SNOWBE ONLINE

SP-3 Change Management

Version 2.0

02/25/2023

1. Purpose

The SnowBe Online Change Management Policy aims to establish the rules for creating, evaluating, implementing, and tracking changes made to SnowBe Online Information Resources.

2. Scope

The SnowBe Online Change Management Policy applies to any individual, entity, or process that creates, evaluates, and/or implements changes to SnowBe Online Information Resource.

3. 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 must 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 or how the information is transmitted, it always needs appropriate protection.

4. Roles and Responsibilities

All Employees:

- Responsible for reporting any potential issues or concerns related to a change. They should also adhere to all established policies and procedures related to change management and actively participate in the change management process when required.

Business Owner:

- Responsible for providing feedback and approval on proposed changes that may impact their area of responsibility. They are also responsible for ensuring that any changes that affect their area of responsibility are implemented to minimize disruption to business operations.

Change Management Team:

– Responsible for reviewing and approving all changes, ensuring that each change adheres to the established policies and procedures. They are also responsible for coordinating and communicating with all stakeholders during the change process, tracking and reporting on the status of changes, and ensuring that all changes are properly documented.

IT Staff:

– Responsible for providing technical support and expertise during the change process. They also ensure all changes are tested and implemented per established policies and procedures.

5. Policy

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 the 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 on 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 complexity must include usability, security, impact testing, and back-out plans in the change documentation.
7. Change control documentation must be maintained per the SnowBe Online Data Retention Schedule.
8. Changes to SnowBe Online customer environments and/or applications must be communicated to customers per governing agreements and/or contracts.

9. All changes must be approved by the Information Resource Owner, Director of Information Technology, or Change Control Board (if one is established).
10. Emergency changes (i.e., break/fix, incident response, etc.) may be implemented immediately and retroactively to complete the change control process.

6. Exemption

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should expressly state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions, and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

7. Enforcement

Employees who violate this policy may be subject to appropriate disciplinary action, including discharge and civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

Version History

Version #	**Change Date**	**Document Owner**	**Approved By**	**Description**
1.0	02/19/2020	SnowBe Online	SnowBe Online	First Draft
2.0	02/25/2023	SnowBe Online	SnowBe Online	Fixed version number spacing date missing on the cover page, formatting, and roles and responsibilities. Changed header to make it smaller

Citation

FRSecure