SNOWBE ONLINE Policy#AC-2 Account Management

**Michael Kohronas:**

**<Account Management>**

**Version #3**

**DATE: 06/2024**

Table of Contents

[Policy 2](#_Toc170588310)

[Scope 2](#_Toc170588311)

[Definitions 2](#_Toc170588312)

[Roles & Responsibilities 3](#_Toc170588313)

[Policy 3](#_Toc170588314)

[Exceptions/Exemptions 4](#_Toc170588315)

[Enforcement 5](#_Toc170588316)

[Version History Table 5](#_Toc170588317)

[Citations 6](#_Toc170588318)

Policy

The purpose of this standard is to establish the rules and processes for creating, maintaining, and controlling the access of a digital identity to SnowBe Online Information Technology (IT) resources and assets to protect SnowBe Online data and information.

Scope

This policy applies to all SnowBe Online any account that has access to SnowBes information. These accounts can be owned by staff, contractors, vendors, and third parties. This applies to human accounts, programmatic accounts, service accounts, and privileged accounts.

Definitions

**Administrative Accounts**: Accounts that allow users to modify system settings or other accounts. These accounts must have appropriate security levels, not indicate the user's privilege level in the username, follow a standardized naming convention, and be revoked according to organizational requirements.

**Default Non-Privileged Accounts**: Accounts for users without individual accounts, such as guest or anonymous users. These accounts must be disabled until needed, have limited permissions, only be allowed after a risk assessment, include restricted network access, have passwords changed monthly by an administrator, not be assigned for delegation, and maintain a log of users given the password.

**Default Privileged Accounts**: Accounts like root or Administrator that come with a system and cannot be removed without affecting functionality. These accounts must be disabled if not in use or renamed if possible, only used for initial installation or as a service account, not use the default password, and have passwords known by at least two individuals if the password is known by anyone.

**Emergency Accounts**: Short-term accounts used in crisis situations requiring rapid activation. These accounts bypass normal authorization processes and must be automatically disabled after 24 hours.

**Individual Accounts**: Unique accounts issued to single users for authentication and authorization based on assigned permissions.

**Privileged Accounts**: Accounts providing increased access and requiring additional authorization, used by personnel like network or system administrators. These accounts must comply with the principle of least privilege, granting only necessary access.

**Service Accounts**: Accounts used for processes, not intended for individual users. These accounts must have an assigned owner, be restricted to specific devices and hours, not be used interactively except for initial installation or necessary troubleshooting, follow a naming convention, not have scheduled password resets unless an employee with password knowledge leaves, and have passwords known by at least two individuals if known by anyone.

**Shared Accounts**: Accounts where multiple users know the password or use the same authentication token. Use of these accounts is allowed only when individual accounts are not feasible, and must be documented and reviewed. Shared accounts must have tokens reset when users no longer need access, be restricted to specific devices and hours, have users log in with individual accounts and switch to the shared account if possible, and have limited permissions.

**Temporary Accounts**: Short-term accounts for specific needs, like vendors or manufacturers, with restrictions on creation, usage times, and must have start and stop dates. These accounts should have limited permissions and access only to required systems.

Roles & Responsibilities

**Account Manager –** Account managers maintain accounts. They are the delegated custodians of protected data. Account managers:

* Maintain appropriate levels of communication with the information owners to determine the level or degree of access granted to an individual.
* Determine the technical specifications needed to set access privileges.
* Delegate account management functions to account administrators.
* Create and maintain procedures used in managing accounts.
* Perform all account administrator duties as required.

**Account Administrators –** Account administrators are an optional subset of the account manager role. They do not determine procedures. System rights and/or responsibilities are assigned to them by the account manager. All account administrator responsibilities are contained within the role of account manager should an account administrator not exist. A subset of account administrator duties may be assigned as appropriate. For example, a role for password reset only may exist for service desk employees. Additionally, some of these responsibilities may remain with the account manager should that manager determine it is necessary. For account management, the administrator may:

* Maintain any necessary information supporting account administration activities, including account management requests and approvals.
* Enroll new users.
* Enable/disable user accounts.
* Create and maintain user roles and groups.
* Assign rights and privileges to a user or group.
* Collect data to periodically review user accounts and their associated rights.
* Assign new authentication tokens (e.g. passwords resets).

**Entitlement Administrator –** Entitlement administrators are an optional subset of the account manager role. Rights and/or responsibilities are assigned to them by the information owner and generally include:

* Assign rights and privileges to a user or group.
* Collect data to periodically review user accounts and their associated rights.
* Maintain any necessary information supporting account administration activities including account management requests and approvals.

**Information Owner –** Information owners are people at the managerial level within an entity who:

* Delegate account managers to ensure the appropriate level of information access is provided. Delegation can be to individual users, groups and/or third parties (e.g., another entity).
* Define roles and groups, as well as the corresponding level of access to resources for that role or group.
* Determining who should have access.
* Determine the identity assurance level for the application and/or data.
* Review that accounts and access controls are commensurate with overall business function and that the associated rights have been properly assigned, at a minimum, annually.
* Require business units with access to protected resources to notify account managers when accounts are no longer required, such as when users are terminated or transferred and when individual access requirements change.

# Policy

Account management and access control includes the process of: requesting, creating, issuing, modifying, and disabling user accounts; enabling and disabling access to IT resources; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions.

