Subject: Unattended Computer Logoff/Lock Policy

Policy #: Information Security-P#9.3.2

Regulation: HIPAA, GLB, State of Oklahoma

Effective: 11/16/05

Purpose:
To prevent unauthorized user access to unattended computing devices and to comply with state and federal regulations that require safeguards for computing devices that contains or provides access to sensitive information.

Policy:

Manual logoff or lock - When leaving a computer, server, personal digital assistant, or other computing device unattended, workforce members must manually logoff or lock the device to prevent unauthorized access to University systems or information.

Automated logoff or lock - All computing devices that contain or access sensitive information must be secured with either a password-protected screen saver or automatic logoff that will take effect after no more than 10 minutes of inactivity.

Documentation:
All data collected and/or used as part of the Risk Management Process and related procedures will be formally documented and securely maintained.

Scope/Applicability:
This policy is applicable to all workforce members who use computing devices in conjunction with any OU computer, data, or network.

Regulatory Reference:
State of Oklahoma Information Security Policies, Section 7.4: Access Control
FERPA: 34 CFR Part 99 [Family Educational Rights and Privacy Act]
GLB: 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act")]
USA Patriot Act

Definitions:
See the Information Security Policy Definitions document for definitions

Responsible Department:
Information Technology will maintain computing device policies and standards for safe computing.

Enforcement/Audit:
The university’s Internal Auditing department is responsible for monitoring and enforcement of this policy.

Related Policies:
Access Control, Workstation Safeguards, Emergency Access Procedure

Renewal/Review:
This policy is to be reviewed and updated as needed by IT Information Security Services.