SNOWBE ONLINE
AC-12 SESSION TERMINATION

Author: Emmanuel Estrella

Version 1.0

DATE: 08 December 2025

AC-12 Session Termination – V 1.0
Status: Working Draft X Approved Adopted
Document owner: Emmanuel Estrella
DATE 08 December 2025

Table of Contents

AC-12 Session Termination – V 1.0
Status: Working Draft X Approved Adopted
Document owner: Emmanuel Estrella
DATE 08 December 2025

Purpose

The purpose of this Session Termination (AC-12) policy is to define and enforce requirements for automatically ending user network sessions after periods of inactivity. This policy is the crucial technical control needed to address the previously neglected security hygiene of SnowBe Online's "laid-back culture" by closing the critical risk of abandoned, authenticated connections. This is mandatory for protecting sensitive systems by automatically terminating idle sessions, such as the VPN connections used by the remote sales team and authenticated sessions on the AWS-hosted website platform, ensuring continuous adherence to NIST 800-53 and maintaining overall system security.

Scope

This Session Termination (AC-12) policy applies to all active user sessions and network connections across the entire SnowBe Online operating environment, covering both internal and external access methods where user authentication is required. The scope specifically includes all authenticated sessions established via VPN by remote sales laptops to access company applications, all authenticated user sessions on the AWS-hosted e-commerce website (including the WordPress shopping cart) and CRM system, and all privileged administrative sessions accessing critical on-premise and AWS servers. This comprehensive coverage ensures that regardless of how a user or administrator connects, the policy successfully closes the security risk posed by idle, authenticated sessions across the network.

Definitions

Authenticated Session
This is when the computer system knows and trusts that a person or program is who they say they are.

AWS Platform
This is the huge online computing infrastructure that runs our website and stores our data.

Cardholder Data Environment (CDE)
This refers to the most secure part of our network where all customer payment information is kept.

Compensating Controls
These are extra security measures put in place when we cannot fully follow a primary security rule.

CRM System
This is the main software we use to track and manage all of our customer relationships and interactions.

E-commerce
This refers to all of our business that is done online, such as sales and transactions on the website.

Firmware
This is the basic, essential software built into the hardware of our network devices that tells the device how to operate.

NIST 800-53
This is a comprehensive rulebook that guides us on how to build a highly secure computer system.

Patching
This means applying small software updates that fix security holes or bugs in our systems.

PCI DSS
These are the mandatory rules we must follow because we handle and store customer credit card information.

Security Hygiene
This refers to the basic, necessary, and routine actions needed to keep our computer systems clean and secure.

Session Termination
This is the process of safely and automatically cutting off a user's network connection when they are finished or have been idle too long.

Virtual Private Network (VPN)
This is a secure, private tunnel that allows our remote laptops to safely connect to the office network.

Roles & Responsibilities

The security and protection of SnowBe's IT resources are a shared responsibility, mandated by the Executive Management Team and enforced throughout the organization.

Executive Management & Owners

- **SnowBe Owners/Management Team:**
  - Holds ultimate accountability for funding the security overhaul required to take the company public.
  - Must formally approve the budget necessary to address all consultant-identified fixes (e.g., software licensing, staff training).
  - Required to officially endorse and enforce new security policies to replace the previously "laid-back culture."
- **Chief Information Officer (CIO):**
  - Serves as the single point of contact responsible for the overall security posture and logical position of SnowBe's core infrastructure.
  - Must be formally notified of any significant security changes made by other entities connected to SnowBe's network (as defined in the Scope).

Technical Operations & Maintenance

- **E-commerce & AWS Team:**
  - Responsible for the security, patching, and hardening of the AWS platform hosting the website and online store.
  - Must immediately update the company's WordPress shopping cart.
  - Holds primary responsibility for the security of the website database where credit card and

customer history is stored, driving immediate PCI compliance efforts.

- **Server & Network Administration:**
  - Responsible for physical security by locking the servers in a secured area of the office.
  - Must immediately update the firmware of all network devices.
  - Responsible for applying patches for all Windows servers.
  - Must correct the broad access issue by implementing granular Access Management controls on all servers (on-premise and AWS).
- **Endpoint & Systems Management Team:**
  - Responsible for applying patches for all PCs and laptops (desktops/laptops in LA office and remote sales laptops).
  - Must update the Anti-Virus and backup software across all endpoints.

