IT SECURITY

POLICY

The Sherman Information Technology department shall be authorized to evaluate the seriousness and immediacy of any threat to information resources and to take action to mitigate that threat, including disconnection of information resources. Sherman Information Technology department shall evaluate the impact of disrupting service when devising an action plan that mitigates any threat.

This policy is an important part of Sherman College's efforts to create a secure environment in which to carry out the mission of Sherman College. Security requires the participation of each constituent who comes into contact with Sherman College information or systems.

This policy shall be supported by standards documents that set forth the detailed requirements that apply to individuals, devices, and systems.

Responsibilities:

Sherman Information Technology Department
The department shall investigate Security Events and respond to Security Incidents in accordance with established procedures.

The department shall cultivate awareness of security issues and vulnerabilities within Sherman College. All Sherman faculty and staff are required to complete annual security awareness training.

The department shall assist the executive vice president and vice president for finance and campus operations to assess risks to Sherman College systems.

The department will determine the security specifications and standards for devices connected to the Sherman College data network. Devices connected to Sherman College network will be reviewed on a regular basis for the latest operating system and application security patches applicable to that device as well as the latest anti-virus software. Devices not compliant with Sherman College Information Technology standards may be disconnected from the Sherman College network.

Authorized Users of Information Technology
All authorized users share in responsibility for information security by following all applicable security policies and procedures.

Users must report any discovered unauthorized access attempts or other improper usage of Sherman information resources. Report observed or suspected violations to the IT Help Desk at ext. 228 or help@sherman.edu.

IT SECURITY

Exclusions or Special Circumstances
Exceptions to this Policy shall only be allowed if previously approved by the director of information technology and this approval is documented and verified.

Consequences
Use of College electronic information resources contrary to this policy or applicable federal, state or local law is prohibited and may subject the user to disciplinary action including, but not limited to, suspension of the user's access to the electronic information resources. Users also should be aware of other possible consequences under college policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.

Recourse/Appeals
If a department or individual feels that actions taken under this policy have been inappropriate, a review of the decision may be requested. The review will be conducted by the provost and executive vice president. If, after the review, there is still a disagreement with the decision, appeals should be directed through the existing procedures established for employees and students.