This standard reflects the University's commitment to identify and implement security controls that will keep risks to university resources at reasonable and appropriate levels.

All units must conduct and document an information security risk assessment of university resources held or managed by a unit or by individuals in the unit at least every three years under the guidance of the Information Security Office.

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

All information collected or used as part of the risk assessment process must be formally documented and securely maintained. Risk assessment results must be presented to the UISO.

Related Guidance

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
Data Classification Standard (IS-S302)
Risk Assessment Procedure (IS-P1200)
16 CFR 314.4(b) [Section 501(b) of the Gramm-Leach-Bliley Act]
45 CFR 164.308(a)(1)(i) [HIPAA Security Rule]

Revision History

<table>
<thead>
<tr>
<th>Initial Draft</th>
<th>12/1/08</th>
</tr>
</thead>
<tbody>
<tr>
<td>UA-ISAC Review</td>
<td>4/2/09</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/09</td>
</tr>
</tbody>
</table>