UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information Security Login Banner Policy	**Coverage:** OUHSC
Policy #: Information Security-P#	**Version:** 2.0
Regulation: HIPAA, GLB, State of Oklahoma	**Approved:** 02/14/01
Effective: 02/14/01	**Revised/Reviewed:** 11/18/2014

Purpose:	For legal reasons, in many jurisdictions, it is wise to put all users on notice that the involved system is to be used only for authorized purposes. In the event of a prosecution against those who entered a system unlawfully, one of the most successful defense positions is that there was no notice saying they could not enter. Recent court cases have highlighted the need for organizations to put unauthorized users on notice that their systems are off limits. As a result, a system login banner -- displayed each time a user logs-in -- should provide the electronic equivalent of a no-trespassing sign. A policy such as this is desirable for all multi-user computers, especially those systems with external network connections (dial-up lines, Internet firewalls, etc.). The same type of banner can be used for data communication networks, not just computers.
Policy:	Security Notice In System Login Banner: Every login process for multi-user computers must include a special notice. This notice must state: (1) the system is to be used only by authorized users, and (2) by continuing to use the system, the user represents that he/she is an authorized user. Network Login Banner: The following banner must be displayed when users connect to OUHSC computer networks: "This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity or policy violation, system personnel may provide the evidence of such monitoring to law enforcement or other officials."
Scope/Applicability:	This policy is applicable to all University IT resources.
Regulatory Reference:	45 CFR 164.308(a)(1)(i) [HIPAA Security rule: administrative: security management process] 34 CFR Part 99 [Family Educational Rights and Privacy Act] 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (‘‘GLB Act’’) PCI DSS (Payment Card Industry Data Security Standard) State of Oklahoma Information Security, Policy Procedures Guidelines Electronic Communications Privacy Act of 1986
Definitions:	See the Information Security Policy Definitions document for definitions
Enforcement/Audit:	The University’s Internal Auditing department has enforcement authority and will periodically assess business unit compliance.
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.