SNOWBE ONLINE Policy 11.11

Session Termination

Alex Fhermaye

Session Termination - 11.11

Version: 1.1

DATE: June 17, 2024

Table of Contents

Purpose

The purpose of the Session Termination Security Policy at SnowBe is to establish clear guidelines and procedures for the proper termination of user sessions to safeguard sensitive information, maintain system integrity, and prevent unauthorized access. This policy aims to mitigate security risks associated with inactive or improperly closed sessions, ensuring that all employees, contractors, and third-party users adhere to best practices for session management. By implementing these measures, SnowBe seeks to protect its digital assets, uphold data privacy, and comply with relevant regulatory requirements, thereby fostering a secure and resilient organizational environment.

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.

Enhancement:

Refers to an additional feature or improvement that builds upon the base control to provide more specific, stringent, or comprehensive security measures.

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.

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.

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.

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

AC-12 Session Termination

SnowBe is committed to ensuring the security and integrity of its information systems by implementing robust session termination protocols. The following policy outlines the rules, expectations, and overall approach to session termination to prevent unauthorized access and protect sensitive data.

1. **Automatic Session Termination**: All user sessions will be automatically terminated after a predefined period of inactivity. This period will be determined based on the sensitivity of the information being accessed and the specific needs of the system. Users are required to save their work frequently to avoid data loss due to automatic session termination.
2. **Secure Logout Procedures**: Users must manually log out of all systems and applications when they have completed their tasks or will be away from their workstations for an extended period. This practice is essential to prevent unauthorized access to SnowBe’s systems and data.
3. **Session Termination for Remote Access**: All remote access sessions will adhere to the same termination protocols as internal sessions. Users accessing SnowBe systems remotely must ensure they log out of sessions when their work is complete or when they are no longer actively using the system.
4. **Monitoring and Enforcement**: SnowBe will continuously monitor session activity and enforce session termination policies. Any detected deviations or violations will be addressed promptly to maintain the security and integrity of SnowBe's information systems.

This document exists to establish a formal session termination policy at SnowBe, aimed at preventing unauthorized access, protecting sensitive data, enhancing system security, ensuring regulatory compliance, promoting best practices, and mitigating security risks. By defining clear rules and expectations for session management, including automatic termination of inactive sessions, secure logout procedures, and monitoring mechanisms, the policy strengthens SnowBe's security posture, fosters a culture of security awareness, and helps maintain a resilient IT environment.

Enhancement 1 – User-Initiated Logouts

SnowBe requires all users to initiate manual logouts at the end of each session or before leaving their workstation. This practice ensures that sessions are not left open and vulnerable to unauthorized access.

Enhancement 2 – Termination Message

Upon session termination, users will receive a clear and concise termination message. This message will inform the user that their session has ended and provide instructions for logging back in if necessary.

Enhancement 3 – Timeout Warning Message

Prior to automatic session termination, users will receive a timeout warning message. This message will alert users that their session is about to expire due to inactivity, allowing them to save their work and extend the session if needed.

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	Julie Sosa	Initial Submission for review
1.1	June 17, 2024	Alex Fhermaye	Julie Sosa	Template converted to Session Termination policy

Citations

Understanding session termination. ForgeRock. (n.d.). https://backstage.forgerock.com/docs/am/7.1/security-guide/session-state-session-termination.html

Force, J. T. (2020, December 10). *Security and Privacy Controls for Information Systems and organizations*. CSRC. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Network Access and session controls (SS-08-048). Enterprise Policies, Standards, and Guidelines. (n.d.). https://gta-psg.georgia.gov/psg/network-access-and-session-controls-ss-08-048

Session management. Caspio Online Help. (2024, February 1). https://howto.caspio.com/directories/directory-security/session-management/