SOUTHERN ADVENTIST UNIVERSITY

Network Usage Policy

Revised February 2010

Introduction

The Southern Adventist University network facilitates communication among the members of the university community, provides a resource for gathering information, and supports the university learning environment.

Scope and Purpose of this Policy

Southern's private network is available to authorized users. Network use is governed by this policy. This policy documents standards for appropriate and fair use of limited networking resources, protects user security and privacy, and assures university compliance with local, state, and federal laws.

Exceptions to this policy may be granted by petition to the Administrative Council if any portion of this policy is presumed a hindrance to an academic purpose.

In this document, the term *users* refers to anyone using Southern's network.

Appropriate Use

1. Users are expected to follow the Golden Rule and cooperate with system administrators.
2. User activity on the network must not prevent or inhibit others from accessing network resources or the Internet.
3. Users must not use or provide tools that damage files or computers, compromise network security, or disable accounts.
4. Users must not send obscene, defamatory, or threatening messages or in any way harass others. Information transmitted or published is to be representative of a Christian university.
5. Users must not violate university policy nor local, state, or federal laws.
6. Users must not impersonate another individual or misrepresent authorization to act on behalf of another individual or the university. Messages stored on or transmitted through the university network must correctly identify the sender. Users must not modify the original attribution of email messages or postings and must not send anonymous messages.
7. Users must not distribute copyrighted material without written consent of the copyright holder. The copyright law makes provision for fair use of short excerpts from copyrighted materials. When using such excerpts the source must be credited. Unless otherwise

indicated by the author, users should assume that any material not created by themselves is copyrighted.

8. Users are responsible for all use made of their accounts. Account owners are to prevent unauthorized use and to report suspected intrusions or other inappropriate activity to Information Systems.
9. Users must not attempt to undermine the security or integrity of the university network and must not attempt to gain unauthorized access. Users must not use any computer program or device to intercept or decode passwords or similar access-control information. Suspected security breaches or vulnerabilities should be reported immediately to Information Systems.

Privacy

1. User privacy is important to the university and is protected to the extent that is technically feasible and allowed by law. The university does not routinely monitor personal communication or information without probable cause. Messages sent and received electronically are accessible to administrators through normal maintenance activities, and to the public through public record laws, subpoenas, decoding, interception, or other means. Because of this, the university cannot guarantee complete privacy of electronic communications.
2. Network administrators endeavor to maintain the integrity and proper functioning of the systems for the benefit of all users. In connection with this responsibility, designated administrators may need to access or monitor parts of the system. All administrators are to respect the privacy of personal communications encountered on the system. However, if administrators, while involved in routine duties, encounter information that indicates that a crime or a breach of this policy may have been committed or is about to be committed, they are required to report the existence and source of this information to the proper university authorities.
3. Searching and monitoring of personal electronic communications may be authorized by the university president or an employee he appoints. Authorization, including delegation if applicable, must be in writing and must specify the information or communications to be examined.

Security

While it is impossible to make the network totally secure, our goal is to provide a reasonably secure environment for personal and institutional computing and communication.

Network

1. The network is divided into several security zones separating the Internet and university internal networks. In order to maintain network security, computers may not be connected to more than one of these zones at a time.
2. Internet Protocol (IP) addresses used on the university network are university property, are assigned by Information Systems, and may only be used by permission. Every computer connected to the network must use a university supplied IP address.
3. Any device physically connected to the university network must be registered with Information Systems.

Servers

1. Servers are computers connected to the university network that provide services or storage to multiple users.
2. Only persons designated by the executive director of Information Systems have physical access or administrative password access to centrally administered servers or equipment. Keys to these facilities are not issued to any individual without the permission of the executive director.
3. All servers connected to the university network must be registered as such with Information Systems. System administrators must take steps to ensure that the servers are reasonably secure. Information Systems performs periodic security audits of all servers connected to the university network.
4. A university server found to be a security threat will be reported to the administrator of that server as well as to Information Systems. If necessary, the server will be disconnected until the problem is fixed.

Workstations

1. A workstation is a computer connected to one of the university networks and is designated for use by a single person.
2. Workstations connected to a university network must not be configured to allow access to that network from any other network or from off-campus. Users requiring access to secure resources while away from their workstation may request a virtual private network (VPN) account from Information Systems.

General-use Computers

1. A general-use computer is any computer routinely used by more than a single designated user.
2. General-use computers must comply with the policies for workstations.

3. Information Systems must approve and oversee the configuration and installation of any general-use computer connected to the network.
4. General-use computers are not given access to secure network zones.

Blocking

1. Blocking-software is maintained to protect users from encounters with inappropriate materials. However, this should not be construed as an endorsement of any site which is not blocked.
2. Users may report sites which they feel should not be restricted to blocking@southern.edu.

User responsibility

1. While Information Systems takes steps to make the network secure, security is ultimately the responsibility of the user.
2. Users are not to share passwords with anyone. No one, including Information Systems employees, is authorized to ask for a password. We strongly suggest that all users take time to learn passwords in order to avoid writing them down.
3. Users should not remain logged in to university systems when away from their desks for an extended period of time.

Sanctions

1. **First Minor Incident.** When a user appears to have violated the Network Usage Policy in a manner that is deemed minor by Information Systems and the user has not been implicated in prior incidents, he/she is furnished a copy of the Network Usage Policy and is asked to sign an "agreement to conform to policy" statement.
2. **Repeated and/or Major Violations.** Repeated or major violations are referred to Student Services (for students) or the appropriate vice president or the president (for employees) for disciplinary action.
3. Disciplinary actions for violations may include, but are not limited to, loss of network access, dismissal, and legal action. When violations may constitute criminal offenses, the university reports the activity to the appropriate authorities.
4. The processes for appealing actions are outlined for students and employees in the respective handbooks.