SNOWBE ONLINE #0001

Physical Security Policy

Sean Redding

Physical Security Policy –

V 1.0 10/05/2025

Table of Contents

Purpose

This Physical Security Policy describes SnowBe's Online physical security measures and their implementation. This level of security will help to maintain SnowBe's vision and protect day-to-day activities, subsidiaries, employees, and SnowBe's physical assets. This policy provides guidelines for physical security at SnowBe's online headquarters and offices. As well as covering the implementation of various security measures for physical security. This policy defines the following controls and acceptable practices:

- Definition of physical security perimeters and required controls
- Personnel and visitor access controls
- Protection of equipment stored off-site

Scope

This policy applies to all SnowBe Online physical facilities and users of information systems within SnowBe, which typically include employees and contractors, as well as any external parties that have physical access to the company's information systems. This policy must be made readily available to all users.

Definitions

CISO: Chief Information Security Officer

CFO: Chief Financial Officer

EHS: Environment, Health, and Safety

HR: Human Resources

LAN: Local Area Network, the immediate, on-premises network.

NIST: National Institute of Standards and Technology

NIST 800-53: In summary, it is a cybersecurity framework developed by NIST providing a robust catalog of security and privacy controls for protecting the U.S. federal information systems. While it is mandatory for federal agencies, it is more commonly being implemented in civilian companies and organizations to improve security posture and compliance.

Roles & Responsibilities

The **Chief Financial Officer (CFO)** is responsible for proper funding of the Security Program.

The **Chief Information Security Officer (CISO)** is responsible for overseeing, enforcing, and communicating physical and technical security. This policy will be maintained, updated, and reviewed by the CISO.

The **EHS Director** is responsible for overseeing EHS strategies, ensuring regulatory compliance at all levels, managing large-scale programs, and leading the EHS department.

Employees are responsible for adhering to, suggesting improvements, and maintaining compliance with security standards.

HR is responsible for employee lifecycles, onboarding, legal compliance, employee relations and issues, and maintaining company policies, fostering a positive work environment.

The IT/ IT Security Team is responsible for the implementation, maintenance,

The **Security Team** will provide protection for employees and the physical facility.

Policy

General Security:

- All access to SnowBe Online facilities is strictly restricted to employees, third parties, and authorized visitors.

- All personnel are required to be authenticated and authorized for permission to enter SnowBe's physical facilities. This is achieved through key cards, locked gates around the premises, and key fobs required for doors inside parts of the premises (server rooms, management level offices). Visitors must be properly signed in at the front desk and have communication with security before their arrival, due to the property's security gates. Anyone not on the expected visitor list prior will not be let on to the premises.

  - All employees are required to wear their employee badges/ key fobs visibly throughout the premises and will have access assigned based on roles and responsibilities.

- The purpose of this security measure is to keep track of access to the property in the event of any suspicious access to sensitive areas. This is an implementation of NIST 800-53 and is to prevent unauthorized access to sensitive areas.

  - Visitors and vendors must always be escorted by a security team member or an IT security personnel employee while on the premises.

- This security measure is put in place to prevent any potential insider threat, unauthorized access to sensitive areas, and overall to mitigate risk.

  - In the event of any suspicious activities, employees are responsible for reporting the occurrence and identifying the unauthorized visitor/access to the Security/ IT Security Team.

- When maintenance is performed and repairs it must be recorded. This applies to security equipment, including but not limited to surveillance cameras/systems, windows, doors, locks of any kind, etc.

- All records must be retained for a 7-year minimum.

Building security, including fire extinguishers, detectors of any sort, escape routes, exit signs, and EHS responsibilities, will be held and maintained to the local applicable laws and regulations.

- Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
- All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized

attempts to access systems/applications as per the System Access Control Policy.

- All workstations purchased by SnowBe are the property of SnowBe and are distributed to personnel by the company.
- A security perimeter must be defined and established to protect areas containing sensitive data and critical information processing facilities.
- The walls, ceilings, and floor of any secure area must be of the same strength.
- Windows and doors have locks, and all entry points are secured by access control mechanisms and have cameras for additional monitoring as needed.
- Spaces around the perimeter are monitored with CCTV or security patrols.
    - CCTV recordings need to be kept for at least 3 months.
- Alarms are activated outside working hours.
- The most sensitive assets must be stored in the most secure areas. Using the "onion technique", each perimeter "layer" should house progressively more sensitive assets.
- Keys to all secure or public areas housing IT equipment (including wireless access points, gateways, and more) must be protected in a centralized fashion.
- A controlled reception area must establish where:
    - All visitors are required to report first.
    - Security guards challenge unknown persons.
- Off-site backup locations are physically secure for backups, and the security measures are reviewed at least annually.
-
    - The building is unlocked Monday-Friday from 9 am-4 pm
    - After hours, the building is secured and requires an access card for entry
    - The office is secured and requires an access card for entry for after-hours access
    - All server rooms are secured 24/7 and require an access card for entry

Data Center Security:

SnowBe's physical security of data centers is ensured by AWS, the cloud infrastructure service provider.

- Data center employees are responsible for reporting any suspicious activity.

- Servers must be in a locked server room with only authorized personnel having access.

Access and Visitor management:

Physical access is restricted using monitored gates, smart and badge-required locks, and a security team.

- In restricted and sensitive areas, facilities are to remain locked and accessible only to authorized personnel.

- Access and badges are to be revoked upon termination.

- Access and permissions must be re-provisioned upon job promotion/transfer.

- Lost or stolen badges must be reported to the individual's manager, Security Team, or HR.

  Visitors must sign a visitors' log indicating the date and time in/out, organization represented, purpose of visit, and point of contact for the company. A visitor badge will be assigned and must always be visible. Badges must be returned upon leaving the facility.

Exceptions/Exemptions

Requests for an exception, must be submitted in writing to consult with the IT Director or IT Manager.
The request must be detailed with information, including:
· Length of time
· Policy or standard
· Reason
And the Exception Request form must be signed by:
· CIO
· Information Security Officer
· CEO
· Commissioner
Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.
If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.
The CISO, the information security officer representing, and the commissioner must maintain constant communication during the exception. If approved, the CISO's office will send the letter of approval to the requester with details. IN the event of denial, a letter of explanation will be sent to the requester with the reason the CISO denied the request and an explanation.

Enforcement

- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from SnowBe.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
V 1.0	10/05/25	Sean Redding		Physical Security Policy Creation

Citations

https://help.drata.com/en/articles/7763364-physical-security-policy-guidance

https://www.unit.co/docs/onboarding/information-security-policy/

https://online.fullsail.edu/class_sections/272734/modules/907366/activities/5193256

https://online.fullsail.edu/class_sections/272734/modules/907366/activities/5193257