SNOWBE ONLINE
AC-6 LEAST PRIVILEGE

Author: Emmanuel Estrella

Version 1.0

DATE: 08 December 2025

AC-6 Least Privilege – V 1.0
Status: Working Draft X Approved Adopted
Document owner: Emmanuel Estrella
DATE 08 December 2025

Table of Contents

AC-6 Least Privilege – V 1.0
Status: Working Draft X Approved Adopted
Document owner: Emmanuel Estrella
DATE 08 December 2025

Purpose

The primary purpose of this Least Privilege policy is to provide the critical security solution needed to immediately mitigate the high risk of widespread data access identified across SnowBe Online's environment. This policy enforces the principle of minimum necessary access on all systems from the AWS-hosted databases storing credit card and customer purchase history to all on-premise servers and end-user devices. Adoption of this policy is the mandatory first step required to protect customer trust, ensure continuous adherence to PCI DSS and NIST standards, and establish the robust, auditable security posture essential for the company's planned public offering.

Scope

This policy about Least Privilege defines exactly where and to whom the rule of "minimum access" applies, effectively drawing the security boundary around SnowBe Online's entire digital operation to protect our vital data. This rule is required everywhere that handles our information, especially customer details and credit card numbers, meaning it covers all employees and computer programs (like automated processes) and applies to every piece of technology we use, including our online shopping website hosted on the AWS Cloud, all our servers, the desktops and laptops used by the sales and office teams, and the credit card machines in our retail stores. The goal is that no one or no system is allowed to skip this minimum access rule, ensuring we are fully compliant with major security standards like NIST and PCI DSS.

Definitions

Audit Trail
This is like a security journal that records every important action someone takes on a computer.

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.

Least Privilege (Principle of)
We only give people and programs the smallest set of "keys" they need to do their job.

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

Non-Privileged Access
This is your standard, everyday computer access that lets you do your normal tasks but not change the core systems.

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

Privilege Creep
This happens when an employee keeps access they no longer need after changing jobs.

Privileged Accounts
These are special, powerful accounts that can make critical changes to our core network and servers.

Process Privilege
This refers to the limited permissions given to our computer programs so they can run automatically.

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 are 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-6 LEAST PRIVILEGE

SnowBe Online shall strictly implement and maintain the principle of least privilege for all information systems, applications, and processes within the defined scope. The security team shall enforce that all access rights and privilege levels, for both human users and system processes, are the **minimum necessary** to accomplish assigned organizational tasks and business functions.

4.1 Core Least Privilege Mandates (AC-6)

The following requirements shall govern the implementation and enforcement of access controls:

- **Access Restriction:** All access rights, including read, write, modify, and execute permissions, shall be meticulously restricted to the lowest functional level required for a role or process to

  perform its duties.
- **Process Privilege:** System processes, APIs, and automated tasks (including those running on the AWS platform) shall operate at privilege levels no higher than necessary to perform their assigned functions (e.g., separating database connection roles).
- **Role Establishment:** New, specialized user roles, system accounts, and security groups shall be established within the Access Management system to eliminate the practice of granting broad, general access to critical data on servers.

4.2 Non-Privileged and Privileged Access Separation (AC-6(2), AC-6(5))

SnowBe Online shall maintain strict separation between non-privileged and privileged accounts to minimize the risk of privilege escalation.

- **Non-Privileged Access:** Users **must** perform all routine, non-security-related functions (such as web browsing, email, and general office tasks) using a **non-privileged account**. This separation applies specifically to all desktops and laptops connected to the network.
- **Privileged Accounts:** Access to administrative, superuser, or system-level accounts (e.g., those managing the six critical servers) shall be highly restricted and granted only to authorized personnel who require the access to perform system-wide maintenance and configuration changes.

4.3 Technical Execution and Enforcement (AC-6(10))

Technical controls shall be implemented to prevent unauthorized access to sensitive data and functions.

- **Function Prohibition:** Technical security mechanisms **shall** be implemented on all application and server layers to **prohibit non-privileged users from executing privileged functions**. This requirement is mandatory for protecting the integrity of the **website database** where all credit card information is stored.
- **Permission Enforcement:** Application and database controls **must** validate and strictly enforce permissions to enforce that non-privileged users cannot bypass system checks to access or modify sensitive data.

4.4 Auditing and Review (AC-6(7), AC-6(9))

To address the historical lack of control and logging, ongoing auditing and periodic review processes shall be enforced:

- **Review of User Privileges:** User privileges **shall** be formally reviewed at least **quarterly** by the responsible manager to systematically detect and remove any "privilege creep" and enforce that granted access remains consistent with the current job duties of the user.
- **Logging of Privileged Functions:** All uses of privileged functions, system changes, or access attempts to critical servers **shall be logged** to create a detailed, non-repudiable audit trail. These **login audit records must be saved**, and records older than 3 months **must be archived** to a cloud storage facility, ensuring the consultant has the data needed to detect misuse or unauthorized changes.

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 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