SNOWBE ONLINE

Policy# AC-02

Account Management

Daphnie Bruno

Policy #AC-02 - Version # 1.2

November 09, 2024

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 2

POLICY 3

EXCEPTIONS/EXEMPTIONS 3

ENFORCEMENT 10

VERSION HISTORY TABLE 11

CITATIONS 12

Purpose

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to SnowBe Online information resources. An account, at minimum, consists of a user ID and a password. Supplying account information will usually grant access to some set of services and resources. This policy establishes guidelines for issuing and managing accounts.

Scope

This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices; information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally by the Information Technology Division.

Definitions

Anomalous accounts

Accounts that exhibit unusual or unexpected behavior, such as irregular access patterns or unexpected changes, which may indicate potential security risks.

Attribute-based access control

An access control method that grants or denies access to resources based on user attributes (e.g., role, location, or department) rather than solely on the identity of the user.

Atypical usage

Unusual or out-of-the-ordinary behavior in system account usage, such as logging in at odd hours or from unusual locations, which may suggest security concerns or unauthorized access.

Automated mechanisms

Tools or systems that perform tasks automatically, often without direct human intervention, to streamline processes such as account creation, modification, and deletion.

Confidentiality Agreement

A formal agreement in which a party agrees to protect and not disclose sensitive or private information. Often used to maintain the privacy and security of organizational data.

Entity validation

The process of confirming the identity or legitimacy of an individual, device, or organization, typically before granting access to resources.

Provisioning/Deprovisioning

The processes of creating (provisioning) and removing (deprovisioning) user accounts, resources, or services, especially as individuals join or leave an organization.

Revocation of privileges

The act of removing a user's access rights or permissions, usually due to a change in their role or as a response to a security issue.

Runtime access control

A method of managing access to resources dynamically, based on real-time conditions or attributes, allowing permissions to be adjusted instantly without needing to restart sessions.

Trust relationships

Connections or partnerships between entities (e.g., systems, organizations, or individuals) that are built on a basis of mutual reliability, typically to facilitate secure information sharing or system access.

User ID

Is a unique identifier assigned to an individual user within a system, application, website, or platform. It is used to differentiate one user from another, allowing the system to track user-specific information, preferences, and activities.

Roles & Responsibilities

Audit Team:

- Conduct independent reviews of account management practices
- Verify compliance with internal policies and external regulations

Compliance Officer:

- Ensure account management practices comply with relevant laws and regulations
- Review and approve account management policies

Contractors/Vendors:

- Follow account management policies and procedures set by SnowBe Online
- Use assigned accounts only for authorized purposes
- Report any suspicious activities or potential security breaches
- Adhere to password policies and multi-factor authentication requirements
- Return or surrender access credentials upon completion of contract

Employees:

- Create and manage user accounts as per their job responsibilities
- Follow account creation, modification, and termination procedures
- Use assigned accounts responsibly and maintain password security
- Report any unauthorized access or suspicious activities
- Participate in regular security awareness training

Human Resources:

- Initiate account creation/termination processes for new hires and departing employees
- Communicate role changes that affect access privileges
- Assist in maintaining accurate user account information

Information Security Department:

- Develop and maintain account management policies and procedures
- Conduct regular audits of user accounts and access privileges
- Monitor account activities for potential security threats
- Implement and manage access control systems
- Provide guidance on account management best practices
- Investigate and respond to account-related security incidents

IT Manager:

- Oversee the implementation of account management policies
- Ensure proper account provisioning and deprovisioning processes
- Coordinate with HR for employee onboarding and offboarding
- Manage technical aspects of access control systems
- Review and approve access requests for sensitive systems
- Ensure compliance with relevant standards (e.g., PCI DSS)

System Owners:

- Define access requirements for their systems or data
- Regularly review and validate user access rights

Policy

Server Owners and Application Administrators are responsible for ensuring that all accounts at the OS level or within a particular application are created according to the following procedures:

AC-02.1 Account Provisioning and Access Control Standards

Accounts that access electronic computing and information resources require prudent oversight. The following security precautions should be part of account management:

- All accounts must have a password that adheres to the practices outlined in the Password Management Policy document.
- Any account that is not used for interactive login or authentication must be "locked" or "disabled" according to the definition of those terms for the particular OS in question.
- Prior to creating a user account, that user's affiliation with the SnowBe Online must be verified by the sponsoring unit or division (i.e., Human Resources, Registrar).
- Users must attend all appropriate application or data handling training courses prior to their account being activated.
- Accounts for individuals not affiliated with the SnowBe Online must have prior approval from IT.
- There may be only one user associated with an account. Users may NOT share an account.
- Accounts should not be granted any more privileges than those that are necessary for the functions the user will be performing. When establishing accounts, standard security principles of "least required access" to perform a function must always be used, where administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will suffice.
- Directory and file permissions should be set correctly to prevent users from listing directory contents or reading, modifying, or deleting files that they are not authorized to access.
- Account setup and modification shall require the signature of the account requestor, the requestor's immediate supervisor, the data owner and the Office of Information Technology.
- The organization responsible for a resource shall issue a unique account to each individual authorized to access that networked computing and information resource. It is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/ revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

- The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access (e.g., user accounts used for email do not require an identity validation process as thorough as for those user accounts that can be used to post information to public web pages or modify department budgets).
- Passwords for new accounts should NOT be emailed to remote users unless the email is encrypted.
- The date when the account was issued, and its expected expiration date (if applicable) should be recorded in an audit log.
- All managers of accounts with privileged access to SnowBe Online data must sign a Confidentiality Agreement that is kept in the department file under the care of a Human Resources representative or liaison.

