Title: Data Security Policy
Approved Date: 1/28/2011
Revision Date: 1/28/2011
Description: Provide a framework for university data security

SCOPE

This policy statement covers all systems and devices of any kind that connect to the Olivet Nazarene University network regardless of device ownership. The Olivet Nazarene University network is defined to be any ONU network infrastructure (e.g. wired, wireless, residential, administrative, faculty/staff) on which systems can connect to each other or to the Internet.

Goals of this Policy

The goals of this network security policy are:

- Protect Olivet Nazarene University's computing infrastructure from abuse, unauthorized access, and inappropriate content.
- Set standards for security breach management and reporting.
- Provide a framework for university data integrity during traditional usage and times of transition.
- Maintain Olivet Nazarene University's legal and ethical responsibilities in direct relation to any networks and computers and their connectivity to worldwide resources.

Policy Statement

This policy is designed to incorporate Olivet Nazarene University standards while maintaining the highest level of data integrity, user computing experience, and security incident protection to highlight and maintain the university mission of "Education with a Christian Purpose".

RESOURCE PROVISION AND USER SCOPE

The overall responsibility of network security at Olivet Nazarene University does not fall to just one person or group. All users are a part of the end result of data integrity and security. This policy is created in collaboration with areas of the Olivet Nazarene University community such as Information Technology, Student Development, Campus Life, and Academic Support.

All network users shall abide by this policy and the Olivet Nazarene University Acceptable Use Policy or potentially risk loss of computing privileges and referral to the appropriate campus departments/authorities.

CAMPUS NETWORK OPERATIONAL FUNCTIONS AND RESPONSIBILITIES

1. Network Management Team

To accomplish the goals of this policy, the Olivet Nazarene University network *management team will perform the following functions.*

• Monitor network traffic, as necessary and appropriate, for the detection of network infrastructure problems, intrusions (internal and external based), and network policy violations.

  • If a security problem is identified, the network management team will seek the cooperation of the appropriate administrators or staff for the systems and networks involved in order to mitigate such issues. If necessary, the network management team will act unilaterally to isolate and contain the problem by isolating systems and their services from the network infrastructure, and promptly notify the appropriate resources when this is done.

• Monitor and maintain campus infrastructure to allow compliance with university policies against pornographic and mature content via network connections. Traffic detected that violate these policies will be submitted to the office of Student Development.

• Plan, implement, and review the results of network-based security scans of the systems and devices on university networks in order to detect vulnerabilities or compromised hosts.

• If detected security vulnerabilities, deemed to be a significant risk to others, are not addressed in a timely manner, the network management team may take steps to disable network access to those systems and/or devices until the problems have been rectified.

• Prepare summary reports of network security activities on a quarterly basis.

• Provide security assistance and incident prevention advice to system administrators.

• Coordinate all Olivet Nazarene University network security efforts and act as the primary administrative contact for all related activities. To ensure that this coordination is effective, security compromises should be reported to the network management team via e-mail at it@olivet.edu or telephone 815-928-5302.

• Cooperate with Olivet Nazarene University departments (e.g., Student Development, Public Safety, Human Resources), state, and federal investigations into any alleged computer or network security incidents.

• Cooperate in the identification and prosecution of activities contrary to university policies and the law. Actions will be taken in accordance with relevant university policies, codes, and procedures with, as appropriate, the involvement of the Public Safety and/or other law enforcement agencies.

• Abide by a Code of Conduct for IT staff and administration.

2. System Administrators
System Administrators will perform the functions listed below:
• Follow procedures and policies to protect the systems and services for which they are responsible.

• Employ recommended practices and guidelines where appropriate and practical.

• Cooperate with the network management team in addressing security problems identified by network monitoring.

• Address security vulnerabilities identified by network management team scans deemed to be a significant risk to others.

• Report computer/server security compromises to the network management team for assistance in tracking and containing intrusions.

3. Network Users
Network users are required to follow the mandates listed below.

Comply with the intended use of any system or service at Olivet Nazarene University.

All systems and services provided by Olivet Nazarene University are used for academic and campus business priorities, with non-academic use being a secondary priority.

Prohibited activities include, but are not limited to, the following misuses:

- Circumvention of Olivet Nazarene University technical, administrative, or access controls

- Any activity which disrupts usage, such as causing a device failure or exceeding normal usage parameters on a system or service

- Subversion of a system or service for inappropriate or illegal use

Ensure the proper and ethical use of Olivet Nazarene University technology resources.
Usage of any Olivet Nazarene University system or service for unethical or illegal activities is prohibited. Harassment of any medium, violation of privacy, inappropriate computer use, and digital attacks using Olivet Nazarene University technology are examples of activities that are forbidden.
Respect Olivet Nazarene University property.
Users must continually respect Olivet Nazarene University property. The university retains the right at all times to review and audit any and all information sent, received, or maintained on any university owned electronic communication devices as well as

any system or service within the Olivet Nazarene University network to enforce the policy.