USW Computer & Network Responsible Use and Best Practices

Purpose:
In an effort to protect the security of University of the Southwest, the University mission, the University network, and any data contained therein, the University has adopted the following guidelines for responsible use of USW computers and network.

Scope
This policy applies to all users of the USW network.
Use of the network constitutes consent to monitoring and disclosure of monitoring. Users have no reasonable expectation of privacy on the network. The network and its data are property of University of the Southwest.

Instructions
Please read these guidelines, provide the information requested, sign where indicated, and return the signed original to the Personnel Services Coordinator for placement in personnel file.

Failure to accept and abide by these guidelines may result in the revocation and/or forfeiture of USW network privileges including Internet and email access.

Guidelines for Network Use

Users may NOT:

- Share passwords.
- Maliciously log into or access user accounts not specifically assigned to them.
- Access objectionable sites (e.g. gaming, pornographic sites, etc.) containing subject matter or graphics contrary to the University mission.
- Access, or attempt to access, network resources without obtaining proper access permissions from a system administrator.
- Intentionally abuse or damage USW computer hardware or software.
- Unlawfully access, or attempt to access, proprietary networks outside of the USW domain.
- Publish information for public access containing profanity or other language, subject matter, and/or graphics that are contrary to the University mission.
- Allow unauthorized users (including individuals whose authorizations have been revoked) to access the University network.
- Install any software (licensed, unlicensed, and/or personal) on a computer that belongs to University of the Southwest without the prior consent and authorization of the network administrator.
- Transfer or loan accounts to another user.

Users SHOULD:

- Be responsible for the assigned account.

- When leaving workstations unattended for an extended time, the account should be locked or logged out.
- Change passwords often. Use strong passwords containing both upper and lower case letters, numbers, and other characters.
- Be responsible for ensuring that virus definition files are up to date.
- Notify Computer. Services if anti-virus software is malfunctioning, missing, or out of date.

Employee Communications Acknowledgment Form

I understand that all electronic and telephonic communication systems and all information transmitted by, received from, or stored in these systems are the property of the University. I also understand that these systems are to be used solely for job-related purposes and not for personal purposes, and that I have no expectation of privacy in connection with the use of this equipment or with the transmission, receipt, or storage of information in this equipment.

I agree not to use a code, access a file, or retrieve any stored communication unless authorized. I acknowledge and consent to the University monitoring my use of this equipment at any time at its discretion. Such monitoring may include printing and reading all e-mail entering, leaving, or stored in these systems.

_____
Name of Employee (Please print)

_____
Employee's Signature

_____
Date

_____
Melody Arnold, Management Witness (Please print)

_____
Signature of Witness