UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Policy

Information System Compliance Sanctions Policy

Purpose:

The University will impose appropriate sanctions for non-compliance with its Information System policies, procedures, and standards.

This policy reflects the University's commitment to identify and implement security controls which will keep risks to information system resources at reasonable and appropriate levels.

Policy:

The University shall impose appropriate sanctions for non-compliance with its Information System policies and/or regulations.

Employees: A violation of Information Systems policies is also considered a violation of the University's Compliance and Quality Improvement Program. Therefore, these sanctions will apply equally for violations of the University's Information System policies. The sanctions imposed for a violation of Information System policies will depend on the severity of the violation and will be imposed in accordance with the University's Positive Discipline Policy, the Faculty Handbook or other applicable document.

Students: Students who violate the University's Information System policies will be subject to sanctions which may include but are not limited to fines, suspension or expulsion. The type of sanction imposed will depend on the severity of the violation. Sanctions will be imposed on students in accordance with applicable University policies and procedures.

Volunteers: Volunteers who violate the University's Information System policies will be subject to sanctions which may include but are not limited to access removal or modification, re-assignment, or revocation of volunteer status.

Business Associates: A pattern of activity or practice that constitutes a breach or violation of the obligations under contract will result in the University taking the following actions, as warranted: cure the breach or end the violation, terminate the contract, or report the problem to applicable government agency.

For the protection of the University and its network/infrastructure, violations may result in restricted or revoked network access.

When sanctions are imposed for the inappropriate use and/or disclosure of "sensitive" data, the sanctions should be commensurate with the nature and severity of the violation, and the following must be carefully considered:

A. Carelessness or negligence
B. Curiosity or concern
C. Desire for personal gain or malice

Scope:

This policy is applicable to all faculty, staff, students, volunteers, and business associates of OUHSC and OU Health Care Components.

Regulatory Reference:	• HIPAA 45 CFR 164.308(a)(1)(ii)(B), 16 CFR Part 314 Standards for Safeguarding Customer Information • [section 501(b) of the Gramm-Leach-Bliley Act (‘‘G–L–B Act’’), Standards for Safeguarding Customer Information, • State of Oklahoma Information Security, Policy Procedures Guidelines, • Payment Card Industry Data Security Standard (PCI DSS)
Definitions:	For additional Information Technology definitions, see Information Technology Policy Definitions Document at http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf
Responsible Department:	Human Resources, Office of Compliance, Legal Counsel, Student Affairs
Policy Authority/ Enforcement:	This policy is authorized and approved by the OUHSC Dean’s Council and Senior Vice President and Provost. Internal Audit may periodically assess Business Unit compliance with this policy and may report violations to the Board of Regents.

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
04/11/2007	2.0	Campus IT	Baseline Version

Table 2 Approval History

Version	Approval Date	Approved by:	Title:
2.0	04/11/2007	Dean’s Council	

Table 3 Review History

Version	Review Date	Reviewed by:	Title:
2.0	11/19/2014	Campus IT	