NEOnet | Northeast Ohio Network for Educational Technology

System Security Policy

Table of Contents

1 System Security Policy

1.1 Overview

The Governing Board of the Northeast Ohio Network for Educational Technology (NEOnet) recognizes that data maintained by NEOnet is held in public trust by contractual agreement on behalf of each participating board of education. The NEOnet Board adopts the following policy statements concerning access to and security of the data. These statements are intended to assure the inviolability of the data, provide for procedures to permit access to data, and recommend features which districts and NEOnet can implement to promote system and data access and security.

1.2 Data Access

Data maintained by NEOnet shall be under the control of the district for purposes of access and the provisions of ORC 149.43, "Availability of Public Records".

- District personnel access upon the written authorization of the District's Superintendent or the Treasurer if the request is for access to financial data. NEOnet shall provide a standard form for authorization. Such access may be restricted (as may be practical or technically possible) to certain data sets and/or specific access types.

- NEOnet staff may access data when such access is within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities.

- Requests for information within the scope of the ORC 149.43 "Availability of Public Records" shall be administered within the Board Policies and Procedures of each participating member district.

1.3 Security Recommendations

The first point of security is access to the computer system and its data via the local network of users. Each user must complete the NEOnet "User Account Authorization Form" before an account will be assigned. All policies and procedures outlined in the "User Account Authorization Form" are considered a part of this policy.

To enhance security and reduce the risk of unauthorized access, the following guidelines shall be followed:

- Users will be assigned one unique account (username) for access to the system.

- Access to privileged or system accounts shall only occur with the authorization of the NEOnet Executive Director.

- Sufficient audit alarms shall be enabled to track attempts to break into a user or system account and other security related events. The audit log shall be reviewed daily for suspicious entries.

- In the event any district personnel, (including but not limited to: administrators, treasurers, staff, students, etc.), violate or attempt to violate this policy or the computer system, the proper district authorities (and if necessary, legal authorities) will be notified. The NEOnet Board of Director's reserves the right to take whatever legal steps they deem appropriate.

In all events, the NEOnet Executive Director shall have the authority and responsibility to take actions necessary to insure the integrity of the data and security of the computer system, or to enable district users to utilize the computer system to fulfill the duties associated with their position. In such cases, a return to the adherence of these guidelines shall be made as soon as practical.

1.4 Account Holder’s Responsibilities

- Account holders may use the NEOnet computer system for business-related activities only. Users are expected to report all potential misuse to their appropriate supervisor and/or to the NEOnet Executive Director.

- Improper use includes, but is not limited to, the use of NEOnet-owned and/or NEOnet-operated computer systems and networks for the purpose of gaining unauthorized access to internal or external computer systems or accounts, for personal purposes, or for purposes of personal gain. Examples of misuse could be transmitting offensive, harassing and/or devaluing statements, developing and transmitting inappropriate graphics, transmitting sexual or ethnic slurs or jokes, soliciting other employees, developing chain letters, communicating matters of private conviction or philosophy, permitting unauthorized access, etc.

- Account holders are responsible to safeguard their passwords, other access protocols, school district and NEOnet information, in whatever form. This information is defined as any plans, ideas, or data that has not been approved for release to the general public. This could be technical data, business data, or employee data.

- Printed output that is considered confidential shall not be printed on any common printer. Instead, it must be printed in a secure area or some other restricted area, such as the employee's office.

- Account holders will ensure that their account is protected from unauthorized access. Passwords are the computer's first line of defense against unauthorized system access. All users should adhere to the following password controls:

    - Passwords shall be non-meaningful terms and should contain a combination of both letters and numbers. Passwords should not be of a common nature such as last name, job title, children's names, street address, pet's names, etc.

    - Passwords should not be displayed, divulged, or accessible to or shared with others. If there is any reason to suspect that a password has become known, it should be changed immediately using the MENU item PASSWORD CHANGE. Passwords should never be written down, attached to the terminal, placed under the keyboard, or any other means which would allow for possible break-in.

  - Users should be aware of the LAST LOGIN time of his/her account and report to the NEOnet staff if it does not correspond with the last actual log in.

  - Users should not put passwords into command files or program them into hot keys.

- Users should notify the NEOnet staff of any unauthorized access to their account when detected.

- Users should ensure their computers, when not in use, are properly logged off the system.

1.5 Account Management Policies

- Requests for new accounts must be submitted in writing using a NEOnet Account Request Form. The approval process will include a written signature by the user. This signature represents understanding and adherence to the policies contained in this document.

- Copies of the NEOnet Account Authorization Form are available in both electronic and hardcopy formats. Either form can be obtained by contacting the NEOnet staff.

- Account requests will be received Monday through Friday. The account request will be processed and available within 3 business days of receipt of a properly filled out and signed form. The employee should contact NEOnet to receive his /her password.

- All account usernames will be set-up with all or part of the district name and user name. If another user has the same last name within the district, the new account will contain the user's last and first names and, possibly, a number to form a unique username.

- Passwords for new accounts will be initially set by the NEOnet staff. It will be up to the employee to determine a proper password for subsequent changes. The initial password will be pre-expired, meaning it must be changed during the first login session.

- No GUEST accounts will be issued.

- For security reasons, each school district should immediately notify NEOnet if an employee has been terminated or has left their organization. The accounts and files of terminated employees will be disabled immediately and the account and files will be deleted.

- Similarly for security reasons, each school district should notify NEOnet when any account holder is placed on a leave of absence, short-term or long-term disability. That person's account will be disabled. The account can be re-opened at the request of the Superintendent and/or Treasurer. Password controls for all accounts include the following:

  - All accounts are set to expire the password every 90 days. It is the user's responsibility to reset their password. The password expiration will be 90 days from the time the password was last changed.

  - All accounts will have a password minimum length of 8 characters. Up to 31 characters may be used. Letters, numbers, and the underscore character may be used in a password.

  - If a password is lost or forgotten, the user must call the NEOnet staff to establish a new one. The computer stores passwords using a one-way encryption algorithm. After they are encrypted, passwords cannot be returned to their original readable form. Since there is no method to look up a user's password, a new pre-expired password will be generated.

- Any accounts that have not been used in 180 days, including those never logged into, and all accounts with pre-expired passwords will be “DISUSERED”. These accounts will be deleted at the discretion of the Executive Director.

Adopted: May 3, 2009 Edited: January 2014