

NMI Computer & Network Usage and Security Policy

1. Executive Summary

The purpose of this policy is to outline employee, student, employee family, and visitor behavior requirements for the protection of Northland Mission, Inc. (NMI) information technology resources. Access to networks and computer systems owned or operated by NMI is a privilege, not a right, and implies user responsibilities. Such access is subject to NMI policies, standards, and procedures as well as federal, state, and local laws.

2. Scope

This policy addresses proper use of all NMI computing and network resources, including proper management of those resources. All business agreements and contracts must comply with this policy. Other policies, standards, procedures, and safeguards documents may augment restrictions for the sake of security but may not reduce the minimum requirements established in this policy.

3. User Responsibilities

The responsibilities below extend to every NMI student and employee. The responsibilities also apply to employee families or visitors that utilize NMI technology resources.

3.1. Privacy

In accordance with NMI's responsibility to educate and discipline, users should have no expectation of privacy when using NMI computing resources. All computer and network activity logs are subject to periodic review, and files are subject to inspection at any time.

3.2. Intellectual works and copyrights

3.2.1. Copyright Infringement

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

3.2.2. Civil and Criminal Penalties

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than \$750 and not more than \$30,000 per work infringed. For "willful" infringement, a court may award up to \$150,000 per work infringed. A court can, at its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense.

3.2.3. Legal Downloading Alternatives

Respecting copyrights is also possible through the use of legal downloading alternatives. EDUCAUSE compiles a list of legal sources for online content, which may be reviewed at their website:

<http://www.educause.edu/legalcontent>

3.3. Data confidentiality and integrity

Users are responsible for upholding the confidentiality and integrity of data. Users are prohibited from inspecting, copying, altering, or destroying anyone else's files without proper authorization.

3.4. Responsible use of resources

Users must ensure that NMI computer systems and network resources are used for scholarly or NMI business purposes only. Incidental personal use is permissible if the use meets the following standards:

- Does not create a security or legal risk for Northland Mission, Inc.
- Does not interfere with worker productivity
- Does not consume more than a trivial amount of resources that could otherwise be used for scholarly or business purposes

- Does not require the installation of any software or hardware unrelated to business or scholarly use
- Does not constitute inappropriate behavior for Northland's work environment

Messaging and publication technologies (e.g. e-mail, instant messaging, newsgroups, daily journals, blogs) carry a common set of responsibilities, including appropriate content, distribution, and security. Messages should only be distributed to those requiring the information. Virus alerts, chain letters, prayer requests, and items for sale are unacceptable uses of mass messaging technologies and may only be sent by authorized NMI employees.

3.5. Networking implementation and management

The Technology Department is responsible for planning, implementing, and managing the NMI network, including wireless connections. The following technologies cannot be implemented without prior written approval: routers, switches, hubs, wireless access points, and other networking technologies.

3.6. Use of personally-owned systems

Authorized users have a responsibility to ensure the security and integrity of personally-owned (or managed) systems as well as Institute Data accessed through such systems. Any connection of a personally owned computer to the NMI network, excluding "NMI" (public) or "NMI2" (apartment/duplex) wireless connections, requires written approval by the director of Technology. Users may consult with the Technology Department on security and system administration issues and responsibilities, although the Technology Department bears no responsibility for maintaining personally-owned systems.

3.7. Security

3.7.1. Sharing of access

Authorized users are individually responsible and accountable for any use of their account and password. Sharing of passwords is only permissible when minor children of NMI employees are granted an account, and the password should only be shared with the minor's parents.

3.7.2. Permitting unauthorized access

Authorized users may not run or otherwise configure software or hardware to intentionally allow access to any NMI information resources by unauthorized users.

3.7.3. Protection of information

Authorized users may have access to privileged information that must be protected. In receiving access to this information, authorized users accept responsibility to protect the information accessed and used with their account.

3.8. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This does not preclude the use of security tools by appropriately authorized personnel. While the following list provides examples of disallowed practices, it is not a comprehensive list and is only intended to provide examples:

- Password decrypting or cracking tools
- Denial of service (DoS) or distributed denial of service (DDoS)
- Harmful activities (e.g., IP spoofing, port scanning, disrupting services, damaging files, or intentional destruction of or damage to equipment, software, or data)
- Unauthorized access (e.g., using another's account, using a special purpose account, or escalating their own privileges)
- Unauthorized monitoring (e.g., keyboard logging or network packet capturing)

3.9. Lab Policies

3.9.1. Atmosphere

NMI computer labs are to maintain a library-like atmosphere at all times. Verbal communication in the labs should be kept to a minimum, except as directed by faculty during a regularly scheduled class meeting time.

3.9.2. Food and Drink

Food and drink is not permitted within the lab rooms. This includes, but is not limited to, coffee, water, candy, and gum.

3.9.3. Damage

Users will be held responsible for damages caused by neglect or intentional misuse of equipment.

4. Policy Modifications

This policy may be changed by directive of the director of Technology. All exceptions to this policy must be approved by the director of Technology prior to the exception occurring.

5. Violations

Each possible violation of the NMI Computer & Network Usage and Security Policy is reviewed by the director of Technology. Penalties for violations may include, but are not limited to, verbal/written warning, loss of internet/network privileges, revocation of NMI computer account, and/or termination of employment. Other penalties may be assessed by other entities of NMI in addition to these penalties.