SNOWBE ONLINE 11.12
CHANGE CONTROL MANAGEMENT

Alex Fhermaye

11.12 Change Control

Management - 1.0

DATE: Jun 24, 2024

Table of Contents

Purpose

The Change Control Management policy of SnowBe is designed to establish systematic procedures and guidelines for managing changes to our organization's IT infrastructure, applications, and related processes. The primary objective of this policy is to ensure that all changes are implemented efficiently, securely, and with minimal disruption to business operations. By adhering to this policy, SnowBe aims to achieve the following objectives:

1. **Minimize Disruptions:** Ensure that changes to IT systems and services are planned and executed in a manner that minimizes disruptions to business operations, thereby maintaining high availability and reliability.

2. **Enhance Security:** Implement changes in a secure manner to safeguard SnowBe's sensitive data, intellectual property, and infrastructure from unauthorized access or vulnerabilities.

3. **Compliance:** Ensure that all changes comply with relevant regulatory requirements, industry standards, and internal policies to mitigate risks and uphold corporate governance.

4. **Quality Assurance:** Maintain the integrity and performance of IT systems by conducting thorough testing, validation, and risk assessments before implementing changes into production environments.

5. **Accountability:** Clearly define roles, responsibilities, and approval processes to ensure accountability throughout the change lifecycle, from request through implementation and post-implementation review.

6. **Continuous Improvement:** Foster a culture of continuous improvement by analyzing the outcomes of changes, identifying opportunities for optimization, and incorporating lessons learned into future change management practices.

7. **Communication:** Facilitate effective communication and collaboration among stakeholders, including IT teams, business units, and third-party vendors, to align change initiatives with strategic business objectives.

Scope

This Change Control Management policy applies to all aspects of SnowBe Online's IT infrastructure, systems, applications, and processes. It encompasses the management of changes across the entire organization, including but not limited to, online sales platforms, customer databases, and physical storefronts in the U.S. and Europe.

The scope of this policy includes the following key areas:

Website and Online Sales Platform: All changes to the SnowBe Online website, housed on the AWS platform, must adhere to this policy. This includes updates to the website's infrastructure, credit card processing systems, customer data storage, and any modifications to the WordPress shopping cart.

Customer Data Management: Any changes involving the storage, access, and management of customer information and purchase history must comply with this policy to ensure data integrity, security, and compliance with regulatory requirements such as PCI DSS.

Physical Storefronts: Changes to the credit card processing systems, including bank-provided terminals, and any updates to the hardware or software used in the U.S. and European storefronts are included in the scope of this policy.

Office IT Infrastructure: This policy applies to the twenty desktops and thirty laptops used in the Los Angeles main office, including updates to firmware, operating systems, antivirus software, and backup solutions. Additionally, it covers the VPN connections used by laptops to access company applications remotely.

Server Management: All changes to the six servers, both on-premises and on AWS, used for access management, storage, customer relations management, order management, accounting, and vendor applications, fall under this policy. This includes physical security measures, firmware updates, and access control processes.

Access Management: The policy governs changes related to the access management system, ensuring that only authorized personnel have access to specific data and systems, and implementing necessary processes to enforce these controls.

Compliance and Security Updates: This policy ensures that all changes necessary to maintain compliance with relevant standards, such as PCI DSS, and to enhance security measures, such as login audit record management and cloud storage archiving, are managed appropriately.

Definitions

Access Controls:
Security techniques and measures that regulate who or what can view or use resources in a computing environment.

Availability:
The assurance that information and resources are accessible to authorized users when needed.

Compliance:
The act of adhering to and demonstrating adherence to laws, regulations, guidelines, and specifications relevant to its business processes.

Confidentiality:
The assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Information Assets:
Data, images, text, or software stored on hardware, paper, or other storage media that hold value to SnowBe Online.

Integrity:
The assurance that information is accurate, complete, and has not been altered in an unauthorized manner.

IT Security Advisory Committee:
A group of individuals within an organization tasked with advising on matters related to IT security policies, practices, and procedures.

IT Security Exception Request Form:
A formal document used to request deviations from established IT security policies.

Legal, Regulatory, and Industry Standards:
Set of laws, regulations, guidelines, and specifications established by regulatory authorities or industry groups to ensure security, privacy, and operational efficiency.

NIST 800-53:
A publication that provides a catalog of security and privacy controls for federal information systems and organizations.

Patch:
A piece of software designed to update or fix problems with a computer program or its supporting data, including fixing security vulnerabilities and other bugs.

PCI DSS (Payment Card Industry Data Security Standard):
A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

Risk Assessments:
The process of identifying, evaluating, and estimating the levels of risk involved in a situation, followed by coordinated efforts to mitigate and manage the risk.

Security Controls:
Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

Security Incidents:
Events that indicate that an organization's systems or data may have been compromised or that measures put in place to protect them may have failed.

Security Posture:
The overall security status of an organization's software, hardware, services, networks, information, and systems.

Security Threats:
Potential events or actions that could cause harm to information systems through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Technology Infrastructure:
The composite hardware, software, network resources, and services required for the existence, operation, and management of an enterprise IT environment.

Roles & Responsibilities

Chief Information Officer (CIO)

- Develop and implement the overall IT security strategy in alignment with business objectives.
- Oversee the IT department to ensure effective execution of security policies and controls.
- Ensure compliance with industry standards and regulatory requirements, including NIST 800-53 and PCI DSS.

Compliance Officer

- Ensure the company adheres to all relevant legal, regulatory, and industry standards.
- Conduct regular audits and assessments to identify compliance gaps.
- Work with other departments to implement corrective actions and maintain compliance.

