SNOWBE ONLINE Policy# CM-3

Change Management Policy

Humberto Gonzalez

Version # 3.0

DATE: July 21, 2024

Table of Contents

Purpose

The SnowBe Online Change Management Policy establishes the standards for creating, evaluating, implementing, and recording changes to SnowBe Online Information Resources.

Scope

This policy applies to all individuals, entities, and processes that create, evaluate, or execute changes to SnowBe Online's information systems.

Definitions

Impact: The extent of the damages resulting from an adverse event (i.e. realized threat) affecting Company Information Resources.

Information Resource: An asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can be stored in many forms, including hardware assets (e.g. workstation, server, laptop) digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means including courier, electronic or verbal communication. Whatever form information takes, or how the information is transmitted, it always needs appropriate protection.

Information Resource Owner: the person, department, or entity responsible for classifying and approving access to an Information Resource.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Roles & Responsibilities

- Employees: Must comply with change management regulations and report any suspicious activity or violations.
- IT Department: Responsible for managing the technical parts of the change management program, such as change control implementation and maintenance, system updates, and documentation.
- Senior Management/Executive Team: Sets the tone and direction for change management, and allocates resources to manage information changes successfully.
- Third-Party Vendors: Must comply with SnowBe Online's change management standards and ensure that their access is limited to only the resources required for their job. Access concerns or breaches must be notified immediately.

Policy

Production Changes for SnowBe Online Information Resources must be documented and classified as follows:

- Importance
- Urgency
- Impact
- Complexity

Change documentation should include the following information:

- Submission date and change date
- Contact information for the owner and custodian
- Description of the change
- Requestor of the change
- Change classification(s)
- Roll-back plan
- Approver of the change
- Implementer of the change
- Success or failure indication

Significant modifications must be properly scheduled, and information system owners must be notified of changes that affect their systems. High-impact modifications require authorized change windows. Complex and high-impact changes must document usability, security, impact testing, and backup preparations. Change control records must adhere to SnowBe Online's Data Retention Schedule. Changes to client environments or applications must be disclosed to them in compliance with any agreements or contracts.

All changes must be approved by:

- The Information Resource Owner
- The Chief Information Officer
- Senior IT executive

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
3.0	07/21/2024	Humberto Gonzalez	Robin Groff Alarcon	Change Control Management Policy Implemented.

Citations

Change Control Management- Microsoft Word - Information Services Digital Letterhead.docx (up.edu)

Change Management Policy Template | FRSecure

Definitions- Information Security Definitions: Appendix A | FRSecure

Enforcement- Sample Detailed Security Policy (bowiestate.edu)

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

NIST SP 800.53 R5- Security and Privacy Controls for Information Systems and Organizations (fso-lms4-immortal-assets.s3.us-east-1.amazonaws.com)

Purpose/Introduction- Michigan Technological University Information Security Plan (mtu.edu)

Roles & Responsibilities- Sample Detailed Security Policy (bowiestate.edu)