Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S14-013
IT Standard: **Account Management/ Access Control**	**Updated:** 02/13/2024 **Issued By:** NYS Office of Information Technology Services **Owner:** Chief Information Security Office

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 New York State (NYS) Information Technology (IT) resources and assets in order to protect NYS data and information.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], established January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, NYS-P08-002: Authority to Establish Enterprise Information Technology Policies, Standards, and Guidelines

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

3.0 Scope

This policy applies to all “State Entities” (SE), defined as “State Government” in Executive Order 117 or “State Agencies” as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any Information Technology (IT) Resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different policy/standard, it must include the requirements set forth in this one. Where a conflict exists between this policy/standard and an SE’s policy/standard, the more restrictive policy will take precedence.

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 IT resources; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions. An SE should carefully consider relevant rules and regulations, as well as the need and breadth of access, to carefully determine how to best protect its IT resources. An SE may need to create its own policies and procedures to implement the requirements of this standard.

4.1 Account Management and 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 by the SE. The associated tasks and responsibilities for each role are described below. Each role may belong to one or more individuals depending on the resource or application. In some cases, a single individual or group may be assigned more than one of these roles.

a. **Information Owners** are people at the managerial level within an SE who:

- Delegate Account Managers to ensure the appropriate level of information access is provided. Delegation can be to individual users, groups, or third parties (e.g., another SE);
- Define roles and groups, as well as the corresponding level of access to IT resources for that role or group;
- Determine who should have access;
- Determine the Identity Assurance Level (IAL) for the application or data via the NYS-P20-001: Digital Identity Policy;
- Review that accounts and access controls are commensurate with overall business function and that the associated rights have been properly assigned annually, at a minimum; and
- Require business units with access to protected IT 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 Managers maintain accounts and are the delegated custodians of SE protected data who:

- Maintain appropriate levels of communication with the SE 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, if applicable;
- Create and maintain procedures used in managing accounts; and
- Perform all Account Administrator duties as required.

c. Account Administrators are an optional subset of the Account Manager role. They do not determine procedures. System rights and 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 or 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; and
- Assign new authentication tokens (e.g., password resets).

d. Entitlement Administrators are an optional subset of the Account Manager role. Rights and responsibilities are assigned to them by the Information Owner and generally include:

- Assigning rights and privileges to a user or group;
- Collecting data to periodically review user accounts and their associated rights; and
- Maintaining any necessary information supporting account administration activities, including account management requests and approvals.

4.2 Account Types

Account types used in NYS 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 NYS-S14-006: Authentication Tokens Standard. SEs must determine which account(s) are appropriate for access to IT resources based on the principle of least privilege.

a. **Individual Accounts** are a unique account issued to a single user. The account enables the user to authenticate to IT resources with a digital identity. After a user (e.g., NYS citizen, resident, employee, or other applicable user type) 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** are 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 who require it to accomplish their job duties. The use of Privileged Accounts must be compliant with the principle of Least Privilege, with access 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 Privileged Accounts.

   1. **Administrative Accounts** are given to a user to allow the right to modify the operating system or platform settings, or those which allow modifications to other accounts.

      Administrative accounts must:

      - Be at an IAL commensurate with the protected IT resources to which they access;
      - Not have user IDs that give any indication of the user's privilege level, (e.g., supervisor, manager, administrator, or any flavor thereof);
      - Be internally identifiable to the SE as an administrative account per a standardized naming convention; and
      - When no longer required, be revoked in accordance with the NYS-S20-001: Digital Identity Standard.

   2. **Default Privileged Accounts** (e.g., root, Administrator) are provided for a particular system and cannot be removed without affecting the functionality of the system.

      Default privileged accounts must:

      - Be disabled if not in use or renamed if technically possible;
      - 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;

- Not use the initial default password provided with the system; and
- 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** are not intended to be given to a user but are 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:

- Have an assigned owner responsible for documenting and managing the account;
- Be restricted to specific devices and hours when possible;
- 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” or “run as” for executing processes as service accounts;
- Never be for any purpose beyond their initial scope;
- Be internally identifiable to the SE as a service account per a standardized naming convention, where possible;
- 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 SE, that password must be changed immediately; and
- 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.

d. **Shared Accounts** are any accounts where more than one person knows the password 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) or designated security representative. Additional compensatory controls must be implemented to confirm accountability is maintained.