Users & Enforcement

- **Technical Consultant:**
  - Provides initial oversight and strategic direction for implementing the NIST 800-53 framework.
  - Responsible for guiding internal teams through the urgent steps needed to achieve system control and PCI compliance.
- **All Employees (Sales, Accounting, Customer Support):**
  - Must adhere to all new security policies, especially those related to restricted Access Management on servers and systems.
  - Must enforce the security of the devices they use for work (e.g., Laptops using the VPN connection).
  - Responsible for immediately reporting any security incidents or suspicious physical activity.

Policy

A-12 SESSION TERMINATION

SnowBe Online shall strictly implement and maintain requirements for session termination across all systems that require user authentication, utilizing automated timeouts and ensuring manual logouts are available.

Automated Session Termination (AC-12)

The following requirements shall govern the termination of active sessions:

- **Inactivity Limit:** All active network and application user sessions shall be automatically terminated after a defined period of inactivity. This timeout period shall be configured to minimize the security risk posed by idle authenticated sessions, particularly the **VPN connections** used by the sales team, while balancing operational needs.
- **Session State:** Termination shall fully remove the session from the system, destroy any temporary authentication tokens, and require the user to re-authenticate to establish a new session.

User-Initiated Logouts (AC-12(1))

SnowBe Online shall ensure users can manually end their authenticated sessions to promptly close network access:

- Functional Logout: A clear and easily accessible user-initiated logout capability must be provided and maintained on all applicable systems, including the CRM and the WordPress shopping cart application on the AWS platform, as a fundamental security measure.
- Mandatory Use: All employees shall be required to manually log out of applications, especially when leaving their workstation unattended or when a device is being physically secured.

Timeout Warning Message (AC-12(3))

To support usability and prevent loss of work, users shall be properly notified before an automated session termination occurs:

- Explicit Warning: A clear and explicit warning message shall be displayed to the user prior to the automated termination of their session due to inactivity.
- Applicability: This is mandatory for all user interfaces where loss of connectivity could disrupt work, particularly for the remote sales team utilizing the VPN to access company applications.

Exceptions/Exemptions

Exceptions or formal exemptions to the requirements defined within this IT Security Plan must be approved through a formal, tiered process reflecting the company's new status as a publicly traded entity requiring strict PCI DSS and NIST 800-53 adherence.

- **Approval Authority:**
  - All minor exceptions must be formally documented and approved by the Chief Information Security Officer (CISO) or the Head of IT who manages the security program.
  - Any exception that significantly increases the risk to the Cardholder Data Environment (CDE) or severely compromises a mandated NIST 800-53 control must also receive final approval from a member of the Executive Management Team (CEO, COO, or CFO).
- **Documentation and Review:**
  - All exceptions will be formally documented, including the business justification, compensating controls (alternative protections) in place, and the duration of the exemption.
  - All plan exceptions will be reviewed on a periodic basis (no less than annually) or whenever the system configuration or underlying business justification changes, to enforce continued appropriateness.

Enforcement

SnowBe Online requires all employees, contractors, vendors, and partners to follow the security policies and procedures outlined in this document. Failure to comply with these requirements may

result in disciplinary action, which can include retraining, loss of access privileges, formal warnings, or termination of employment, depending on the severity of the violation. Individuals who create risks

to company systems, customer data, or operations may face legal consequences if their actions are intentional, expose data, or cause financial damage.

All employees are required to immediately report any suspected policy violations, security incidents, or improper data handling to the appropriate manager or security team. SnowBe reserves the right to monitor system activity and investigate potential breaches of policy at any time. Using SnowBe's systems and resources, all users acknowledge and accept their responsibility to maintain a secure computing environment.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	08 December 2025	Emmanuel Estrella	Management	Added Purpose, scope, definitions, roles and responsibilities, exceptions/exemptions, policy, enforcement, and citations.

Citations

(Used in Policy, Exceptions/Exemptions, Enforcement, Roles & Responsibilities, Definitions, Introduction)
Google. (2025). *Gemini* (Flash 2.5) [Large language model]. Retrieved November 24, 2025, from https://gemini.google.com/

(Used in Policy)
Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controls for Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

(Used in Purpose and Scope)
Guidelines to Writing an Effective Policy Statement. (n.d.). Retrieved December 8, 2025, from https://www.archercenter.org/uploads/3/1/1/3/31139795/policy_statement_outline.pdf