NORTHUMBERLAND COUNTY PUBLIC SCHOOLS

NES NMS NHS

Information Technology Department

Password Policy

Version:	1.3
Effective Date:	08/01/2022
Last Reviewed:	06/14/2022
Last Approver:	Javornda Ashton
Replaces:	1.0

PURPOSE

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and frequency of change. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Northumberland County Public Schools (NCPS) resources. All users, including contractors and vendors with access to NCPS systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

SCOPE

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that is used for NCPS operations.

RESPONSIBILITY

The Director of Educational Technology is responsible for the review, approval, and enforcement of this policy. This policy must be reviewed and updated annually, or when significant changes occur that could impact any safeguard in this policy.

COMPLIANCE

Compliance is expected with all NCPS 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 NCPS function, entities shall request an exception through a technology request in the IncidentIQ system at https://ncps.incidentiq.com. Any associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Password Policy

All users of NCPS systems should use strong passwords and change their passwords at regular intervals. Systems should be configured for adherence and enforcement of this Password Policy.

1. Password Construction
    1.1. Passwords should be securely constructed by users including:
        1.1.1. A minimum of 14 characters.
        1.1.2. Containing at least three of the five following character classes:

1.1.1.1. Lower case characters
1.1.1.2. Upper case characters
1.1.1.3. Numbers
1.1.1.4. Punctuation
1.1.1.5. “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)

2. System Password Restriction
   2.1. The minimum password age should be set to 1 day.
   2.2. All passwords should be changed at minimum every 365 days.
   2.3. Password history should be set to 24 passwords remembered.
   2.4. Reversible encryption should not be used for any password storage.
   2.5. Users should be locked out for 15 minutes after 10 invalid login attempts.
   2.6. Teachers' computers should have a screensaver lockout set to 60 minutes of idle time. All other computers should be configured to lock the computer after 15 minutes of idle time.
   2.7. Users should be required to put in their password to unlock the system before resuming after the screensaver lockout has been engaged.
   2.8. Users should lock computers when they are to be unattended, so the password is required for any access.
3. Password Guidance
   3.1. Users should try to create passwords or passphrases that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or " Th1s m@y b 1 way 2 remember" or some other variation. (NOTE: Do not use either of these examples as passwords!)
   3.2. Passwords should not consist of:
      3.2.1. Common single dictionary words (English or foreign.)
      3.2.2. Anything that could be easily guessed based on public information of a user or tied back
      3.2.3. Names of family, pets, friends, co-workers, birth dates, address street names, phone numbers, or any other information that can be easily gleaned from social media or the internet.
      3.2.4. The words “Password” “Northumberland" "NCPS" or any derivation.
      3.2.5. Any word or number patterns like “aaabbb” “qwerty” “zyxwvuts” “123321” etc.
      3.2.6. Any of the above spelled backwards.
      3.2.7. Any of the above preceded or followed by a digit or year (e.g., secret1, 1secret, secret2022)
4. User Protection of Passwords
   4.1. Always use different passwords for NCPS accounts from other non NCPS access (e.g., personal ISP account, option trading, benefits, etc.).
   4.2. Always use different passwords for various NCPS access needs whenever possible. For example, select one password for systems that use directory services (i.e., LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.

4.3. Do not share NCPS passwords with anyone. All passwords are to be treated as sensitive, confidential NCPS information.
4.4. Passwords should never be written down or stored on-line without encryption.
4.5. Do not reveal a password in email, chat, or other electronic communication.
4.6. Do not speak about a password in front of others.
4.7. Do not hint at the format of a password (e.g., "my family name")
4.8. Do not reveal a password on questionnaires or security forms.
4.9. If someone demands a password, refer them to this document and the IT Department.
4.10. If an account or password compromise is suspected, report the incident to the IT Department.

Policy References to IT Standards

K-12 Model Security Plan V1.0 – Create a password policy if you do not currently have one. This policy should include:

- Complexity and Length
- Password Age
- Not Repeating Passwords
- Hashing stored passwords
- Failed password attempt lock outs
- Not allowing sequential or repeated characters