SNOWBE ONLINE
Policy #5.1.1 PHYSICAL SECURITY

Adam Duckworth

VERSION 1.0 June 6, 2023

Table of Contents

Purpose

(Please note that this has been adapted from The UCONN Administrative Policy)

To establish requirements for the management, control, monitoring, and removal of physical access to SnowBe facilities containing Information Technology (IT) Electronic Resources.

Scope

(Please note that this has been adapted from The UCONN Administrative Policy)

This policy applies to all SnowBe employees and other individuals with access to SnowBe restricted/controlled areas containing IT Electronic Resources.

Definitions

(Please note that this has been adapted from The UCONN Administrative Policy)

Restricted/Controlled Area – Any area not open to the public containing IT Electronic Resources

Physical Security - Security measures designed to deny unauthorized access to facilities containing IT Electronic Resources and protect personnel and property from damage or harm.

IT Electronic Resource – Any computing system used for the ongoing operations of institutional activities including workstations, laptops, removable storage, networking equipment and other technologies.

Policy

(Please note that this has been adapted from The UCONN Administrative Policy)

Physical Security

- All facilities containing IT Electronic Resources must be physically protected relative to the importance of the function or purpose of the managed area.
- Access to facilities containing IT Electronic Resources will be granted only to personnel whose job responsibilities require access. Electronic access control systems shall be used to manage access to facilities containing IT Electronic Resources, where available and appropriate.
- Access rights to facilities containing IT Electronic Resources shall be based on the individual's role or function in the organization.
- Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft or unauthorized physical access to confidential data.

Facility Access Key Cards

- Access cards and/or keys for access to restricted/controlled areas containing IT Electronic Resources must not be shared or loaned to others.
- Lost or stolen access cards and/or keys must be reported immediately to management.

Facility Access

- A log of access to restricted/controlled areas containing IT Electronic Resources must be maintained, by the responsible unit/department, to provide a physical audit trail of access to facilities, computer rooms and data centers where sensitive information is stored or transmitted.
    - For individuals without electronic badges, a paper log will be used and shall document the individual's name, the organization represented, and the SnowBe representative authorizing physical access, where applicable.
- Any individual accessing restricted/controlled areas containing IT Electronic Resources shall wear a SnowBe badge or other identification. Non-workforce members will be issued a temporary badge that expires and that visibly distinguishes the individual from SnowBe employees. Badges must be visible at all times while in restricted/controlled areas containing IT Electronic Resources.
    - All electronic badges must be worn so that both the picture and information on the badge are clearly visible.
- Non-workforce members without a badge compatible with an electronic badge reader must be escorted at all times within restricted/controlled areas where IT Electronic Resources are located.

Procedures

(Please note that this has been adapted from The UCONN Administrative Policy)

An annual review of physical access rights to restricted/controlled areas containing IT Electronic Resources shall be performed to determine the appropriateness of facility access and controlled zones.

Management is responsible for adding approved access to all Identification Badges. Facilities Development and Operations is responsible for issuing keys.

Requests for access shall come from the applicable manager in the area where the data/system/ equipment resides.

Revocation of all facility access shall occur immediately upon termination including the collection of keys, access cards, and/or any other asset used to enter restricted areas.

Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration.

Exceptions/Exemptions

(Please note: this has been adapted from The University of Tennessee System)

Requests for exceptions from SnowBe security controls, standards, or practices must be submitted in writing to the IT Department. At a minimum, each request shall have the following information completed by the requestor, or the request will not proceed:

- Contact information on the requestor and authorized signer
- The standard, practice, or controls from which an exception is desired
- Request type (i.e. Exception, Exemption)
- Explanation of the Request
- Business Justification/Reason

The IT Department conducts a risk assessment on the request.

- If needed, the IT Department will conduct a review of the assessment.

The IT Department documents the results of the risk assessment and will then accept or reject the request.

All requests that are granted must be reviewed and/or renewed annually.

Enforcement

(Please note: this has been adapted from the SANS Acceptable Use Policy)
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Version History Table

Version #	Change/ Implementation date	Document Owner	Approved By	Description
1.0	June 6, 2023	SnowBe Online	Adam Duckworth	Initial Draft

Citations

2021-01 it physical security policy - uconn health. (n.d.-a). https://health.uconn.edu/policies/wp-content/uploads/sites/28/2021/03/2021-01-IT-Physical-Security-Policy.pdf

Acceptable use policy - assets.contentstack.io. (n.d.). https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt207beda4b7c14d22/636f1a30e3836b0c88e8f0a8/Acceptable_Use_Policy.pdf

GP-001.02 – security exceptions and exemptions to its standards practices & controls. UT System Policies. (2022, June 23). https://policy.tennessee.edu/procedure/gp-001-02-security-exceptions-and-exemptions-to-its-standards-practices-controls/