

# **Lakeshore Northeast Ohio Computer Association**

5700 West Canal Road  
Valley View, Ohio 44125

Telephone: 216-520-6900  
Fax: 216-520-6969

URL: [WWW.LNOCA.ORG](http://WWW.LNOCA.ORG)

## **System and Network Security Policy Internet User Guidelines and Policy**

Effective: July 1, 2006

# LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION

## System and Network Security Policy

Data maintained by the Lakeshore Northeast Ohio Computer Association ("LNOCA") is the property of the school district or other customer which entered such data or to which such data is assigned. As a custodian of customer data, LNOCA is concerned that unauthorized use of such data be prevented. Accordingly, LNOCA has developed the following policy to maintain the integrity of customer data, to promote system security, to permit authorized access to data, and to prohibit unauthorized access.

### I. DATA ACCESS

Access to customer data shall be available as follows:

#### A. Customer Personnel

1. The Superintendent, or Chief Executive Officer of a LNOCA customer shall have read-only access to all customer data. The Treasurer or Chief Financial Officer shall have full access to fiscal data and read-only access to non-fiscal data.
2. Other employees of a LNOCA customer shall be granted access to said customer's data with the authorization of the customer's Superintendent, Chief Executive Officer, Treasurer or Chief Financial Officer as appropriate. Authorization for access must be provided in writing, preferably on the LNOCA provided user authorization form.
3. The Superintendent, Chief Executive Officer, Treasurer or Chief Financial Officer may designate an individual, or individuals, with authority to grant access to the customer's data.
4. Customers may restrict (to the extent practical and technically possible) access to certain datasets and/or specific access types.
5. LNOCA shall provide each customer with an authorization form for the purpose of granting user access.

#### B. LNOCA Personnel

LNOCA employees shall be granted access to customer data if such access is necessary to carry out their assigned duties, but only for the purposes of maintaining data structure, researching and correcting problems, and providing back-up capabilities.

#### C. Third Parties

1. Third parties shall be granted access to customer data only when authorized in writing by the Superintendent, Chief Executive Officer, Treasurer, Chief Financial Officer or their designee. A "third party" is defined as any individual or group of individuals not employed by customer or LNOCA.
2. Detailed staff and financial data and aggregate student data shall be transferred to the Ohio Department of Education, as authorized and/or required by applicable laws and regulations.

# LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION

## System and Network Security Policy

### II. DATA SECURITY PROCEDURES

The local network of users is the first point of security in the LNOCA network. To enhance security and reduce the risk of unauthorized access, LNOCA requires that the following procedures be followed:

- A. Each user will be assigned one unique account for access to the network.
- B. Each user account must have a password containing at least 6 characters. The password shall be treated as confidential information by the user. The user is responsible for protecting the confidentiality of his or her password, other access protocols, as well as customer and LNOCA information, in whatever form. Neither LNOCA nor any LNOCA customer shall maintain a list of passwords.
- C. Fiscal system users are required to change his or her password at least once every 90 days. Other system users are required to change his or her password at least every 180 days. "Captive" accounts (accounts which have access to only limited, non-system programs and commands) will be assigned passwords by LNOCA, and their passwords will be changed at least once every year.
- D. A review of user account activity will be performed by LNOCA staff on a quarterly basis. User accounts that have not been accessed within the prior 180 days will be disabled. Users are responsible for ensuring that their terminals, when not in use, are properly logged off the system.
- E. A user shall be granted only those privileges that are consistent with the duties and responsibilities of his or her position. Authorized privileges shall be categorized as " normal " or " extended. " " Normal " privileges will be granted when a user logs onto the system, and they represent those privileges required for the performance of the user's normal duties. "Extended" privileges are those privileges which the user may be authorized to use, but which must be specifically enabled by the user before being utilized.
- F. Access to the LNOCA network via an electronic network outside the LNOCA area will be restricted to the minimum level of access necessary for authorized users. No "general access" accounts shall be maintained.
- G. Access to privileged or system accounts shall be granted only upon authorization of the LNOCA Executive Director, LNOCA Assistant Director, Business Services, or LNOCA System Administrator. Upon completion of outside access to a privileged account, the account password shall be changed to prevent further access without authorization by LNOCA.
- H. OECS\_SYSMAN privileges to any state software shall be granted only upon written request from the Superintendent, the Chief Executive Officer, Treasurer or Chief Financial Officer of a customer, and such request must state the purpose, length of time needed, and the employees who shall be granted such access. LNOCA shall not be responsible for such customer's files during the specified time period. LNOCA will not modify or make corrections to the customer's files, but will serve only in an advisory capacity.

# LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION

## System and Network Security Policy

- I. Audit alarms shall be used to track attempts to break into a user or system account, as well as other attempts to breach security. LNOCA shall review the audit log for suspicious entries on a daily basis, and such entries shall be filed for future reference.
- J. For security reasons, each customer must inform LNOCA immediately of any employee of such customer who has been terminated or has voluntarily left the employment of such customer. The accounts and files of such an employee shall be disabled and deleted within five business days.  
  
Each customer must notify LNOCA immediately of any employee who has been placed on leave of absence, or short-term or long-term disability. Such an employee's account shall be disabled and re-opened only at the request of the employee's immediate supervisor.
- K. In order to maintain the integrity of production data and software LNOCA may create test, demonstration and "play" datasets with user accounts as necessary and appropriate. A user authorization form for creation of non-production accounts is not required. Access to non-production datasets shall be granted to individuals consistent with the duties and responsibilities of his or her position for testing and training purposes.

In all events, the Executive Director, Assistant Director, Business Services and the System Administrator of LNOCA shall have the authority and responsibility to take all actions necessary to ensure the integrity of data and the security of the computer system and to enable users to utilize the computer system as authorized.

# LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION

## System and Network Security Policy

### III. NETWORK SECURITY POLICIES

#### A. Open Ports on LNOCA's Firewall/DMZ

LNOCA administers the firewall that protects all of the systems within the educational entities served by LNOCA from the Internet; LNOCA is responsible for creating open ports for access to systems within the network. Open ports create an inherent security risk for the specified system and subsequently other systems within LNOCA's Network. Open ports could allow systems to be compromised by malicious entities on the Internet. Once a system is compromised, since that system is already behind LNOCA's firewall, the reality exists for that system to be used to attack other systems in other school buildings without firewall protection.

All outside access shall be denied at the firewall. However, if a District or school wishes to have access from the Internet to a node in their network, a release form shall be signed authorizing the creation of an open port. The individual signing the authorization form states that they understand the risks and the District or School assumes the responsibility to secure the system and to accept the liability for any resulting damages caused through this open port.

**LNOCA reserves the right to disable an open port if it is determined that said open port has been compromised.**

# LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION

## System and Network Security Policy

### IV. E-MAIL FILTERING POLICIES

#### A. SPAM filtering

LNOCA administers the flow of e-mail from the Internet to the schools within the network. LNOCA has facilities to block e-mail messages categorized as SPAM and/or unacceptable. Any effort to reduce the amount of unwanted e-mail messages will result in the loss of some legitimate e-mail messages. LNOCA's Staff will make every effort to minimize the number of legitimate e-mail messages that are blocked by the filter.

#### B. Virus filtering

LNOCA has facilities to block e-mail messages containing computer viruses. E-mail messages containing computer viruses will be blocked to prevent computer viruses from infecting the LNOCA network.

LNOCA's systems will filter all inbound e-mail served by LNOCA's internal e-mail servers. LNOCA's systems will also filter all inbound e-mail messages served by non-LNOCA e-mail servers. Any District or School that does **not** want e-mail filtering enabled for their own internal e-mail servers must provide written authorization to bypass filtering signed by the District Superintendent or by the Non-Public School Administrator, as appropriate.

