UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Computer Lock/Logoff Policy	**Coverage:** OUHSC
Policy #: Information Security-P#9.3.2	**Version:** 1.1.2
Regulation: HIPAA, GLB, PCI DSS, State of Oklahoma	**Approved:** 11/16/05
Effective: 11/16/05	**Revised/Reviewed:** 11/13/2014

Purpose:	To prevent unauthorized user access to unattended computing devices and to comply with state and federal regulations.
Policy:	**Manual lock or logoff** - When leaving a computer, server, portable computing device (PCD), or other computing device unattended, workforce members must manually lock or logoff the device to prevent unauthorized access to University systems or information. **Automated lock or logoff** - All computing devices must be secured with either a password-protected screen saver or automatic logoff that will take effect after no more than 15 minutes of inactivity.
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:	HIPAA Security rule 45 CFR 164.312(a)(2)(iii) Implementation Specification for Access Control Standard, 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 has enforcement authority and will periodically assess business unit compliance.
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.
Procedures:	Each department that maintains information systems is responsible for developing procedures to comply with this policy.