NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 89 Washington Avenue Albany, NY 12234	**NYSED ISO POLICY** User Account Password Policy **No: SECP5 - V:3.0: (Rev 11/20/2019)**
Issued By: NYSED Chief Information Security Officer	**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Policy

Passwords are an important part of the Department's information security program. Strong passwords applied to Department Information Technology (IT) resources reduce the risk of unauthorized access to electronic information. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of changing these passwords.

The benefit to the Department will be an enhanced security of Departmental information through use of stronger passwords.

2.0 Scope

There are four types of logon accounts used by the Department:

1. User Accounts – Unique accounts issued to a single Individual (i.e. employees, vendors, consultants, interns, volunteers, affiliates, etc.), often referred to as 'end-users' and do not possess the privileges as an administrative account.

2. Administrative Accounts (Privileged) – Unique accounts issued to a single Individual, but these accounts have a higher degree of access privileges to systems (e.g. 'root' access on a Unix system). These accounts are intended to be used by authorized personnel only (such as IT personnel), for performing administrative tasks such as maintaining user accounts, performing password resets, and managing systems.

3. Public/Anonymous accounts – Use of these accounts is purposefully unrestricted. There may or may not be an associated password with such accounts, but when there is such a password, the password may be shared freely (e.g. public wireless password provided in a conference room). In such cases, as a matter of best practice and as feasible, the public password shall follow strong password rules as described for user and administrative account password requirements, below.

4. Service Accounts – Used only for automated processes between systems. These accounts are not to be used by individuals to login to systems, with the exception of troubleshooting to ensure that the account is working properly.

This policy applies to all User, Administrative, and to Public/Anonymous accounts and to all Department IT resources where a password is required or optional, including all system logon passwords, encryption passwords, portable storage device passwords, file passwords, etc.

Service accounts are covered under the NYSED Service Account Password Policy (SECP8).

It is the responsibility of all users of Department IT resources to read and understand this policy and to create their passwords in accordance with its terms. In addition, users must read and understand the NYSED Information Security Policy and its associated policies and standards.

3.0 General Password Requirements

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Department's entire network. As such, all users and administrators are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. It is important to set a strong password and change them regularly.

The following password minimum requirements apply to ALL logon accounts:

- Passwords:
  - Must never be shared or displayed on a screen.
  - Must be classified and handled as Department Confidential information.
  - Must be changed whenever there is any indication of compromise.
  - Must not be reused for at least 4 iterations.
  - Must be encrypted when transmitted electronically with a strong encryption protocol
  - Must be encrypted or hashed when held in storage.
  - When embedded in configuration files, source code or scripts, they must be either encrypted or secured with compensating controls which provide a comparable level of protection.
- Whenever technically feasible, a password-protected screen lock must be activated on a system after 10 minutes of user inactivity.
- Whenever technically feasible, all systems that provide access to sensitive, restricted, or confidential information must automatically disable an account after six (6) sequential invalid login attempts within a fifteen (15) minute period. After such account is disabled, the account must remain disabled for a minimum of fifteen (15) minutes.
- Department system passwords should be different than any other non-Department system passwords used by an individual (e.g. a social media site password such as for Facebook should not be the same as the one used by an individual to login to the NYSED network).

4.0 User and Administrative Account Password Requirements

A password is used to authenticate or identify an individual. When an individual is first granted access to a system, or when a password reset is required, the individual will be given a temporary or initial password. The following minimum requirements must be met for temporary or initial passwords:

- Temporary or initial passwords will not be shared with anyone except the system administrator, the Individual's manager, and the individual for which the password was intended.
- Temporary or initial passwords will not be reused. A new password will be created for each new account.
- The Individual wishing to change his/her password, or have it reset must be positively identified by identification, by knowledge of the current password, or by demonstrating knowledge of the account.

- Whenever technically feasible, temporary or initial passwords will be set to automatically expire in a system after first initial use.
- Individuals will change the temporary or initial password immediately upon first logon to the system.

Thereafter, each individual is responsible for selecting and protecting passwords that provide security for the Department information they access. The following password minimum requirements must be met:

