

## Security Standards for EMU Network Users

---

Computer security means preventing unauthorized access to information stored on the computer or the network and preventing the loss or destruction of that information and related equipment.

Computer security is a part of a larger security mindset encouraged at EMU. A security mindset means being careful with confidential, sensitive, and private information in all forms. It means sound judgment and habits such as locking unattended offices and shredding confidential documents when disposing of them. Computers and the network are increasingly used to store sensitive, private, and confidential information. Access to such information should be shared based on a need to know and should be carefully guarded against unauthorized access, just as the paper copy would be guarded.

Good security practice requires that an internal monitoring system be used for performance monitoring and trend analysis of the campus computer network.

### Privacy

Network monitoring takes place within the context of respecting the privacy rights of users. “Persons with access to confidential institutional data are not permitted to access or disclose this information unless such action is required in the performance of their duties and responsibilities” (from *Acceptable Use Policy for EMU Campus Computers Networks*). Network monitoring data are confidential institutional data. You can expect that data identifying you and your use of the network will not be viewed routinely.

### Rationale for Monitoring

Network monitoring addresses the following issues:

- a) Protecting university resources from potential damaging activity originating from “within” the EMU network.
- b) Protecting university resources from potential damaging activity originating from “outside” the EMU network.
- c) Protecting resources outside the EMU network from potential damaging activity involving the use of EMU network resources.
- d) Ensuring adequate bandwidth performance for EMU network users.

### How Monitoring Works

EMU network monitoring continuously collects data on all network activity, including but not limited to identification of all sites visited, addressing of email sent and received, and names of all files accessed on campus network servers. Data collected for monitoring does not include contents resulting from network activity—whether web sites, emails or files accessed.

Whenever possible, data are collected and initially analyzed in a form such that users are not directly identifiable. Initial analysis is automated and Information Systems staff reviews only aggregate data. Data are not further processed unless anomalies occur. Such anomalies include potential security violations identified by automated scripts, network congestion and bounced e-mail. If anomalies turn out to impact network security or liability, or involve overuse of network resources, data will be further reviewed, and if necessary, processed to the point of identifying individuals who may have been involved. Network administrators will identify and contact users only when necessary to track network system anomalies that have a negative impact on the network, or when directed to do so by the President or Provost, or their designees through the Director of Information Systems.

Certain data are collected about EMU-owned computers in order to manage them efficiently (broadly, “desktop management”). This includes collecting a list of software installed and connected hardware peripherals. As with network monitoring, if anomalies occur for an EMU owned computer the collected information may be reviewed by appropriate Information Systems staff members.

EMU’s standards for computer security, required of all computer users at EMU, are as follows:

1. **Personal computers are to be secured against unauthorized access** when unattended during the work day or outside of office hours. You can accomplish this either by logging out of the computer, locking your office

## Eastern Mennonite University

### Security Standards for EMU Network Users

---

door, or protecting your computer with a password enabled screensaver that activates after no more than 15 minutes. Computers running Windows XP can also be locked by pressing Ctrl-Alt-Del followed by Enter.

2. **Username\* and passwords should not be shared under any circumstance.** Users are often tempted to share username and/or password when working together on projects that require sharing computer documents and data files. At EMU these sharing requirements are accommodated with separate usernames that share network data folders.
3. **Username passwords are not to be saved by your computer or applications in a way that lets you log into the network without entering your password.** For example, Macs let you store your password in a way that logs you into the network automatically without ever again entering the password. (The problem is that it logs anyone else into the network who turns on your computer.) You should never violate this standard, even though you may lock your door or perform other security measures.
4. **Username passwords should consist of at least 5 characters and include at least two numeric and two alphabetic characters.** Your password should NOT be any word that can be found in any dictionary. It also should NOT be any proper name. Ideally, your password should contain at least one special character. Examples: / , . \* -.
5. We actively protect our network from computer viruses. **Do not disable the anti-virus software on your computer and do report any incidence of viruses to Information Systems.**
6. We must all be very careful to protect sensitive, private, or confidential information stored electronically. To this end, **you should not store sensitive, private, or confidential information on the local hard drive of your computer.** Instead, use the network drives that require logging in with a username and password. If you choose to store such information on the local hard drive, you must assume total responsibility for your data, taking care to lock physical access to the computer when unattended, not sharing your computer with other users, and backing up the data yourself.
7. Electronic communication used wisely broadens our world and improves our communication. However, **for private, sensitive, or confidential information, e-mail should be used carefully and sparingly,** as misspelled e-mail addresses and network problems often result in e-mail being directed to network administrators for evaluation, or worse, being made public. Security experts consider e-mail messages no more secure than a postcard.

\*Username is a permanent code assigned by Information Systems to EMU associated individuals to provide secure access to various EMU technology systems, including the EMU computer network. It is typed into a login prompt on a computer along with a password to gain access to the network. It is usually comprised of part of the person's name or initials. The username and password are used to access the EMU e-mail system. An EMU e-mail alias name may be selected to provide an easily recognizable name for individual EMU e-mail addresses.

Reviewed by ISPC  
April 17, 2008

Approved by Cabinet  
May 21, 2001