Queens College Information Technology Standard	No: PR.AC.1.2 Account Management / Access Control
IT Standard: **Account Management**	Updated: 10/18/2002 Issued By: Office of the CISO Owner: Information Technology Services

1.0 Purpose and Benefits

The purpose of this standard is to establish the rules and processes for creating, maintaining and controlling the access of a digital identity to an entity's applications and resources for means of protecting their systems and information.

2.0 Authority

- **Responsible Office(s):** Information Technology Services
- **Responsible Executive(s)**: CIO
- **Responsible Officer(s)**: Chief Information Security Officer

3.0 Scope

This standard covers all systems developed by, or on behalf of the entity, that require authenticated access. This includes all development, test, quality assurance, production and other ad hoc systems.

4.0 Information Statement

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

4.1 Account Management/Access Control Roles

Account management and access control require that the roles of Information Owner, Account Manager and, optionally, Account Administrator and Entitlement Administrator, are defined and assigned for each resource and application. A listing of authorized users in these roles must be documented and maintained. The associated tasks and responsibilities for each role are described below. Each role may belong to one or more individuals depending on the application. In some cases, a single individual or group may be assigned more than one of these roles.

a. **Information Owner:** Information owners are people at the managerial level within an entity who:
    1. 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).
    2. Define roles and groups, as well as the corresponding level of access to resources for that role or group.
    3. Determining who should have access.
    4. Determine the identity assurance level for the application and/or data.
    5. 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.
    6. 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.

b. **Account Manager:** Account managers maintain accounts. They are the delegated custodians of protected data. Account managers:
    1. Maintain appropriate levels of communication with the information owners to determine the level or degree of access granted to an individual.
    2. Determine the technical specifications needed to set access privileges.
    3. Delegate account management functions to account administrators.
    4. Create and maintain procedures used in managing accounts.
    5. Perform all account administrator duties as required.

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

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

4.2 Account Types

Account types include: Individual, Privileged, Service, Shared, Default Non-Privileged (e.g., Guest, Anonymous), Emergency, and Temporary. All account types must adhere to all applicable rules as defined in the Authentication Tokens Standard.

a. **Individual Accounts:** An individual account is a unique account issued to a single user. The account enables the user to authenticate to systems with a digital identity. After a user is authenticated, the user is authorized or denied access to the system based on the permissions that are assigned directly or indirectly to that user.

b. **Privileged Accounts:** A privileged account is an account which provides increased access and requires additional authorization. Examples include a network, system or security administrator account. A privileged account may only be provided to members of the workforce whom require it to accomplish their job duties. The use of privileged accounts must be compliant with the principle of least privilege. Access will be restricted to only those programs or processes specifically needed to perform authorized business tasks and no more. There are two privileged account types - Administrative Accounts and Default Accounts.

    1. **Administrative Accounts:** Accounts given to a user that allow the right to modify the operating system or platform settings, or those which allow modifications to other accounts. These accounts must:
        i. be at an Identity Assurance Level commensurate with the protected resources to which they access.
        ii. not have user-IDs that give any indication of the user's privilege level, e.g., supervisor, manager, administrator, or any flavor thereof.
        iii. be internally identifiable as an administrative account per a standardized naming convention.
        iv. be revoked in accordance with organizational requirements

    2. **Default Privileged Accounts:** Default privileged accounts (e.g., root, Administrator) are provided with a particular system and cannot be removed without affecting the functionality of the system. Default privileged accounts must:
        i. be disabled if not in use or renamed if technically possible.

ii. only be used for the initial system installation or as a service account. When technically feasible, alerts must be issued to the appropriate personnel when there is an attempt to log-in with the account for access.
iii. not use the initial default password provided with the system.
iv. have password known or accessible by at least two individuals within the SE, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

c. Service Accounts: A service account is not intended to be given to a user but is provided for a process. It is to be used in situations such as to allow a system to run jobs and services independent of user interaction. Service accounts must:

