**Subject:** Information System Control Review and Risk Assessment Policy  
**Coverage:** OUHSC

<table>
<thead>
<tr>
<th><strong>Policy #:</strong></th>
<th>Information Security-P#6.1.8</th>
<th><strong>Version:</strong> 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regulation:</strong></td>
<td>HIPAA, GLB, State of Oklahoma</td>
<td><strong>Approved:</strong> 04/11/07</td>
</tr>
<tr>
<td><strong>Effective:</strong></td>
<td>04/11/07</td>
<td><strong>Revised/Reviewed:</strong> 11/13/2014</td>
</tr>
</tbody>
</table>

**Policy Summary:** All information system resources must undergo a formal assessment process to properly identify risks and determine appropriate responses and controls.

**Purpose:** This policy reflects the University’s commitment to identify and implement security controls that will keep risks to information system resources at reasonable and appropriate levels.

**Policy:** Once information system data and resources have been identified and appropriately classified, information system resources must undergo a control review and risk assessment. The level of this assessment will be determined by the classification of the information system resource and its data.

This assessment must identify what controls for the resource are in place and what controls must be added to keep risks to information system resources at reasonable and appropriate levels.

This assessment process must be repeated any time changes occur in the classification, controls, environment, or operation that could impact the confidentiality, integrity or availability of the information system resource, for example, when there is a significant update or major version revision to the application or operating system, and/or the supporting architecture.

**Documentation:** All data collected and/or used as part of the Risk Management Process and related procedures will be formally documented and securely maintained.

**Scope/Applicability:** This policy is applicable to all OUHSC departments that operate information systems.

**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 (“GLB Act”)]

**Definitions:** See the Information Security Policy Definitions document for definitions

**Responsible Department:** Each OUHSC business unit that manages its own information systems is responsible for complying with this policy.

**Enforcement/Audit:** The university’s Internal Auditing department is responsible for monitoring and enforcing this policy.

**Related Policies:** Risk Analysis, Data Classification, Resource Identification, Resource Classification

**Renewal/Review:** This policy is to be reviewed and updated as needed by IT Information Security Services.