Southern Adventist University

Acceptable Use Policy

Version 3.1 - Revised December 2016

Introduction

The Southern Adventist University network facilitates communication for the members of the university community or the persons associated with the university, 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 networking resources, protects user security and privacy, and assures university compliance with local, state, and federal laws.

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

Appropriate Use

1. Users are expected to 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 policies, nor local, state, or federal laws.
6. Users must not misrepresent another user's identity.
7. Users must not distribute copyrighted material without written consent of the copyright holder. Unless otherwise indicated by the author, users should assume that any material not created by themselves is copyrighted.
8. 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 Technology.

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 systems maintain a certain level of logging of network activities. Messages sent and received electronically are accessible to administrators through normal maintenance activities, and to external agencies through laws, subpoenas, or other authorized 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. 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 computing resources and network activities may be authorized by the university administration as outlined in the *Southern Information Security Policy*. Authorization, including delegation if applicable, must be in writing, and must specify the information or communications to be examined.

Security

Our goal is to provide a secure environment for personal and institutional computing and communication. The security principles are outlined in *Southern Information Security Policy*. The following are a few practical applications of those principles:

Network

1. The network is divided into several security zones separating the Internet and university internal networks.
2. Any device connected to the restricted security zones must be registered with Information Technology
3. Internet Protocol (IP) addresses used on the university network are university property, are assigned by Information Technology, and may only be used with permission. Every computer connected to the network must use a university supplied IP address.

Servers

1. Servers are computers connected to the university network that provide services or storage to multiple users.
2. Only persons designated by Information Technology have physical access or administrative password access to centrally administered servers or equipment. Access to these facilities are not issued to any individual without the permission of Information Technology.
3. All servers connected to the university network must be registered as such with Information Technology. System administrators must take steps to ensure that the servers are secure. Information Technology 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 Technology. 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.
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 without proper authorization from Information Technology. Users requiring access to secure

resources while away from their workstation may request a virtual private network (VPN) account from Information Technology.

General-use Computers

1. A general-use computer is any device designated to work in a lab or kiosk environment.
2. General-use computers must comply with the policies for workstations.
3. Information Technology 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 that is not blocked.
2. Users may request an exception to the blocking policy by emailing to blocking@southern.edu.

User responsibility

1. While Information Technology takes steps to make the network secure, the user plays a very important role in maintaining security.
2. Users are not permitted to share passwords with anyone. No one, including Information Technology employees, is authorized to ask for a password. It is strongly suggested that all users protect their credentials.
3. Users are not allowed to share their access to university systems without authorization from Information Technology.
4. Users should either log out or lock their screens when away from their computers for an extended period of time.
5. Users are to report suspected intrusions or other inappropriate activity to Information Technology.

Violations

1. **First Incident.** When a user appears to have violated this policy and the user has not been implicated in prior incidents, he/she is furnished a copy of this policy and is asked to sign an "agreement to conform to policy" statement.
2. **Repeated Violations.** Repeated or what Information Technology deems as a major violation, is going to be referred to the respective vice president 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.