SNOWBE ONLINE 11.13
NEW ACCOUNT PROCEDURE

Alex Fhermaye

Policy Name - 1.0

DATE: June 24, 2024

Table of Contents

Purpose

The purpose of the New Account Policy at SnowBe Online is to establish standardized procedures for the creation, management, and deactivation of user accounts. This policy aims to ensure that only authorized individuals have access to SnowBe Online's systems, applications, and data, thereby enhancing the overall security and integrity of the company's digital environment. By implementing these procedures, we seek to protect sensitive customer information, ensure compliance with relevant regulatory requirements, and maintain a high level of operational efficiency. This policy is designed to align with the guidelines of the NIST 800-53 r5 framework and the PCI compliance standards, thereby fostering a secure and well-managed IT infrastructure.

Scope

This policy applies to all employees, contractors, vendors, and any other individuals who are granted access to SnowBe Online's systems, applications, and data. This includes, but is not limited to, all desktop and laptop computers, on-premises and cloud-based servers, network devices, and the company's WordPress shopping cart platform. The policy covers the entire lifecycle of user accounts, from initial creation and access provisioning to periodic review, modification, and eventual deactivation. It encompasses access management for both online and offline environments, including the main office in Los Angeles and all storefronts in the U.S. and Europe. This policy is mandatory for all personnel to ensure the security and integrity of SnowBe Online's operations and customer data.

Definitions

Access Audits:
Regular inspections conducted to ensure user accounts and their access privileges are appropriate and comply with company policies and regulatory requirements.

Access Review and Revalidation:
The periodic reassessment of user access levels to ensure they are appropriate based on the user's current role and responsibilities.

Authorization and Request Process:
The formal procedure for requesting and approving the creation, modification, or deactivation of user accounts.

Compliance with Regulatory Requirements:
Adhering to laws, regulations, and standards relevant to the management of user accounts, such as PCI DSS and NIST 800-53.

Emergency Account Disabling:
The immediate deactivation of a user account in response to a security threat, without prior notice.

Incident Reporting:
The procedure for notifying the IT security team about security incidents involving user accounts.

Inactive Accounts:
User accounts that have not been accessed for a specified period, typically 90 days, and are subject to deactivation if not justified.

Initial Password Setup:
The assignment of a temporary password to a new user account, which must be changed upon the user's first login.

Logging and Monitoring:
The recording and regular review of login attempts to detect and respond to suspicious activity.

Minimum Privilege Principle:
The policy of granting user accounts only the access necessary to perform their job functions, to minimize security risks.

Modifications to Account Privileges:
Changes made to a user's access permissions, which must be requested and approved through a formal process.

Multi-Factor Authentication (MFA):
A security system that requires more than one method of authentication to verify a user's identity for access to sensitive information or critical systems.

Naming Conventions:
The standardized format for creating user account names, typically based on the user's first initial and last name.

Password Management:
Policies and procedures for creating, changing, and maintaining passwords to ensure security and compliance with company standards.

Physical Security:
Measures taken to protect the physical infrastructure housing Active Directory servers, including restricted access and controlled environments.

Secure Access Controls:
Restrictions and monitoring of access to the Active Directory environment to ensure only authorized personnel can make changes.

Unique User Identification:
The requirement that each user account is linked to a specific individual and is not shared among multiple users.

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

Active Directory Policy

1. Account Creation

1.1 **Authorization and Request Process:**
Account creation requests must be submitted through the company's helpdesk ticketing system. The request must include justification for the new account, the required level of access, and approval from the requestor's manager.

1.2 **Unique User Identification:**
Each user account must be uniquely identifiable and linked to a specific individual. Group or shared accounts are strictly prohibited.

1.3 **Minimum Privilege Principle:**
New accounts will be created with the minimum level of access necessary for the user to perform their job functions. Access levels are determined by the user's role and responsibilities.

