SNOWBE ONLINE Policy#AP-2 Access Control Policy and Procedures

**Michael Kohronas:**

**<Access Control Policy and Procedures>**

**Version #3**

**DATE: 06/2024**

Table of Contents

[Policy 2](#_Toc170594761)

[Scope 2](#_Toc170594762)

[Definitions 2](#_Toc170594763)

[Roles & Responsibilities 2](#_Toc170594764)

[Policy 3](#_Toc170594765)

[Exceptions/Exemptions 5](#_Toc170594766)

[Enforcement 5](#_Toc170594767)

[Version History Table 5](#_Toc170594768)

[Citations 6](#_Toc170594769)

Policy

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the requirements set forth by the State to implement the family of Access Control security controls at the organization, process and/or system level for all information assets / State data.

Scope

The scope of these regulations and procedures are applicable to all information resources owned or operated by SnowBe Online. All users are responsible for adhering to these regulations and procedures. Information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

Definitions

**Access control –** The process of granting or denying specific requests to:

* obtain and use information and related information processing services;
* enter specific physical facilities (for example, employee only locations in store locations)

**Authorized User –** An individual who has approved access to an information asset to perform job responsibilities.

**Demilitarized zone –** A host or network segment inserted as a “neutral zone” between an organization’s private network and the Internet.

Roles & Responsibilities

**All Employees, contractors, or interns –** Follow PCI compliance when handling cardholder information and ensure there are no unknown third-party devices on card readers that can hinder security.

**CISO –** Oversee the development, implementation, and maintenance of the PCI Compliance Policy.

**IT Security team –** Ensure that all cardholder data is being collected and stored properly and reporting and resolving any data or devices that aren’t meeting PCI compliance.

# Policy

The following procedures serve as the base requirements for SnowBe Onlines information assets. They represent the security controls established to provide an acceptable level of protection from unauthorized system access.

1. **CREATE USER ACCESS**
2. Define the process for requesting and approving new User Access. Items to be included:
   * How access is requested
   * Level of accesses available
   * Business justification needed for access and access level
   * Approvals and/or authentications needed
   * How user and/or requester is notified of approval or denial of access
   * If notifications about decisions are given to others, and to whom
   * who grants access, when & how
3. **CHANGE USER ACCESS**
4. Define the process for requesting and approving existing User Access Changes. Items to be included:
   * How changes are requested
   * Business justification for changes
   * Approvals and/or authentications needed
   * How user and/or requester is notified of approval or denial of changes to users access
   * If notifications about decisions are given to others, and to whom
   * Who grants access, when & how
5. **SUSPENSION OR TERMINATION OF USER ACCESS**
6. Define the process of suspending or terminating User Access when access is no longer required or authorized. Items to be included:
   * When termination will be used and when suspension will be used with the business reasons
   * How the System Owner is notified of the need that a user’s access be suspended or terminated including controls used to ensure timely notification of terminations and transfers
   * Who is authorized to provide such notification
   * Justification necessary
   * Approvals needed
   * How user and/or requester is notified of suspension or termination
   * If notifications about decisions are given to others, and to whom
   * Who grants access, when & how
7. **REVIEW OF USER ACCESSES**
8. Define the process of reviewing user accesses. Items to be included:
   * A review of user accesses for inactivity
9. For the review of existing accesses, the documentation should include:
   * Frequency and timing of the reviews (intervals should be relative to risk)
   * Method of review
   * The criteria used for continued necessity
   * The criteria used for appropriateness of level of access
   * Who reviews users’ access for continued necessity
   * Who reviews for appropriateness of level of access
   * Approvals and/or authentications needed
   * How user and/or requester are notified of results
   * If notifications about decisions are given to others, and to whom
   * What results may include in terms of access changes and who executes them
10. Criteria used must include confirmation of:
    * Continuing employment
    * Current roles and responsibilities and/or any changes
    * Current access levels and/or any needed changes
    * Record of acceptable use of user’s access
11. For the review of inactivity of accounts the documentation should include:
    * Frequency and timing of the reviews (intervals should be relative to risk)
    * Method of review
    * The specified period of inactivity used for the review
    * Any methods used to validate continued necessity for inactive accounts (who, what & how)
    * The consequences of various levels of inactivity (suspension or termination)
    * Approvals needed
    * How user and/or supervisor is notified of access suspension or termination
    * If notifications about decisions are given to others, and to whom
    * How and when suspension or termination occurs
12. Monitoring, Logging and Investigation of Unusual Activity should:
    * Define the monitoring and logging of access to application and related database files
    * Who is responsible for the monitoring and logging of access
    * Describe the procedures for what is logged
    * Define the process to monitor what is logged
    * How and when the System Owner is notified when unusual activity occurs
    * Describe how to investigate unusual activity
    * Describe the reporting of unauthorized access

Exceptions/Exemptions

Exceptions to this Policy will be considered on a case-by-case basis and do not guarantee approval. To request an exception, please submit a written request to the IT Director outlining the following:

How to Request Exceptions/Exemptions?

To request an Exception or Exemption from a Policy that is in place please message ITDirector@SnowBe.com with the following format:

What Exception/Exemption are you requesting?

Why are you requesting this Exception?

How long are you requesting this Exception/Exemption for?

The IT Director, in consultation with relevant stakeholders, will review the request and determine if an exception can be granted. The decision will be based on the potential impact on security, the justification provided, and the availability of alternative secure solutions. Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

Enforcement

The failure to comply with policies, Policys, or Policys will result in a warning or disciplinary action depending on the severity of the infraction.

Version History Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version #** | **Implementation Date** | **Document Owner** | **Approved By** | **Description** |
| v1 | 06/06/2024 | Michael Kohronas |  | Added the exception and exemption and enforcement as a group |
| V2 | 06/07/2024 | Michael Kohronas |  | Fixed issues with text size and font, added name and date to header, |
| V3 | 06/24/2024 | Michael Kohronas |  | Created the Access Control Policy & Procedures |

Citations

<https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment>

<https://www.tarleton.edu/technology/wp-content/uploads/sites/170/2022/07/ac-1-access-control-policy-and-procedures.pdf>

<https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/docs/VITA-AGENCY-TEMPLATE-Logical-Access-Controls-Policy.docx>