SNOWBE ONLINE Policy 11.1
ACCESS CONTROL POLICY

Alex Fhermaye

Access Control Policy – 11.1

DATE: June 10, 2024

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

Table of Contents

PURPOSE 3

SCOPE 3

DEFINITIONS 4

AVAILABILITY: 4
COMPLIANCE: 4
CONFIDENTIALITY: 4
INFORMATION ASSETS: 4
INTEGRITY: 4
IT SECURITY ADVISORY COMMITTEE: 4
IT SECURITY EXCEPTION REQUEST FORM: 4
LEGAL, REGULATORY, AND INDUSTRY STANDARDS: 4
NIST 800-53: 4
PATCH: 4
PCI DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARD): 4
RISK ASSESSMENTS: 4
SECURITY CONTROLS: 5
SECURITY INCIDENTS: 5
SECURITY POSTURE: 5
SECURITY THREATS: 5
TECHNOLOGY INFRASTRUCTURE: 5

ROLES & RESPONSIBILITIES 6

CHIEF INFORMATION OFFICER (CIO) 6
COMPLIANCE OFFICER 6
IT CONSULTANT 6
IT SECURITY MANAGER 6
SALES TEAM 6
SYSTEM ADMINISTRATOR 6
WEB DEVELOPER 6

POLICY 7

SECURITY OF SYSTEMS 7
SECURITY OF NETWORKS AND SERVICES 7
PHYSICAL SECURITY 7

ACCESS REQUESTS 7
ACCESS AUTHORIZATION 7
ACCESS ADMINISTRATION 7
ACCESS REVIEW 8
ACCESS REMOVAL 8
PRIVILEGED ACCESS 8
LOGGING & MONITORING 8

EXCEPTIONS/EXEMPTIONS 9

HOW TO REQUEST AN EXCEPTION/EXEMPTION 9
APPROVAL PROCESS 9
DURATION AND REVIEW 9

ENFORCEMENT 9

VERSION HISTORY TABLE 10

CITATIONS 11

Purpose

The purpose of this Security Policy is to provide an overview of the framework and measures necessary to protect the confidentiality, integrity, and availability of SnowBe's information assets and technology infrastructure. This plan contains the strategies, policies, and procedures required to safeguard against security threats, minimize risks, and ensure compliance with applicable legal, regulatory, and industry standards.

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

Security of Systems

The organization uses several systems to operate effectively, and it's important to maintain the confidentiality, integrity, and availability of these information assets through this access control policy. Threats associated with the information assets have been considered and addressed as far as possible through the risk management process.

Security of Networks and Services

Access to the organization's networks shall be limited to prevent unauthorized and unintended consequences. Devices will not be connected to the network without authorization from the IT Support Company. The WIFI connection details will not be shared without the authorization of the IT Support Company. Guests, visitors and third parties will use ONLY the visitor WIFI network made available.

Physical Security

The physical security of the organization's assets, including buildings and offices, should be always considered. Please ensure the main door is closed and secure, do not leave it ajar. All visitors and third parties must report to reception and sign in. Challenge any strangers on-site who do not appear to be accompanied.

Access Requests

Access requests, including new user accounts, should be submitted to the IT Support Company by email. The job functions as described by the department manager should be reviewed to ensure that the requested access is relevant and acceptable. In the case of IT systems including Active Directory, a profile including privileges may be copied from a colleague with the same job functions.

Access Authorization

The managing director has overall governance of access control within the company and May, for legitimate business reasons, grant or revoke access at their discretion. Department managers are responsible for determining the access levels required by their staff and should, where possible, maintain security groups.

Access Administration

When an access request has been approved by the Gatekeeper, a record of that decision will be maintained to allow an audit trail. The gatekeeper will provide access to the user and inform them via an appropriate method, so as to keep any username separate from a password. Where systems allow, a temporary password will be used and the user will be required to change their password at first log-in.

Access Review

The access to systems will be reviewed on a regular basis to ensure that users are still authorized to access each system and that the privilege level assigned to that user is still acceptable. Gatekeepers will be responsible for reviewing their own systems and may need to refer to department managers for confirmation of user requirements.

Access Removal

In cases of disciplinary or where an employee is within their probation period, access should be removed immediately. Where a notice period has been agreed, or the user is changing job function within the company, access should be removed when it has been confirmed by their line manager.

Privileged Access

All privileged access should be reviewed against the job function before the details or assets (including access cards/fobs) are issued to the user. The use of privileged accounts will be limited, and uniquely identifiable username will be used to enable all activity under an account to the traced back to a single individual.

Logging & Monitoring

User activity is logged and may be monitored for the purposes of error detection and security.

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 template
1.2	June 10, 2024	Alex Fhermaye		Converted to Access Control Policy

Citations

Access control policy. (n.d.-a). https://s3-eu-west-1.amazonaws.com/coachdirect.library/files/policies/Access-Control-Policy.pdf