1.4 **Naming Conventions:**
User accounts must adhere to the company's standard naming convention: [First Initial] [Last Name] (e.g., jdoe for John Doe). Exceptions require approval from the IT Manager.

1.5 **Initial Password Setup:**
Newly created accounts will be assigned a temporary password, which the user must change upon first login. Temporary passwords must meet the complexity requirements specified in the password policy.

2. Account Management

2.1 **Access Review and Revalidation:**
User access levels must be reviewed and revalidated every six months. Managers are responsible for ensuring their team's access is appropriate. Any necessary changes must be submitted through the helpdesk ticketing system.

2.2 **Modifications to Account Privileges:**
Any changes to a user's account privileges must be requested through the helpdesk ticketing system and approved by the user's manager. Changes must be documented, and records retained for audit purposes.

2.3 **Password Management:**
Passwords must comply with the company's password policy, which includes complexity requirements, expiration periods, and restrictions on reuse. Users are required to change their passwords every 90 days.

3. Account Deactivation

3.1 **Termination of Employment:**
When an employee leaves the company, their account must be disabled immediately upon termination. The manager must inform the IT department through the helpdesk ticketing system at least one day in advance.

3.2 **Inactive Accounts:**
User accounts that have not been accessed for 90 days will be flagged as inactive. The IT department will notify the respective manager, and if there is no valid reason to maintain the account, it will be disabled after 30 days of inactivity.

3.3 **Contractor and Vendor Accounts:**
Accounts for contractors and vendors must have predefined expiration dates based on the duration of their contract. The sponsoring manager is responsible for ensuring these accounts are disabled upon contract completion.

3.4 **Emergency Account Disabling:**
In cases where there is an immediate security threat, the IT department has the authority to disable any user account without prior notice. The manager and relevant stakeholders will be informed as soon as possible.

4. Audit and Compliance

4.1 **Logging and Monitoring:**
All login attempts, both successful and unsuccessful, must be logged. Audit logs must be maintained for at least one year and reviewed monthly for suspicious activity.

4.2 **Access Audits:**
Regular audits of user accounts and access privileges must be conducted quarterly. The results of these audits must be documented, and any discrepancies addressed promptly.

4.3 **Compliance with Regulatory Requirements:**
The Active Directory policy must comply with relevant regulatory requirements, including PCI DSS for credit card information, NIST 800-53 for security controls, and any other applicable laws and regulations.

5. Security Controls

5.1 **Multi-Factor Authentication (MFA):**
All user accounts with access to sensitive information or critical systems must use multi-factor authentication to enhance security.

5.2 **Secure Access Controls:**
Access to the Active Directory environment must be restricted to authorized personnel only. Administrative access must be limited and closely monitored.

5.3 **Physical Security:**
Servers housing Active Directory must be in a secured area with controlled access. Only authorized IT personnel should have physical access to these servers.

6. Incident Response

6.1 **Incident Reporting:**
Any security incidents involving user accounts must be reported immediately to the IT security team. The team will investigate the incident and take appropriate action.

6.2 **Account Compromise Protocol:**
In the event of a suspected account compromise, the affected account must be disabled immediately. Affected users must change their passwords, and a full security review of the account activity must be conducted.

7. Training and Awareness

7.1 **User Training:**
All employees must receive training on account management policies and procedures during onboarding and annually thereafter. Training should cover the importance of security, password management, and recognizing phishing attempts.

7.2 **Policy Acknowledgment:**
Employees must acknowledge understanding and acceptance of the Active Directory policy during onboarding and whenever the policy is updated. This acknowledgment must be documented and retained in the employee’s file.

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	Samuel Herrera	Policy created

Citations

User account creation and management. (n.d.-f). https://www.sdstate.edu/sites/default/files/2017-09/user_account_creation_management.pdf

User account management policy - chinle unified school ... (n.d.-g). https://www.chinleusd.k12.az.us/pdf/user-account-managementrevised020110-final-policy1.pdf