Shared accounts must:

- Have the tokens (e.g., password) reset when any of its users no longer need access, or otherwise, in accordance with the NYS-S14-006: Authentication Tokens Standard;
- Be restricted to specific devices and hours when possible;
- Have the users log on to the system with their individual accounts and “switch user”, or “run as” the shared account, wherever technically

feasible; and

- Have strictly limited permissions and access only to the system(s) required.

e. **Default Non-Privileged Accounts** (guest or anonymous user) are 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:

- Be disabled until necessary;
- Have limited rights and permissions;
- Only be allowed after a risk assessment;
- Have compensatory controls that include restricted network access;
- Be assigned a password that the user cannot change but that is changed monthly, at a minimum, by an administrator;
- Not allow the account to be assigned for delegation by another account; and
- Have a log maintained of users to whom the password is given.

f. **Emergency Accounts** are intended for short-term use and include restrictions on creation, point of origin, and usage (e.g., 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** 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. SEs 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 IT resources 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 or access control role(s) must be notified when account management activities occur, such as when accounts are no longer required, users are terminated or transferred, or system usage or need-to-know changes. The notification should be automated where technically possible.

Automated access control policies that enforce approved authorizations for IT 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 IAL of a system determines the degree of certainty required. The following table describes the level of confidence associated with each IAL.

IAL	*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

SEs must follow the NYS-P20-001: Digital Identity Policy to determine the appropriate IAL for their system. 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·	3
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, NYS driver's license ID, NYS 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 IALs, 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 or Removing Access**

- **Event/Risk Based (Administrative Disable) –** When an account poses or has the potential to pose a significant risk, either the account is disabled, or access attributes are removed upon discovery of the risk. Close coordination between the Information Owners, account managers and administrators, legal, incident response stakeholders and human resource managers is essential for timely execution of removing or restricting user access. Significant risk may include a disgruntled employee or one who has been identified by the SE 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 IT resources to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, or other organizations. An account identifier is required to identify these accounts and prevent inappropriate re-enabling of the account or access. Re-enabling the account requires explicit approval of the SE. Self-service mechanisms may not be used to re-enable the account.

- **De-provisioning Upon Separation –** All user accounts (including privileged) must be disabled immediately upon separation. In addition, credentials must be revoked in accordance with the NYS-S20-001: Digital Identity Standard, and access attributes must be removed. Self-service mechanisms may not be used to re-enable the account.

- **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 –**
- Information Owners must review all accounts on at least an annual basis to determine if they are still needed.
- Access to Privileged Accounts must be reviewed at least every six months to determine whether they are still needed.
- Information Owners must review account authorizations and user access assignments on at least an annual basis to determine if all access is still needed.
- Accounts or records of the account must be archived by their Authenticator Assurance Level (AAL) in accordance with the NYS-S20-001: Digital Identity Standard.

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 NYS-S14-006: Authentication Tokens Standard, or through the associated NYS-S20-001: Digital Identity Standard registration process.

h. **Secure Log on Procedures –** Where technically feasible, access must be controlled by secure log-on procedures as follows:
- Must not display tokens (e.g., password, PIN) being entered; and
- Must display the following information on completion of a successful log-on:
  - Date and time of the previous successful log-on; and
  - 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 NYS-S14-005: 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 required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

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

6.0 Definitions of Key Terms

All terms shall have the meanings found in http://www.its.ny.gov/glossary.

7.0 Contact Information

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

Chief Information Security Office
Reference: NYS-S14-013
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: https://its.ny.gov/policies

8.0 Revision History

This policy document should be reviewed consistent with the requirements set forth in *NYS-P09-003 Process for Establishing Information Technology Policies, Standards, and Guidelines*

Date	Description of Change	Reviewer
08/15/2014	Original Standard Release	Deborah Snyder, Acting Chief Information Security Officer
02/01/2017	Update of contact information and rebranding.	Deborah Snyder, Deputy Chief Information Security Officer
07/16/2020	Update revised Scope and Authority and update links from Identity Assurance to Digital Identity	Karen Sorady, Acting Chief Information Security Officer
12/1/2020	Update to align with federal guidance and industry best practices.	Karen Sorady, Chief Information Security Officer
05/19/2021	Updated Scope language	Karen Sorady, Chief Information Security Officer
02/13/2024	General Review, Update all links	Chief Information Security Office

9.0 Related Documents

- NYS-P20-001 Digital Identity Policy
- NYS-S20-001 Digital Identity Standard
- NYS-S14-006 Authentication Tokens Standard
- NYS-S14-005 Security Logging Standard
- NIST Special Publication 800-63-3 Digital Identity Guidelines