Acceptable Use of Information Systems Policy

1. Purpose

The Information Systems (IS) at University of Oklahoma Health Sciences Center support the educational, instructional, research, administrative and healthcare activities of the University. University IS consist of the computer devices, data, applications, and the supporting network infrastructure. As a user of these services and facilities, users have access to valuable University information, to regulated data, and to internal and external networks. Users have an obligation to use IS in a responsible, ethical, and legal manner.

This policy establishes guidelines for acceptable use of IS. It includes examples of what you can do and cannot do, and what rights you have. All of these guidelines are based on the underlying principles:

- Information Systems are provided to support the essential mission of OUHSC.
- OUHSC policies, standards, state and federal law govern the use of IS.
- Users are expected to use IS with courtesy, respect and integrity.

2. Policy

Access to University of Oklahoma Health Sciences Center Information Systems is predicated on user compliance with certain responsibilities and obligations including University policies; procedures; regulatory requirements; and local, state, and federal laws.

By using University Information Systems, users agree to abide by and comply with the applicable policies, procedures, regulatory requirements, and laws. Users should understand that information created or stored on University computer resources, networks, and systems may be subject to disclosure in compliance with the Oklahoma Open Records Act, and user activity may be subject to review or monitoring in compliance with University policy or law.

In making use of Information System resources, users **MUST:**

- comply with all University policies, procedures, and regulatory requirements, and with federal, state, and local laws.
- comply with Portable Computing Device (PCD) Security policies, which include encrypting all PCDs used for University business.
- use computing resources only for authorized University administrative, academic, research, clinical, or other business use.
- protect user-IDs from unauthorized use. Users are responsible for all activities on their user-ID.
- access only information that is publicly available or to which they have been given authorized access.
- protect University data that they have been authorized to access.
- comply with all applicable copyright laws, licensing terms, patent laws, trademark laws, trade secret laws, and all contractual terms.
- be responsible in their use of shared resources. For example, users must refrain from monopolizing systems, overloading networks, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.
- ensure their access is compliant with the principles of intellectual property, ownership of data, system security mechanisms, and the right of others to be free from intimidation and harassment.
- be ethical and reflect academic integrity.

In making use of Information Systems resources, users **MUST NOT:**

- use another person's system, portable computing device, files, or data without express authorization.
- use another individual's user-ID or password.
- use computer programs to decode passwords or access control information without explicit permission from OU Legal Counsel or the OUHSC Chief Information Officer.
- attempt to circumvent or subvert system or network security.
- engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to or sharing of University data.
- use University Information Systems for commercial, private, personal, or political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
- harass or intimidate another person including, but not limited to, broadcasting unapproved, unsolicited messages; repeatedly sending unwanted or threatening mail; or using someone else's name or user-ID.
- waste computing resources or network resources including, but not limited to, intentionally placing a program in an endless loop, printing excessive amounts of paper, or sending chain letters or unapproved, unsolicited mass mailings.
- attempt to gain access to Information System resources or any data to which they have no legitimate access rights.
- take University data from Information Systems when leaving the University without approval.
- use unsecured cloud or other unapproved storage or use unencrypted PCDs for University business.
- engage in any other activity that does not comply with this or any other University policy and procedure, regulatory requirement, or applicable law.

3. Enforcement

Individuals using or accessing computer systems owned by the University do so subject to applicable laws and University policies.

The University considers any violation of these Acceptable Use Principles to be a serious offense and reserves the right to copy, monitor, and/or examine any files or information residing on University systems, networks, or computing resources allegedly related to unacceptable use, and to protect its systems and networks from events or behaviors that threaten or degrade operations. Violators are subject to disciplinary action including, but not limited to, discipline or sanctions outlined in the Student Code, Staff Handbook, Resident Handbook, college and department handbooks, or the Faculty Handbook, as applicable. Offenders also may be investigated and/or prosecuted under laws including, but not limited to, the Communications Act of 1934 (amended), Family Educational Rights and Privacy Act of 1974, Computer Fraud and Abuse Act of 1986, Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, Digital Millennium Copyright Act, Health Insurance Portability and Accountability Act, Electronic Communications Privacy Act, Health Information Technology for Economic and Clinical Health Act, Payment Card Industry Data Security Standard, Oklahoma Open Records Act, and State Ethics Rules.

The user assumes all risk of loss of materials or data or damage thereto. The University disclaims any responsibility for or warranties related to information and materials residing on non-University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of the University, its faculty, staff, or students. This Policy should not be construed as a limit on any individual's rights under the Constitution of the United States or the laws of Oklahoma.

4. Scope

This Policy is applicable to all OUHSC faculty, residents, fellows, staff, students, trainees, volunteers, business associates, and any individual or entity granted access to OUHSC Information Systems.

5. Regulatory References

- 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 (“GLB Act”)
- 16 CFR Part 314 Standards for Safeguarding Customer Information, GLB Act
- Payment Card Industry Data Security Standard (PCI DSS)

6. Authorization & Disciplinary Actions

This Policy is authorized and approved by the OUHSC Dean’s Council and Senior Vice President and Provost, and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University, including but not limited to Information Technology and the Office of Compliance, may periodically assess Business Unit compliance with any provisions of this Policy and may act on or report violations to the department and University administration and the Board of Regents.
Consequences for infractions include, but are not limited to:

- Verbal warnings
- Revocation of access privileges
- Disciplinary probation
- Suspension or termination from the University
- Criminal prosecution

The University reserves the right to protect its electronic IS from threats of immediate harm.

7. Revision, Approval and Review

7.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	01/01/2000	OUHSC IT	Baseline Version
3.1	04/11/2007	OUHSC IT	Minor language changes
3.2	08/20/2015	OUHSC IT	De-duplication by removing policy statement from purpose and minor language changes.
3.3	08/24/2015	OUHSC IT	Revised first policy statement to include any access to OU Information Systems
3.3	03/03/2016	OUHSC Legal Counsel and University HIPAA Privacy Official	See SharePoint document track changes for 03/03/2016
3.4	05/06/2016	OUHSC Legal Counsel and University HIPAA Privacy Official	See SharePoint document track changes for 05/06/2016
3.4	10/31/2016	OUHSC IT	See SharePoint document track changes for 10/2016
3.5	12/13/2016	OUHSC Information Security Review Board	See SharePoint document track changes for 12/13/2016
3.6	01/11/2017	OUHSC Dean's Council and Senior Vice President and Provost	See SharePoint document track changes for 01/26/2017

7.2 Approval History

Version	Date	Approved By
1.0	01/01/2000	OUHSC Dean's Council and Senior Vice President and Provost
3.1	04/11/2007	OUHSC Dean's Council and Senior Vice President and Provost
3.6	01/11/2017	OUHSC Dean's Council and Senior Vice President and Provost

7.3 Review History

Version	Review Date	Reviewed by:
3.1	11/12/2014	OUHSC IT
3.3	02/18/2016	OUHSC Information Security Services
3.4	10/28/2016	Legal Counsel
3.4	10/28/2016	OUHSC IT
3.5	12/13/2016	OUHSC Information Security Review Board