**LAKESHORE NORTHEAST OHIO COMPUTER ASSOCIATION**  
**System and Network Security Policy**

**V. INTERNET CONTENT FILTERING POLICIES**

**A. Content filtering**

Customers that that choose to administer Internet content filter provided by LNOCA for their school, or school district, must designate those individuals the district authorizes to block and/or unblock access to specific Internet websites. Content filter administrators have the authority to bypass the filtering service provided by LNOCA. Individuals granted this authority also assume the responsibility for their actions as administrators of the Internet content filters.

# **Lakeshore Northeast Ohio Computer Association**

## **Internet User Guidelines and Policy**

The LNOCA communication network is an electronic computer network with access to the Internet. The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. LNOCA users, therefore, have access to electronic mail communication with people all over the world; information and news from, as well as the opportunity to correspond with, research institutions; public domain and shareware software of all types; discussion groups on a plethora of cultural, political, scientific, and general or special interest topics; and many universities, libraries (including the Library of Congress), non-profit organizations, commercial companies, and other organizations.

Along with access to computers and people all over the world comes the availability of material, which may not be considered to be of educational value within the context of the school setting. While it is impossible to control all materials on a global network, LNOCA has taken precautions to restrict access to controversial materials. The guidelines below are designed to prevent inappropriate use of the LNOCA network.

### **I. INAPPROPRIATE USES**

The LNOCA network shall not be used in any inappropriate ways or for any inappropriate purposes as determined by LNOCA system administrators. Inappropriate uses include, but are not limited to, the following:

- A.** Placement of unlawful information, computer viruses or harmful programs on the system, whether in public or private files or messages.
- B.** Unauthorized alteration of system software.
- C.** Transmission of any material in violation of state or federal law or regulation (including but not limited to copyrighted material, material protected by trade secret, and threatening or obscene material).
- D.** Use of obscene, vulgar, threatening, abusive, defamatory or otherwise objectionable material or language in public or private files or messages. No one shall use any LNOCA resource to obtain, view, download, store, forward or otherwise access any such material or language.
- E.** Use for personal business, for-profit activities or commercial transactions, unless authorized in writing by LNOCA in advance.
- F.** Use for employee recruiting (except posting of available positions by school districts), securing employment, product advertisement or political activities.
- G.** Use of another user's password or account.
- H.** Any use that violates another user's privacy, including without limitation, disclosure of such user's password, personal address, phone number or social security number.
- I.** Any use that interferes with use of the network by others or that degrades system performance.

# Lakeshore Northeast Ohio Computer Association

## Internet User Guidelines and Policy

### II. POLICY

The user's use of the computer network and Internet is a privilege, not a right. A user who violates this Policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which LNOCA may refuse to reinstate indefinitely. A user violates this Policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this Policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. LNOCA may also take other disciplinary and punitive actions including pursuit of civil and/or criminal charges against individuals and/or organizations that violate this policy.

Use of the LNOCA network is limited to its registered account holders. Each account holder is responsible for any use or misuse of his or her password and/or account. While the network is intended for the private use of LNOCA's account holders, it is not guaranteed to be private. LNOCA reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. LNOCA system administrators will determine whether any use of the network is inappropriate or unauthorized, or whether any material or language is objectionable. LNOCA's decision will be final.

A teacher must closely supervise students using the LNOCA network at school. Parents or guardians shall be responsible for supervising students' use of the network outside school.

**Use of any information obtained through the LNOCA network is at the user's risk. LNOCA specifically denies any responsibility for the accuracy or quality of such information.**

**LNOCA does not make any warranties, express or implied, including without limitation any warranty of merchantability or fitness for a particular purpose, with respect to the network, its services or features. Furthermore, LNOCA shall not be liable for any special, incidental, indirect, or consequential damages or for the loss of profit, revenue, or data arising out of any use of, or inability to use, the network, even if LNOCA shall have been advised of the possibility of the potential damage or loss.**

**Legal Reference:** *Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)*  
*Communications Act of 1934, as amended (47 U.S.C. 254[h],[i])*  
*Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)*