SNOWBE ONLINE
CHANGE CONTROL
MANAGEMENT POLICY

Your name: Jacob Barrera Section 01

CHANGE CONTROL

MANAGEMENT POLICY

Version 1.2 DATE: 12/17/2024

Table of Contents

Purpose

This policy is aimed at setting a standard procedure for the management of changes for IT systems and business operations to minimize disruption and maintain integrity, security, and safety of systems. The policy scope involves all changes being assessed, authorized, implemented, and reviewed in a controlled manner that up keeps reliability and security for operations of SnowBe Online.

Scope

The policy pertains to all employees, contractors, and third-party service providers involved in any initiation, approval, or implementation of the change of SnowBe Online's systems and procedures. This includes senior management, middle management, operational teams, and outside partners and vendors involved in the lifecycle of managing changes. The policy ensures that each and every individual and entity engaged in the activities of change management will follow the standard procedures that will enhance security, stability, and efficiency in the IT infrastructure of SnowBe Online, as well as its business operations. All departments and collaborations shall be included in this wide scope for handling changes with regularity and effectiveness.

Definitions

Change Request: A formal request for the alteration of a system or process.

Change Advisory Board (CAB): Group that reviews and approves change requests.

Emergency change: Change that must be implemented immediately because of its critical nature.

Rollback: Reversing a system to its original state in cases of change failure.

Roles & Responsibilities

Chief Information Security Officer (CISO)

- Lead the company's security efforts and make sure they meet business and legal requirements.
- Approve security policies and handle major security issues.
- Report on security risks and incidents to the leadership team.

Department Managers

- Approve employee access based on job needs.
- Let the IT Department know if someone's role changes or they leave the company.
- Make sure their teams follow the security rules.

Employees

- Follow security rules and training.
- Use strong passwords and keep accounts private.
- Report anything suspicious or unusual to IT.
- Keep company devices secure and use them responsibly.

IT Department

- Set up and manage security tools like firewalls, antivirus, and encryption.
- Control and monitor access to company systems and data.
- Fix security issues and keep systems updated.
- Watch for threats and respond quickly to security problems.

Security Team

- Check for risks and find ways to improve security.
- Keep an eye on the network for unusual activity.
- Plan and test how the company will respond to security incidents.
- Train employees to stay safe online.

Technical Consultant

- Employs controls using the NIST 800-53 framework and presents security advancement suggestions.

Third-Party Vendors

- Follow SnowBe Online's security rules and agreements.
- Use company systems only for approved tasks.
- Report any security issues immediately.

Policy

This policy shall lay down the framework for controlling and coordinating the implementation of changes. It would involve the following steps:

Change Identification: All changes shall be appropriately documented through CRF.

Impact Assessment: Assess the potential risks and impacts of changes. Also, assess any potential benefits that might accrue from the proposed change.

Approval Process: Changes shall be subjected to the review and approval of the CAB. Emergency changes may be approved by designated emergency change authority.

Implementation Planning: Detailed planning of implementation with timelines, roll-out procedures, resource allocation, etc.

Documentation: Detailed record maintenance of all change requests, approvals, implementation steps, and outcomes.

Communication: The scope of the change, when it would be implemented, and possible ramifications should be communicated to all the right people.

Monitoring and Review: Monitor to ensure that the change is being implemented in the right way; then, review the effects after the change has been completed and document the lessons from that.

Exceptions/Exemptions

Exceptions and exemptions to SnowBe Online's security policies are granted on a case-by-case basis and are not guaranteed. Each request will be carefully evaluated to ensure it aligns with the company's overall risk management strategy and compliance requirements. Approved exceptions or exemptions must not create unacceptable security risks or regulatory violations and will be subject to regular review.

1. **How to Request an Exception or Exemption**
    - Submit a written request detailing the policy or control in question, the reason for the request, proposed mitigations, and the requested duration via the designated request platform (e.g., Service Desk or email to IT Security Team).
2. **Why an Exception or Exemption is Requested**
    - Provide a clear justification, including specific business, technical, or operational reasons that make adherence to the policy impractical or detrimental.
3. **Who Can Approve an Exception or Exemption**
    - Exceptions or exemptions must be approved by the IT Director or IT Manager. In some cases, approval may also require input from the Risk Management or Compliance team.
4. **How Long the Exception or Exemption Will Be in Place**
    - Specify the duration of the exception or exemption, including an expiration date. Temporary exceptions will be reassessed before renewal or termination. Permanent exemptions must undergo periodic review to ensure continued relevance and safety.

Enforcement

All individuals accessing Company data at SnowBe must adhere to international, federal, and state laws and comply with all related Company policies and methods concerning the security of high sensitive data. Any Company employee, non-employed individual, vendor, consultant, or contractor with access to company data found involved in unauthorized use, disclosure, alteration, destruction of data will be charged with a violation of this policy and may have to face appropriate disciplinary action. The penalties increase according to the severity of the offense; thus,

Verbal Warning: Minor infractions or the first offence may attract verbal warning only affecting the offender.

Written Warning: Repeat or serious offences shall be dealt with through formal written warning documented in the individual file.

Temporary Suspension of Access: The Company reserves the right to temporarily suspend access to Company data and IT resources pending investigation further.

Training: He shall undergo mandatory security and compliance training before being allowed access to Company resources.

Suspension or Barring: An immediate suspension of Company data and IT resources may prohibit any user found in violation and repeated or gross violation thereof from further access to Company data and IT resources.

Termination of Service or Employment: In the case of serious breach, service or employment may be terminated.

Legal Action: Any gross violation shall attract civil/criminal sanctions including fines and/or imprisonment as may be prescribed under any relevant law.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	12/2/2024	Jacob Barrera	Jacob Barrera	Created
1.1	12/4/2024	Jacob Barrera	Jacob Barrera	Updated
1.2	12/17/2024	Jacob Barrera	Jacob Barrera	Created change control management policy

Citations

https://frsecure.com/physical-security-policy-template/

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

https://www.up.edu/is/files/policy-changemanagement.pdf