# OU Information Technology Security Standards: Information Security Incident Reporting Standard

**Subject:** Information Security Incident Reporting Standard  
**Coverage:** OUHSC Components  
**Policy #:** Information Security-P#  
**Version:** 1.1  
**Regulation:** HIPAA, GLB, State of Oklahoma  
**Revised:** 01/21/14

<table>
<thead>
<tr>
<th>Policy Summary:</th>
<th>All suspected information security incidents must be reported promptly to the appropriate university office or party identified in this standard.</th>
</tr>
</thead>
</table>
| Standard: | **Users** must report information security incidents to the local support provider for that specific IT device or resource.  
In circumstances where the user is also the local support provider the user is obligated to follow the procedures listed under "Local Support Provider," below.  
**Local support providers** must collect appropriate information about the devices or resources that were compromised, disconnect affected IT devices from the network (where appropriate), and notify the IT service desk or IT security personnel about the incident and the action taken. Refer to the incident report form located at http://it.ouhsc.edu/forms/infosecurity/IncidentReport.doc  
Upon performing remedial actions, send mail notification to security personnel at IT-Security@ouhsc.edu or call (405) 271-2476 for accurate closure of the incident.  
Notify affected user of remedial steps taken, recommended mitigating activities and other appropriate information.  
**IT Service Desk or Security personnel** must open and maintain information security incident tickets, contact users and local support providers for the compromised devices about any actions needed, the reasons why, and how to reestablish service. The IT Service Desk or IT Security may initiate escalation procedures to the appropriate office or party.  
The IT Service Desk should handle incident reporting for students and enterprise applications such as e-mail and the network. |
| Documentation | All data collected and/or used as part of the Information System Security Incident process and related procedures will be formally documented and securely maintained. |
| Scope/Applicability: | This policy applies to all users of information systems or data at the OU Health Sciences Center and University Health Care Components. |
| Regulatory Reference: | HIPAA 45 CFR 164.308(a)(6)  
Payment Card Industry Data Security Standard |
| Definitions: | See the Information Security Policy Definitions document for definitions |
| Responsible Department: | IT Security Services |
| Enforcement/Audit: | The university’s Internal Auditing department is responsible for monitoring and enforcement of this policy. |

Procedures: Department should develop procedures