NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office (ISO)
89 Washington Avenue
Albany, NY 12234

User Account Password Policy

-286 0 49 Sscn /TT1 1 Tf (Rev 01/20/2019) 4

- 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.

entuald12 u(o)2 (o)2 (o)20 Tc 0 cas (te6ch0 Tc 0 -0.9a (tct)-0.9 (b)0 -0.9 Td (h

Thereafter, each individual is responsible for selecting and protecting passwords that provide security 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 secur

- 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 passwo used. The following requirements must be implemented to safeguard encrypted Department information.

- Device and file passwords must only be shared with the required individuals ‘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

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 requirem

3/12/2019	Updated ISO Office and phone number, updated information in Section 1, 3, and7	Marlowe Cochran, Chief Information Security Officer
11/20/2019	Reviewed,	