**UNIVERSITY OF OKLAHOMA**  
Information Technology  
Security Policies

<table>
<thead>
<tr>
<th><strong>Subject:</strong></th>
<th>Information System Acceptable Use Policy</th>
<th><strong>Coverage:</strong></th>
<th>OUHSC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy #:</strong></td>
<td>Information Security</td>
<td><strong>Version:</strong></td>
<td>3.1</td>
</tr>
<tr>
<td><strong>Regulation:</strong></td>
<td>HIPAA, GLBA, FERPA, PCI DSS, State of Oklahoma</td>
<td><strong>Approved:</strong></td>
<td>04/11/2007</td>
</tr>
<tr>
<td><strong>Effective:</strong></td>
<td>01/19/2000</td>
<td><strong>Revised/Reviewed:</strong></td>
<td>11/12/2014</td>
</tr>
</tbody>
</table>

**Policy Summary:**
By using the University information systems, you agree to abide by and comply with the applicable policies, procedures, regulatory requirements, and laws. Acceptable use must be ethical, reflect academic honesty, and show responsible use in the consumption of University shared resources.

**Purpose:**
The purpose of this policy is to protect the employees, students, and the confidentiality, integrity and availability of information systems. This policy outlines the acceptable and unacceptable use of information systems at the University of Oklahoma. Inappropriate use could expose our employees, students, and information systems and put them at risk.

**Policy:**
Access to information systems owned, operated, or provided by the University of Oklahoma is predicated on compliance with certain responsibilities and obligations and is granted subject to University policies, regulatory requirements, and local, state and federal laws.

By using the University information systems or computing resources, you agree to abide by and comply with the applicable policies, procedures, and laws. Acceptable use must be ethical, reflect academic honesty, and show responsible use in the consumption of shared resources. Acceptable use also demonstrates respect for intellectual property, ownership of data, system security mechanisms, and freedom from intimidation and harassment. Information created or stored on University computer resources, networks, and systems may be subject to the Oklahoma Open Records Act.

**In making acceptable use of information resources you MUST:**
- comply with all University policies, procedures, and federal, state, and local laws
- use resources only for authorized administrative, academic, research, clinical, or other University business
- protect your user-IDs from unauthorized use (you are responsible for all activities on your user-ID, or that originate from your system)
- access only information that is your own, that is publicly available, or to which you have been given authorized access
- comply with all copyright laws, licensing terms, patent laws, trademarks, trade secrets and all contractual terms
- be responsible in your use of shared resources (refrain from monopolizing systems, overloading networks, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources)

**In making acceptable use of information resources you 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
- 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 unsolicited mass mailings
• attempt to gain access to information system resources or any data to which he/she has no legitimate access rights
• engage in any other activity that does not comply with this policy, acceptable use presented above, University policies and procedures, or applicable law

The University considers any violation of acceptable use principles or guidelines 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, penalties outlined in the Student Code, Staff Handbook, or Faculty Handbook. Offenders also may be 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, Oklahoma Open Records Act, and state conflicts of interest laws.

Individuals using or accessing computer systems owned by the University do so subject to applicable laws and University policies. The user assumes all risk of loss of materials or data or damage thereto. The University disclaims any responsibility and/or warranties for 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. These guidelines should not be construed as a limit on any individual’s right under the Constitution of the United States or the laws of Oklahoma

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


Definitions: See the Information Security Policy Definitions document for definitions

Responsible Department: Human Resources, Office of Compliance, Legal Counsel, Student Affairs, Information Technology
<table>
<thead>
<tr>
<th>Policy Authority/Enforcement:</th>
<th>The University’s Internal Auditing department is responsible for monitoring and enforcing this policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Policies:</td>
<td>This policy stands alone in support of the Risk Management Policy.</td>
</tr>
<tr>
<td>Renewal/Review:</td>
<td>This policy is to be reviewed and updated as needed by IT Information Security Services.</td>
</tr>
</tbody>
</table>