SNOWBE ONLINE Policy 11.4
DATA PRIVACY POLICY

Alex Fhermaye

Data Privacy Policy - 11.4

DATE: June 10, 2024

Data Privacy Policy – V 1.2
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Alex Fhermaye
June 10, 2024

Table of Contents

Purpose

Data privacy laws exist to protect individuals' personal data, both in their private and professional capacities.

SnowBe Online needs to collect and use certain types of personal data about its past, prospective and/or current employees, customers, suppliers, subcontractors, visitors to our sites and websites and other individuals we engage with for a variety of business purposes. The lawful and correct processing of personal data held or used by us as vital to our successful operations, helping to maintain the trust of the people we deal with. Therefore, we must all treat personal data with respect, and always adhere to data privacy laws, and internal guidance. This policy sets out how SnowBe seeks to protect personal data and ensures our company, and our employees are aware of, and understand, the rules governing the use of personal data to which they have access in the course of their work.

Scope

This policy is comprehensive in scope and applies to the entire SnowBe Online community. This includes, but is not limited to, Directors, Department Heads, Team Leads, employees, temporary employees, contractors, volunteers, and guests who have access to any of SnowBe Online's information technology resources. These resources encompass a wide range of assets critical to our operations and security.

Information technology resources include, but are not limited to, all forms of data, images, text, and software. These may be stored on various types of hardware such as servers, workstations, laptops, mobile devices, and other electronic devices. Additionally, this policy covers information stored on non-digital mediums such as paper documents and other physical storage media.

The protection of these assets is paramount to ensuring the confidentiality, integrity, and availability of information, which are the cornerstones of our security posture. This policy sets forth the guidelines and procedures for safeguarding these assets against unauthorized access, disclosure, alteration, and destruction. It is designed to be comprehensive, covering all possible scenarios and providing a clear framework for maintaining and enhancing our information security measures.

Every member of the SnowBe Online community is responsible for understanding and adhering to these guidelines. This responsibility includes recognizing the importance of these resources and the role each individual play in protecting them. By following this policy, we collectively contribute to maintaining the trust of our clients, partners, and stakeholders, and to ensuring the smooth and secure operation of our business processes.

This policy is not static; it is reviewed and updated regularly to adapt to new security challenges and technological advancements. All changes will be communicated promptly to ensure that every member of our community is aware of their responsibilities and the importance of compliance. By adhering to this policy, we uphold SnowBe Online's commitment to excellence in information security.

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

Management and Training

1. Access to non-public personal information shall be limited to authorized users who need to have access to carry out SnowBe's responsibilities as it relates to that information.

2. Each employee and authorized user with access to non-public personal information shall annually sign a copy of SnowBe's Data and Privacy Security Policy and Procedures and agree to abide by its terms.

3. Except as required by law, when SnowBe provides non-public personal information to third parties, it shall first provide a copy of this Data Privacy and Security Policy and require the third party to certify that it has read the policy and agrees to comply with applicable provisions, or that it has a substantially similar data privacy and security policy and that it will comply with the applicable provisions of its policy with respect to the non-public personal information provided.

4. SnowBe Online will perform a background check as further defined in the organization's human resources policies on employees with access to non-public personal information. Any third party with access to non-public personal information must certify that it has performed a background check on its employees who have access to the organization's non-public personal information.

5. SnowBe will have in place a succession plan for key persons in the event of a disruption to normal business processes. As recommended by the Receivership and Insolvency Task Force (11/28/07) 2

6. SnowBe shall ensure to the greatest extent possible based on the size of the organization that there is a clear separation of duties to prevent important management controls from being overlooked. Segregation of duties as defined in the Procedures will preserve the integrity, availability, and confidentiality of information assets by minimizing opportunities for security incidents, outages, and personnel problems.

7. SnowBe shall train employees and other authorized users in the use and maintenance of security procedures.

8. Violations of the data privacy and security policy may result in disciplinary action up to and including termination of employment.

Information Systems

SnowBe shall adopt procedures for protecting and maintaining the security and integrity of its information systems including network infrastructure and software design, information processing, storage, transmission, retrieval, and disposal. These procedures shall address the following matters:

1. Limiting access to those individuals necessary to carry out SnowBe's role with respect to non-public personal information.

2. Limiting access to only those authorized users who shall have signed and agreed to abide by the terms of the Data Privacy and Security Policy or shall have adopted a data privacy and security policy that is substantially similar to SnowBe's policy..

3. Protecting physical and electronic records from unauthorized access, interception, distribution, or destruction.

4. Records back-up and off-site storage procedures to prevent inadvertent loss or destruction of records.

5. Data security procedures to prevent unauthorized access or interception of non-public personal information.

6. Procedures for protecting data when changing, upgrading, or replacing servers, computers, or other storage media.

7. Procedures for properly disposing of unneeded or outdated records.

8. Procedures to monitor, detect, and report upon any improper disclosure or theft of nonpublic personal information.

9. Procedures to periodically test and review the security procedures and maintain a record of the maintenance and review process.

10. Annual audit of procedures for compliance and effectiveness with adjustments as appropriate.

Information Security and Response

SnowBe shall adopt procedures for the prevention, detection, and response to unauthorized access to non-public personal information.

In the event non-public personal information is accessed by someone without proper authorization, SnowBe shall immediately investigate and take appropriate remedial actions to mitigate or prevent loss or damage to affected individuals. Each situation will be evaluated separately, and based upon the potential for loss or damage to affected individuals; the organization will take one or more of the following measures:

- Make such notifications to affected individuals as may be required by law.
- Report the incident to appropriate law enforcement officials.
- Determine the nature and cause of the security breach and implement corrective measures.

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 4, 2024	Alex Fhermaye		Initial Submission for review
1.1	June 10, 2024	Alex Fhermaye		Updated and Corrected submission
1.2	June 10, 2024	Alex Fhermaye		Updated as a Data Privacy Policy

Citations

[organization] data privacy and security policy. (n.d.-d). https://content.naic.org/sites/default/files/inline-files/committees_e_ritf_data_privacy_security_policy.pdf

Global Data Privacy policy. (n.d.-c). https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/investors/debt-securities/global-data-privacy-policy.pdf