IT Consultant

- Provide expert advice and guidance on IT security best practices and frameworks.
- Conduct risk assessments and develop action plans to address identified vulnerabilities.
- Assist in the implementation of security controls, policies, and procedures.

IT Security Manager

- Oversee the day-to-day operations of IT security within the company.
- Manage the IT security team and ensure the implementation of security controls and measures.
- Monitor security incidents and respond to breaches or threats.

Sales Team

- Adhere to IT security policies and procedures, particularly when accessing company systems remotely.
- Report any suspicious activities or potential security incidents to the IT security team.
- Ensure the secure handling of customer data and payment information during transactions.

System Administrator

- Manage and maintain servers, ensuring they are secure and up-to-date.
- Implement and enforce access controls to limit data access based on roles and responsibilities.
- Regularly update and patch operating systems and software to mitigate vulnerabilities.

Web Developer

- Ensure the company's website and applications are secure and up-to-date.
- Implement security measures for online transactions and data storage.
- Regularly update and patch the WordPress shopping cart and other web components.

Policy

SnowBe Online is committed to managing changes to its IT infrastructure, systems, applications, and processes in a controlled, efficient, and secure manner. This Change Control Management policy outlines the principles, responsibilities, and procedures for handling changes to ensure the integrity, availability, and security of SnowBe Online's operational environment.

1. **Change Request and Documentation:**

   All changes must be formally requested and documented using a standardized Change Request form. This documentation should include a detailed description of the change, the rationale, the expected impact, risk assessment, and rollback procedures.

2. **Approval Process:**

   All change requests must undergo a thorough review and approval process before implementation. The Change Advisory Board (CAB), consisting of key stakeholders and technical experts, will evaluate each change request based on its potential impact, risks, and benefits.

3. **Risk Assessment:**

   A comprehensive risk assessment must be conducted for each proposed change to identify potential threats and vulnerabilities. Mitigation strategies must be developed and documented as part of the change request.

4. **Testing and Validation:**

   All changes must be tested in a controlled environment to ensure they function as intended and do not introduce new issues. Testing results must be documented, and any identified issues must be resolved before moving the change to production.

5. **Implementation:**

   Approved changes must be implemented according to the predefined plan, including detailed steps, assigned responsibilities, and a clear timeline. All implementation activities must be documented, and progress should be monitored to ensure adherence to the plan.

6. **Communication:**

   Effective communication is essential throughout the change process. All stakeholders, including affected business units and end-users, must be informed of the planned changes, potential impacts, and implementation schedule.

7. **Post-Implementation Review:**

   After a change has been implemented, a post-implementation review must be conducted to evaluate the success of the change. This review should assess whether the change objectives were met, identify any issues, and document lessons learned to improve future change management processes.

8. **Emergency Changes:**

   In the event of an emergency requiring immediate changes to address critical issues, an expedited approval process must be followed. Emergency changes must still be documented, reviewed, and subjected to a post-implementation review.

9. **Access Control:**

   Access to systems and data must be restricted based on roles and responsibilities. Changes related to access control must be carefully managed to ensure that only authorized personnel have access to sensitive information and critical systems.

10. **Compliance and Security:**

    All changes must comply with relevant regulatory requirements, industry standards, and internal security policies. Special attention must be given to maintaining PCI DSS compliance for handling and storing credit card information.

Exceptions/Exemptions

At SnowBe Online, we recognize that there may be exceptional circumstances requiring deviations from our established IT security policies. However, such exceptions/exemptions are not guaranteed approval and must be carefully evaluated to ensure they do not compromise our security posture. The following outlines the process for requesting and managing exceptions/exemptions:

How to Request an Exception/Exemption

1. All requests for exceptions or exemptions must be submitted in writing via the official IT Security Exception Request Form, available on the company net.

2. A detailed explanation of why the exception or exemption is being requested, including the specific policy or control from which the deviation is sought. The proposed duration for which the exception or exemption is needed.

Approval Process

1. The IT Security Manager will review the request to ensure it includes all required information and assess the potential risks and impacts.

2. The Chief Information Officer (CIO) has the final authority to approve or deny exceptions and exemptions. In cases involving significant risk, the CIO may consult with the Chief Executive Officer (CEO) or the IT Security Advisory Committee.

3. The applicant will be notified in writing of the decision, including any conditions or additional controls required as part of the approval.

Duration and Review

1. Approved exceptions or exemptions will typically be granted for a specified duration, not exceeding one year unless otherwise stated.

2. All active exceptions or exemptions will be reviewed periodically by the IT Security Manager to ensure that they remain necessary and that any associated risks are being adequately managed.

Enforcement

Compliance with the IT security policy and any granted exceptions or exemptions will be monitored continuously. Any deviations from approved exceptions or exemptions must be reported immediately to the IT Security Manager.

Failure to follow the IT security policy, including the proper procedure for requesting and adhering to exceptions or exemptions, may result in disciplinary actions. Penalties may include, but are not limited to, revocation of access privileges, formal reprimand, or other disciplinary actions up to and including termination of employment.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	June 24, 2024	Alex Fhermaye	Sammy Hernandez	Policy document created

Citations

Change management control procedure - rhode island ... (n.d.-c). https://itservices.risd.edu/OIT/Documents/Change_Management_Control_Procedure.pdf

Sample it change management policies and procedures ... (n.d.-d). https://cdn2.hubspot.net/hub/22769/file-13442568-pdf/docs/sample

CSUSTAN. (n.d.-d). https://www.csustan.edu/sites/default/files/2022-09/academic-year-calendar-2024-25-accessible-version.pdf