AC-02.2 Managing Accounts

- All accounts shall be reviewed at least annually by the data owner to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. IT Security may also conduct periodic reviews for any system connected to the SnowBe Online network.
- All guest accounts (for those who are not official members of the Snow Be Online community) with access to computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.
- For access to sensitive information managed by a department, account management should comply with the standards outlined above. In addition, naming conventions must not cause contention with centrally managed SnowBe Online NetIDs. Should the potential for contention arise, the account will not be created until a mutually satisfactory arrangement is reached.
- The identity of users must be authenticated before providing them with ID and password details. In addition, it is required that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.
- Account management should allow for lockouts after a set number of failed attempts (ten is the recommended number). Access should then be locked in a minimum of one hour unless a local system administrator intercedes. Lock-outs should be logged unless the log information includes password information.

Control Enhancements

(01) AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Support the management of systems accounts.
Discussion: Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account I created, enabled, modified, disabled, or removed, or when users are terminated or transferred monitor system account usage; and report atypical system account usage.
Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.
Related Controls: None.

(02) AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

Automatically [Selection: remove; disable] temporary and emergency accounts.
Discussion: Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.
Related Controls: None.

(03) DISABLE ACCOUNTS

Disable accounts when the accounts:

(a) Have expired;
(b) Are no longer associated with a user or individual;
(c) Are in violation of organizational policy; or
(d) Have been inactive for more than 7 days without prior approval.

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.
Related Controls: None.

(04) AUTOMATED AUDIT ACTIONS

Automatically audit account creation, modification, enabling, disabling, and removal actions.
Discussion: Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.
Related Controls: AU-2, AU-6.

(05) INACTIVITY LOGOUT

Require that users log out.
Discussion: Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period.
Automatic enforcement of inactivity logout is addressed by AC-11.
Related Controls: AC-11.

(06) DYNAMIC PRIVILEGE MANAGEMENT

Discussion: In contrast to access control approaches that employ static accounts and predefined user privileges, dynamic access control approaches rely on runtime access control decisions facilitated by dynamic privilege management, such as attribute-based access control. While user identities remain relatively constant over time, user privileges typically change more frequently based on ongoing mission or business requirements and the operational needs of organizations. An example of dynamic privilege management is the immediate revocation of privileges from users as opposed to requiring that users terminate and restart their sessions to reflect changes in privileges. Dynamic privilege management can also include mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, if their job function or assignment changes, or if systems are under duress or in emergency situations. Dynamic privilege management includes the effects of privilege changes, for example, when there are changes to encryption keys used for communications.
Related Controls: AC-16.

(07) PRIVILEGED USER ACCOUNTS

(a) Establish and administer privileged user accounts;
(b) Monitor privileged role or attribute assignments;
(c) Monitor changes to roles or attributes; and
(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

Discussion: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.
Related Controls: None.

(08) DYNAMIC ACCOUNT MANAGEMENT

Create, activate, manage, and deactivate dynamically.
Discussion: Approaches for dynamically creating, activating, managing, and deactivating system accounts rely on automatically provisioning the accounts at runtime for entities that were previously unknown. Organizations plan for the dynamic management, creation, activation, and deactivation of system accounts by establishing trust relationships, business rules, and mechanisms with appropriate authorities to validate related authorizations and privileges.
Related Controls: AC-16.

(09) RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS

Only permit the use of shared and group accounts that meet SnowBe Online account requirements.
Discussion: Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.
Related Controls: None.

~~(10) SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE~~

~~[Withdrawn: Incorporated into AC-2k.]~~

(11) USAGE CONDITIONS

Enforce any usage conditions established for SnowBe Online system accounts.
Discussion: Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.
Related Controls: None.

(12) ACCOUNT MONITORING FOR ATYPICAL USAGE

(a) Monitor system accounts for; and
(b) Report atypical usage of system accounts to appropriate departments.

Discussion: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals.
Organizations assess and document privacy risks from monitoring accounts for atypical.
Related Controls: AU-6, AU-7, CA-7, IR-8, SI-4.

(13) DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Disable accounts of individuals within immediately of discovery of any compromising actions.
Discussion: Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.
Related Controls: AU-6, SI-4.

Exceptions/Exemptions

Exceptions to this Security Plan are only permissible in rare situations where strict adherence would significantly disrupt business operations.

- Any request for an exception must be made in writing to the IT Security Manager.
- The IT Security Manager will evaluate it in collaboration with pertinent stakeholders.
- If granted, the exception will be in place until the policy changes or the person's employment status changes.
- The IT Security Manager and the Risk Management team will perform a detailed risk assessment and put suitable compensation controls in place to reduce potential risks during the exception period.
- The approval of exceptions will depend on these mitigating measures.

Enforcement

Violations of this IT Security Plan will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	05-Nov-24	Daphnie Bruno		First Draft – Created and updated Document.
1.1	06-Nov-24	Daphnie Bruno		Added Access Controls and definitions
1.2	09-Nov-24	Daphnie Bruno		Rechecked Format and converted to PDF

Citations

- https://www.montclair.edu/policies/all-policies/account-management-policy/
- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com Used to correct grammar errors and spelling errors.
- https://purplesec.us/resources/cyber-security-policy-templates/account-management/
- https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_A_5_1_1/home?element=AC
- Enhancement References: [SP 800-162], [SP 800-178], [SP 800-192].