a

SNOWBE ONLINE #018

Account Management SOP(s)

Sean Redding

Account Management SOPs -

Version # 1.0

10-18-25

Table of Contents

Purpose

This procedure provides guidance and direction regarding the granting, maintenance, and removal of access to the information technology assets of SnowBe Online. IT Assets must be protected by controls to ensure that only those persons with a legitimate need to access IT Assets have access, and that the level of access is appropriate to each person's job duties.

Scope

This procedure applies to all employees of SnowBe Online, all vendors, and third parties doing business with SnowBe Online.

Definitions

Account - A means for accessing IT Assets that generally consists of an account name (or user ID) and associated authentication method.

Account Administrator - A designated employee trained in the use of SnowBe Online's software systems for the purpose of performing domain account creation, deletion, and deactivation.

Asset Owner – IT team employee or member of the IT Information Security team to whom the IT Director has delegated the authority to grant access to an IT Asset.

Authorized User - A person who has been granted access to an account and whose access has not been rescinded or terminated.

IT Asset(s) - Digital information and technology assets, which include:
•Software (applications, database management, operating systems, licenses, etc.);
• End User Devices (portable storage devices, computers, laptops, tablets, smart phones, displays, net stations, etc.);
• Digital Information;
• Cloud-based or on-premises Servers (multi-user physical or logical computers, etc.);
• Networks (cables, circuits, switches, routers, firewalls, etc.);
• Digital Storage Devices and Systems (cloud-based, removable, or fixed devices that retain Digital Information, etc.) owned by, under the custody of, or commercially made available to SnowBe Online.

Standard Operating Procedure (SOP) - A standard operating procedure addresses process-related information that is below the level of policies and procedures. Their content often informs the Policy Framework. A SOP is highly detailed, regularly revised, and is deemed internal to SnowBe Online, although a SOP may be shared on a need-to-know basis.

Roles & Responsibilities

Authorized User Responsibilities

- Authorized Users are responsible for all actions made with their User ID.
- Authorized Users must not disclose credentials to any other entity at any time.
- Access to the University's IT Assets must be governed by the 'Acceptable Use of Information Technology (IT) Assets Procedure'. Unauthorized access is prohibited and will be subject to disciplinary action up to and including termination.

IT Director:
Is responsible for the annual review and updating of this policy.

IT Team:
Are responsible for the enforcement of the following procedures.

Policy

Creation of Accounts

- All Accounts must be managed by an Account Administrator.
- All requests to create an Account must be made via a New Employee/Position Change Request Form owned by Human Resources (HR) and approved by the applicable Asset Owner(s).
- Accounts for IT Assets for which no Asset Owner is assigned must be approved by the intended Account holder's Dean or Director using the New Employee/Position Change Request Form.
- All account creation will be subject to Standard Operating Procedures.

Access Requests for third parties

- Accounts may be provided to a third party who is associated with SnowBe Online.
- The requests for Accounts process is the same as above.
- Before submission, requests must be approved by the Applicable Asset Owner and CISO, and include a start date, end date, and reason for access.
- These Access Requests must be received at the IT Service Desk 10 days before the required access date.
- These accounts will be disabled on the end date specified on the New Employee/Position Change Request Form.

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

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 IT Director and the Commissioner must maintain constant communication during the exception. If approved, the Commissioner'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 IT Director denied the request and an explanation.

Exemptions:

Access Control – Access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies, are not to be paused or discontinued.

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
1.0	10-18-25	IT Director	IT Director	Initial draft of SOPs.

Citations

https://www.athabascau.ca/university-secretariat/_documents/procedures/account-mgmt-procedure.pdf

https://www.sdstate.edu/sites/default/files/2017-09/user_account_creation_management.pdf