- All individuals are responsible for their own password security.
- Any individual that suspects a password has been compromised must report this information security incident to the Information Security Office immediately (infosec@nysed.gov).
- Always use a strong/complex password, regardless of whether an IT resource allows for a weaker password.
    - Passwords must be a minimum of 8 characters (15 characters or more is recommended).
    - Whenever technically feasible by the IT resource, passwords must contain at least three of the four requirements below:
        - An uppercase character.
        - A lowercase character.
        - A numeric character.
        - A special character. For example: #$&*
            - NOTE: some systems do not allow use of certain special characters
    - Some legacy systems may not have the capability to enforce these rules, in those cases it is up to the individual to select a password that meets these requirements.
- Never write passwords down and/or post in your work area.
- Never send a password electronically unencrypted (e.g. through unencrypted email).
- Never include a password in a non-encrypted stored document.
- Never tell anyone your password.
- Never provide hints to anyone concerning the format of your password.
- Never use the "Remember Password" feature of application programs such as Internet Explorer, email systems, or any other program.
- If anyone asks for your password, do not provide it, refer them to the Information Security Office (ISO) instead.
- Do not let someone look over your shoulder when typing your password.
- Passwords are not to be shared with other individuals, either inside or outside the Department (individual user accounts must not be shared).
- Users must be careful not to use password hints or answers to challenge questions that can be found on their social media sites (e.g. Facebook).
- Passwords issued by ITS (including the Help Desk) should be changed immediately upon first logon.
- Department passwords must be changed at least every 180 days (except for mainframe systems, which will be 213 days).
- Everyone is directly responsible for use of their passwords. Any action or activity taken with a password will be attributed to the owner of the password.

5.0 Password Reset Requirements

Due to the prolific usage of User, Administrative, and Public/Anonymous accounts by many individuals, these types of logon accounts require frequent password resets. The following password reset requirements must be met for these accounts:

- All password recovery and reset mechanisms, including manual password resets, must verify the user's identity.
- Automated password recovery processes must require some form of personal identification in addition to a personally chosen hint or question and answer. All answers must be stored in hashed format.
- Password reset notifications must always be emailed only to the end user needing the password reset, and no one else. The email must include contact information so that the user can notify the Department immediately if they did not request a password reset.
- Initial or reset passwords issued by system administrators must be valid only for the first log on. Users must create unique passwords at the first log on.

6.0 Device and File Password Requirements

Encrypted devices (e.g. USB flash/thumb drives) and files are IT resources that may be used by individuals, and these also have passwords that must also be protected. The encryption is only as strong as the password used. The following requirements must be implemented to safeguard encrypted Department information.

- Device and file passwords must only be shared with the required individuals on a 'need-to-know' basis.
- Any individual that suspects that a device or file password has been compromised must report this information security incident to the Information Security Office immediately.
- Department password strength requirements must be followed, even if the device or file encryption software does not require them.
- When transmitting an encrypted device or file, the password must be delivered separately from the device or file (e.g. phone call).
- Whenever feasible, device and file passwords must also be changed at least every 180 days.
- Device passwords should never be written down on the device or accompany the device.

7.0 Technical Access Controls

Wherever technically feasible, technical access controls will be enabled on Department IT resources to ensure that the password minimum requirements stated above are enforced (e.g. Microsoft Active Directory Password Complexity rules will be enabled). Wherever not technically feasible, equivalent controls must be established through other methods or procedures. For instance, a system administrator can use software tools periodically to detect weak passwords and require users with such to change them.

Department IT resources may also incorporate multi-factor authentication access controls in order to enhance the security of highly sensitive Department information.

8.0 Password Reset Assistance

System Administrators and Department Help Desk staff shall have the authority and ability to reset system passwords where proper authorization has been given and audit trails are in place.

9.0 Compliance

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least every two years to ensure relevancy. To accomplish this assessment, ISO may issue requests for information from other program office departments. The information garnered will be used to develop any reporting requirements as may be requested by the Department Chief Privacy Officer, the Board of Regents, or Legislative entities.

Compliance with this policy is the responsibility of all persons who have any type of password on any Department system or file. All individuals have the responsibility to protect their passwords and the information that may be accessed by their account if their password has been compromised.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function; the office shall request an exception through the NYSED Information Security Exception Policy process.

Any violation of this standard may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

10.0 Definitions of Key Terms

Information Technology (IT) Resources – Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

Multi-factor Authentication – a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are) (Rosenblatt & Cipriani, 2013).

11.0 ISO Contact Information

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

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Website: http://atwork.nysed.gov/iso/
Email: infosec@nysed.gov

12.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
08/03/2017	DRAFT	CISO

3/12/2019	Updated ISO Office and phone number, updated information in Section 1, 3, and 7	Marlowe Cochran, Chief Information Security Officer
11/20/2019	Reviewed, Updated Contact Information, update user account definition	ITS, CPO, CISO
12/25/2019	Original Standard Release	Marlowe Cochran, Chief Information Security Officer

13.0 Related Documents

- NYSED Information Security Policy
- NYSED Information Security Exception Policy
- NYSED Service Account Password Policy

14.0 References

1. Rosenblatt, S., & Cipriani, J. (2013). Two-factor authentication: What you need to know (FAQ). Retrieved December 06, 2016, from https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/