<table>
<thead>
<tr>
<th>Subject: Information System Resource Re-Assessment Policy</th>
<th>Coverage: OUHSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy #: Information Security-P#</td>
<td>Version: 1.1.1</td>
</tr>
<tr>
<td>Regulation: HIPAA, FERPA, GLB, State of Oklahoma</td>
<td>Approved:</td>
</tr>
<tr>
<td>Effective: TBD</td>
<td>Revised/Reviewed: 11/18/2014</td>
</tr>
</tbody>
</table>

**Policy Summary:**
All information system resources must undergo a formal re-assessment process to ensure data and resource classifications are still valid and verify appropriate responses and controls are still in place.

**Purpose:**
This policy reflects our commitment to identify and implement security controls which will ensure the risks to information system resources are kept at a reasonable and appropriate level.

**Policy:**
All information System Resources which have completed a control review and risk assessment must undergo a regular re-assessment of the data and resource classification and controls.

The frequency at which the reassessment will occur will be dependent upon the overall data and resource classification which will be determined during the resource identification and classification process.

In the event the re-assessment identifies inadequate controls or a lack of compliance with controls, a compliance issue will be open, reported to upper management, and tracked until compliance is achieved or mitigating controls have been established and implemented.

Information system resources which have undergone major changes/revisions which resulted in changes in how controls are implemented and managed must complete a new control review and risk assessment.

**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 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 organizational unit which 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 enforcement of this policy.

**Related Policies:**
Risk Analysis, data classification, resource identification, resource classification

**Procedures:**
Departments should develop procedures

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