**Account Management and Access Control Functions**

Automated mechanisms must be employed to monitor the use and management of accounts. These mechanisms must allow for usage monitoring and notification of atypical account usage. Thresholds for alerting should be set based on the criticality of the system or assurance level of the account.

Staff in the appropriate account management/access control role(s) must be notified when account management activities occur, such as, accounts are no longer required, users are terminated or transferred, or system usage or need-to-know changes. This should be automated where technically possible.

Automated access control policies that enforce approved authorizations for information and system resources must be in place within systems. These access control polices could be identity, role or attribute based.

By default, no one has access unless authorized.

The Identity Assurance Level (IAL) of a system determines the degree of certainty required when proofing the identity of a user. The following table describes the level of confidence associated with each IAL.

|  |  |
| --- | --- |
| *Identity Assurance Level* | *Description* |
| 1 | Low or no confidence in the asserted identity’s validity |
| 2 | Confidence in the asserted identity’s validity |
| 3 | High confidence in the asserted identity’s validity |
|  |  |

Table 1 reflects the standards for account management at each assurance level.

**Table 1 – Account Management Standards per Identity Assurance Level**

|  | Identity Assurance Levels | | |
| --- | --- | --- | --- |
| Category | 1 | 2. | 2 |
| Account disabled automatically after *x* days of inactivity | 1096 | 90 | 90 |
| Send notification *x* days before account disabled | 30 | 30 | 14 |
| Account locked after *x* number of consecutive failed login attempts | 10 | 5 | 3 |
| Account creation requires an authoritative attribute that ties the user to their account. For example, this could be an employee ID, driver’s license ID, tax ID, or unique individual email address. | No | Yes | Yes |
| Email notification will be sent to the user for the following events:   * Token change (password, pre-registered knowledge token, out of band (OOB) token information) * Account disabled due to invalid attempts * Forgotten User Identification (UID) issued * Account attribute change (e.g., name change) * Account re-activation | If known | Yes | Yes |
| Self-service functionality allowed | Yes | Yes | No |

For all Assurance Levels, the following must be adhered to.

* 1. **Creating New Accounts:** To create an account, there must be a valid access authorization based on an approved business justification and a request must be made to create the account.
  2. **Modifying Account Attributes (i.e., changing users’ names, demographics, etc.):** Modifications must only be made by the authenticated user or an authorized account manager.
  3. **Enabling Access:** Access is granted, based on the principle of least privilege, with a valid access authorization.
  4. **Modifying Access:** Access modifications must include a valid authorization. When there is a position change (not including separation), access is immediately reviewed and removed when no longer needed.
  5. **Disabling Accounts/Removing Access:**

1. **Event/Risk Based (Administrative Disable):** When an account poses or has the potential to pose a significant risk, either the account is disabled and/or access attributes are removed upon discovery of the risk. Close coordination between the information owners, account managers/administrators, legal, incident response stakeholders and human resource managers is essential in order for timely execution of removing or restricting user access. Significant risk may include a disgruntled employee, or one who has been identified by as a potential risk. Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations. An account identifier is required to identify these accounts and prevent inappropriate re-enabling of the account/access. Re-enabling the account requires explicit approval of the entity, Self-service mechanisms may not be used to re-enable the account.
2. **De-provisioning Upon Separation**: All user accounts (including privileged) must be disabled immediately upon separation. In addition, credentials must be revoked in accordance with organizational requirements, and access attributes must be removed. Self-service mechanisms may not be used to re-enable the account.
3. **Inactivity Disable:** When an account is disabled due to inactivity, access attributes may remain unchanged if deemed appropriate by the information owner.
   1. **Reviewing Accounts and Access:**
4. Information owners must review all accounts on an annual basis (minimally) to determine if they are still needed.
5. Access to privileged accounts must be reviewed every six months (minimally) to determine whether or not they are still needed.
6. Information owners must review account authorizations and/or user access assignments on an annual basis (minimally) to determine if all access is still needed.
7. Accounts or records of the account must be archived after 5 years of inactivity or after specific audit purposes are met.
   1. **Unlocking User Accounts:** In order for an administrator or user support agent to unlock an account for a user, the user must be vetted through pre-registered knowledge tokens as per the Authentication Tokens Standard.
   2. **Secure Log on Procedures:** Where technically feasible, access must be controlled by secure log-on procedures as follows:
8. Must not display tokens (e.g., password, PIN) being entered.
9. Must display the following information on completion of a successful log-on:
10. Date and time of the previous successful log-on; and
11. Details of any unsuccessful log-on attempts since the last successful log-on.
    1. **Session Inactivity Lock:** Sessions must be locked after a maximum inactivity period of 15 minutes. Session inactivity locks are temporary actions taken when users stop work and move away from their immediate vicinity but do not want to log out because of the temporary nature of their absences. Users must re-authenticate to unlock the session.
    2. **Connection Time-out:** Sessions must be automatically terminated after 18 hours or after “pre-defined” conditions such as targeted responses to certain types of incidents.
    3. **Logging/Auditing/Monitoring:** All account activity must be logged and audited in accordance with the Security Logging Standard. The ability to modify or delete audit records must be limited to a subset of privileged accounts. Any modification to access attributes must be recorded and traceable to a single individual.

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 |

Citations

<https://www.massey.ac.nz/documents/1709/Mobile_Device_Management_Policy.pdf>

<https://www.cisecurity.org/wp-content/uploads/2020/06/Account-Management-Access-Control-Standard.docx>