SNOWBE ONLINE Policy#

Data Encryption

Your name: Jalif Vazquez Melendez

<TEMPLATE> - Version # 1.0

DATE: 12/02/24

w

Table of Contents

Purpose

This policy outlines the guidelines for utilizing encryption to safeguard SnowBe's confidential information and personally identifiable information (PII), both when stored (at rest) and during transmission (in transit). It aims to ensure compliance with relevant regulations and to protect sensitive data from unauthorized access.

Scope

This policy applies to all SnowBe employees, contractors, and third-party service providers who manage confidential information or PII. It encompasses all devices and systems used for data storage or transmission, including laptops, mobile devices, cloud services, and networks.

Definitions

Data at Rest: Data that is stored on devices or systems.

Data in Transit: Data that is actively transmitted between systems or networks.

Encryption: The process of converting information into a coded format to prevent unauthorized access.

PII: Personally identifiable information, including details such as names, social security numbers, and credit card information.

Roles & Responsibilities

Data Protection Officer (DPO): Oversee the implementation of the encryption policy and ensure compliance with relevant regulations. Provide guidance and support to employees regarding data protection best practices. Monitor encryption technologies and recommend updates or changes as necessary.

IT Security Team: Implement and maintain encryption solutions for data at rest and in transit. Conduct regular audits to assess the effectiveness of encryption measures. Provide training and resources to employees on proper encryption procedures and tools.

Compliance Officer: Ensure that the encryption policy aligns with legal and regulatory requirements. Conduct assessments and audits to ensure ongoing compliance with the policy. Report any violations or incidents related to data protection to management.

Employees and Contractors: Adhere to the encryption policy and follow established protocols for handling confidential information and PII. Participate in training sessions to understand the importance of data encryption and best practices. Report any suspected breaches or vulnerabilities related to data encryption to the IT security team promptly.

Third-Party Service Providers: Comply with the encryption policy when managing or processing SnowBe's confidential information and PII. Provide evidence of encryption practices and security measures used to protect data. Report any security incidents related to data handled on behalf of SnowBe.

Management: Support the establishment and enforcement of the encryption policy.

Policy

Data at Rest: All sensitive data must be encrypted using industry-standard encryption algorithms (e.g., AES-256) and stored on secure devices.

Data in Transit: All data transmitted over networks must be encrypted using secure protocols (e.g., TLS, SSL). Protocol TLS 1.0 is outdated, a higher version is required.

Password Protection: Access to encryption keys and sensitive data must be protected by strong password policies.

Exceptions/Exemptions

- Requests must be formally submitted to the IT Director, specifying the security controls affected.

- Following submission, the request will be reviewed by senior management and the legal team. If approved, the exception will be temporary, lasting up to 45 days.

- During this exception period, the IT team will implement necessary risk mitigation measures and monitor for any escalating risks.

- After 45 days, the exception will either expire, necessitating a return to full compliance, or the request will be reassessed for a potential extension.

- If no extension is granted, the IT team will ensure all temporary adjustments are removed and that the system fully adheres to the original security controls.

Enforcement

Enforcing this security policy is crucial for maintaining the integrity and confidentiality of SnowBe Online's information systems. The System Administrator at SnowBe Online has the authority to restrict or suspend access for individuals who do not comply with the established security policies and procedures.

In situations presenting immediate threats, the IT Director can revoke access rights entirely for any parties involved to safeguard the integrity of SnowBe Online’s systems. Violations of security policies may lead to the suspension or termination of system access. Additionally, when appropriate, civil or criminal penalties may be pursued. Disciplinary actions will be determined based on the severity of the offense and the individual's compliance history.

Policy Enforcement Procedures To uphold the integrity and confidentiality of SnowBe Online's information systems, strict enforcement of security policies is vital.

The following outlines the actions that may be taken in response to policy violations:

1. Verbal Reprimand - For minor, first-time offenses that pose minimal risk or damage, a verbal warning will be issued. This serves as a reminder about the importance of following security protocols.

2. Written Warning/Documentation - A formal written warning will be provided for more serious or repeated offenses. This documentation will specify the nature of the infraction and outline necessary corrective actions. It will be added to the employee's performance record.

3. Mandatory Training - Employees who repeatedly violate security policies or demonstrate a lack of understanding may be required to undergo additional cybersecurity training. Completion of this training will be essential for maintaining system access and employment.

4. Suspension of Access or Employment - In cases of severe infractions or ongoing non-compliance, employees may face a temporary suspension of their system access or employment. The System Administrator or IT Director will make this decision and will remain in effect until a comprehensive review and investigation are completed.

5. Termination of Employment - Serious violations resulting in data breaches, financial loss, or substantial harm to SnowBe Online may lead to employment termination. This process will follow a formal investigation conducted by the security and IT teams.

6. Legal Action - In cases where violations lead to criminal activities or breaches of regulatory compliance, SnowBe Online retains the right to pursue civil or criminal penalties and employment-related consequences.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	12/02/24	Jalif Vazquez		Policy Template Draft
1.1	12/05/24	Jalif Vazquez		SnowBe Policy Draft

Citations

Encryption Policy TEMPLATE

Encryption policy

Encryption Policy