   - **User Experience:** Significant changes to the customer-facing website (WordPress cart) or internal applications must be reviewed by the CCB and communicated in advance to all affected sales, customer support, and office teams via internal communication channels.

5. **Review and Improvement**
   - **Post-Incident Review:** A formal "lessons learned" session must occur after any incident (outage, security issue, or data loss) that resulted from a failed change request or from an unauthorized, undocumented change. The goal is to improve the process and prevent recurrence.

Exceptions/Exemptions

Exceptions or formal exemptions to the requirements defined within this IT Security Plan must be approved through a formal, tiered process reflecting the company's new status as a publicly traded entity requiring strict PCI DSS and NIST 800-53 adherence.

- **Approval Authority:**
  - All minor exceptions must be formally documented and approved by the Chief Information
  - Security Officer (CISO) or the Head of IT who manages the security program.
  - Any exception that significantly increases the risk to the Cardholder Data Environment (CDE) or severely compromises a mandated NIST 800-53 control must also receive final approval from a member of the Executive Management Team (CEO, COO, or CFO).

- **Documentation and Review:**
    - All exceptions will be formally documented, including the business justification, compensating controls (alternative protections) in place, and the duration of the exemption.
    - All plan exceptions will be reviewed on a periodic basis (no less than annually) or whenever the system configuration or underlying business justification changes, to enforce continued appropriateness.

Enforcement

SnowBe Online requires all employees, contractors, vendors, and partners to follow the security policies and procedures outlined in this document. Failure to comply with these requirements may result in disciplinary action, which can include retraining, loss of access privileges, formal warnings, or termination of employment, depending on the severity of the violation. Individuals who create risks to company systems, customer data, or operations may face legal consequences if their actions are intentional, expose data, or cause financial damage.

All employees are required to immediately report any suspected policy violations, security incidents, or improper data handling to the appropriate manager or security team. SnowBe reserves the right to monitor system activity and investigate potential breaches of policy at any time. Using SnowBe's systems and resources, all users acknowledge and accept their responsibility to maintain a secure computing environment.

Version History Table

Version #	**Implementation Date**	**Document Owner**	**Approved By**	**Description**
1.0	14 December 2025	Emmanuel Estrella	Management	Added Purpose, scope, definitions, roles and responsibilities, exceptions/exemptions, policy, enforcement, and citations.

Citations

(Used in Exceptions/Exemptions, Enforcement, Roles & Responsibilities, Definitions, Introduction)
Google. (2025). *Gemini* (Flash 2.5) [Large language model]. Retrieved December 14, 2025, from https://gemini.google.com/

(Used in Policy, Purpose and Scope)
IT Change Management Policy. (n.d.). Retrieved December 14, 2025, from https://www.stthomas.edu/about/departments/general-counsel/policy-pdfs/it-change-management-policy.pdf

(Used in Purpose and Scope)
Guidelines to Writing an Effective Policy Statement. (n.d.). Retrieved December 14, 2025, from https://www.archercenter.org/uploads/3/1/1/3/31139795/policy_statement_outline.pdf