1. have an assigned owner responsible for documenting and managing the account.
2. be restricted to specific devices and hours when possible.
3. never be used interactively by a user for any purpose other than the initial system installation or if absolutely required for system troubleshooting or maintenance. Wherever technically feasible, administrators should leverage "switch user" (SU) or "run as" for executing processes as service accounts.
4. never be for any purpose beyond their initial scope.
5. be internally identifiable as a service account per a standardized naming convention, where possible.
6. not allow its password to be reset according to any standardized and/or forced schedule. However, should an employee with knowledge of said password leave the entity, that password must be changed immediately.
7. have password known or accessible by at least two individuals within the entity, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

d. Shared Accounts: A shared account is any account where more than one person knows the password and/or uses the same authentication token. Use of shared accounts is only allowed when there is a system or business limitation preventing use of individual accounts. These cases must be documented by the information owner and reviewed by the Information Security Officer (ISO)/designated security representative. Additional compensatory controls must be implemented to confirm accountability is maintained. Shared accounts must:

1. have the tokens (e.g. password) reset when any of its users no longer needs access, or otherwise in accordance with the Authentication Tokens Standard.
2. be restricted to specific devices and hours when possible.
3. wherever technically feasible, have its users log on to the system with their individual accounts and "switch user" (SU) or "run as" the shared account.
4. have strictly limited permissions and access only to the system(s) required.

e. Default Non-Privileged Accounts: The default non-privileged account (guest or anonymous user) is an account for people who do not have individual accounts. An

example of where this might be necessary is on a public Wi-Fi network. This account type must:

1. be disabled until necessary.
2. have limited rights and permissions.
3. only be allowed after a risk assessment
4. have compensatory controls that include restricted network access.
5. be assigned a password that the user cannot change but that is changed monthly, at a minimum, by an administrator.
6. not allow the account to be assigned for delegation by another account.
7. have a log maintained of users to whom the password is given.

f. Emergency Accounts: Emergency Accounts are intended for short-term use and include restrictions on creation, point of origin, and usage (i.e., time of day, day of week). SEs may establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency accounts must be automatically disabled after 24 hours.

g. Temporary Accounts:** Temporary accounts are intended for short-term use and include restrictions on creation, point of origin, usage (i.e., time of day, day of week), and must have start and stop dates. An entity may establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation, such as for vendors, manufacturers, etc. These accounts must have strictly limited permissions and access only to the systems required.

4.3 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.

a. **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.

b. **Modifying Account Attributes (i.e., changing users' names, demographics, etc.):** Modifications must only be made by the authenticated user or an authorized account manager.

c. **Enabling Access:** Access is granted, based on the principle of least privilege, with a valid access authorization.

d. **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.

e. **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.

f. **Reviewing Accounts and Access:**
    1. Information owners must review all accounts on an annual basis (minimally) to determine if they are still needed.
    2. Access to privileged accounts must be reviewed every six months (minimally) to determine whether or not they are still needed.

3. Information owners must review account authorizations and/or user access assignments on an annual basis (minimally) to determine if all access is still needed.
4. Accounts or records of the account must be archived after 5 years of inactivity or after specific audit purposes are met.

g. 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.

h. Secure Log on Procedures: Where technically feasible, access must be controlled by secure log-on procedures as follows:

1. Must not display tokens (e.g., password, PIN) being entered.

2. Must display the following information on completion of a successful log-on:
    i. Date and time of the previous successful log-on; and
    ii. Details of any unsuccessful log-on attempts since the last successful log-on.

i. 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.

j. 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.

k. 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.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer’s exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

Chief Information Security Officer
Aaron Wheeler
Aaron.Wheeler@qc.cuny.edu

8.0 Revision History

This standard shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
10/18/2022	Initial changes to apply to Queens College	DVogel
03/20/25	Added number convention and control title	AWheeler
	Policy Implemented	

9.0 Related Documents

- Authentication Tokens Standard
- Security Logging Standard
- NIST Special Publication 800-63-3 Digital Identity Guidelines