Employee Information Use and Security Policy

Pensacola Christian College and Affiliates

1 Purpose

The purpose of this policy is to engage each employee in the protection from unauthorized access, loss, or damage through the use of ministry information and communication technology. Ministry information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes. Standards and procedures related to this general policy will be developed and published separately.

2 Policy

Pensacola Christian College or any of its affiliates provides voicemail, e-mail, internet, and other computer or telecommunications systems that are intended for business or academic use. Communications transmitted through these systems should have an approved business or educational purpose. All software and equipment used on or in connection with ministry computers or systems must be purchased through the corporate purchasing system and installed by authorized employees.

Ministry-wide standards of conduct and the law prohibit the unauthorized duplication of copyrighted computer software. Employees will neither engage in nor tolerate the making or using of unauthorized software copies under any circumstances. The institution will provide legally acquired software to meet all legitimate business needs in a timely fashion and in sufficient quantities for all our computers. Employees will comply with all license or purchase terms regulating the use of any software we acquire or use. The ministry will enforce strong internal controls to prevent the making or using of unauthorized software copies, including effective measures to verify compliance with these standards.

Employees may not duplicate or download any software or other materials (such as documents, photos, music, and video files) that are copyrighted, patented, trademarked, or otherwise identified as intellectual property without express permission from the owner of the material and the area supervisor.

Authorized individuals may access electronic communications systems and review communications within the systems, without advance notice to users of the system, whenever staff deems it appropriate to do so. The reasons for such access include but are not limited to: maintaining the system; preventing or investigating allegations of system abuse or misuse; assuring compliance with software copyright laws; complying with legal and regulatory requests for information; ensuring that the ministry's operations continue appropriately during an employee's absence; violation of a policy and any other purpose deemed appropriate.

Employees may not use ministry communication equipment for the following actions:

- Forging messages or creating and sending anonymous messages.
- Attempting to read, delete, copy, or modify another employee's messages.
- Communicating using vulgar, harassing, obscene, or threatening content.
- Sending "junk" or "chain" messages.
- Accessing personal social media platforms or networks.
- Storing personal files, programs, games, etc., on ministry computers or servers.
- Sending, receiving, requesting, or forwarding offensive or pornographic material.
- Attempting to sabotage equipment by sending viruses.
- Attempting to update or install software on ministry computers or systems.
- Attempting to repair, install, or replace any ministry computer system, component, accessory, or peripheral device.
- Remotely accessing ministry systems without prior authorization.
- Attempting to secure a higher level of access privilege on network systems.
- Intentionally attempting to "crash" network systems or programs.
- Decrypting and/or capturing system or user passwords.
- Performing any other action that may be illegal, unethical, or irresponsible.

No one may use electronic communications in a manner that may be construed by others as sexual, racial, or ethnic harassment or discrimination protected by law.

2.1 Computer & Data Usage

It is the employee's responsibility to do their best to protect information assets and comply with related policies and procedures. The following outlines what is entailed in creating and maintaining appropriate password protection as well as outlining what is expected when leaving your computer unattended. The ministry requires the use of strong passwords and Multi-factor Authentication (MFA) among other security actions for accessing computer systems. This requirement better protects institutional systems and data.

2.1.1 Passwords

Employees will not share their password with anyone for any reason. Passwords should not be shared with anyone, including any students, faculty, or staff. In situations where someone requires access to another individual's protected resources, delegation of permission options should be explored. For example, Microsoft Exchange calendar will allow a user to delegate control of his or her calendar to another user without sharing any passwords. This type of solution is encouraged. Passwords should not be shared even for the purpose of computer repair. An alternative to doing this is to create a new account with an appropriate level of access for the IT Help Desk repair person.

2.1.2 Data Handling

Employees will handle ministry data with extreme care. This policy refers to the following: internal, third-party, and any other data entrusted to the institution's care.

2.1.3 Malicious Software

Employees may not introduce malicious code such as viruses, worms, Trojan horses, password cracking or login spoofing programs on any college computer or network nor compromise the security of any system. This includes non-technical activities such as misrepresenting one's identity or impersonating another user.

2.1.4 E-mail

Each employee is assigned a ministry e-mail address. Employees need to check their ministry e-mail and the Employee Services website daily while at work for important announcements and updated campus information. Hourly employees are not required to read or respond to e-mail using their ministry-issued e-mail address unless at work, using ministry-provided computers.

Almost all cybersecurity attacks begin with a phishing e-mail to an unsuspecting victim, so employees must be alert to protect the ministry. Phishing attacks can trick employees into opening malicious attachments, clicking on links, or sharing sensitive data such as personally identifiable information, login credentials, or financial details. Employees will be trained on how to identify & report suspected phishing e-mails, but regardless employees should only open e-mail attachments when expecting them and know what they contain even when the e-mail is from someone the employee knows.

2.2 Security and Compliance Awareness Training

Each employee will participate in security and compliance awareness training and fully understand the requirements contained within the company's information security policies. The training will include evaluation questions upon completion to test users' understanding of the material. In addition, all users shall be trained on how to identify, report, and prevent potential security incidents.

Security and compliance awareness training is an ongoing activity and shall be delivered using a multi-modal approach. All users must complete security and compliance awareness training based upon their role prior to accessing any ministry information assets, and each year thereafter. Approved security reminders or notifications will be distributed by Information Security and shall keep users informed of current information security threats, such as new malware or phishing scams.

Security and compliance awareness training shall cover various topics, such as data security, security incident response reporting, social engineering, and the protection of ministry data, where applicable. Role-specific security training shall be provided when necessary.