UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Security Incident Response Policy	**Coverage:** OUHSC
Policy #: Information Security-P#13.2	**Version:** 1.3
Regulation: HIPAA, GLB, State of Oklahoma	**Approved:** 09/14/11
Effective: 10/01/11	**Revised/Reviewed:** 11/19/2014

Purpose:	The University utilizes information technology resources extensively to conduct its mission. These resources are critical to the daily operation of the University's business. Additionally, they often interact with information governed by federal, state, and local laws or industry regulations. Ensuring the availability, confidentiality, and integrity of these resources and the information they interact with is critical to the University's continued success. The University recognizes potential threats to information systems originating from numerous sources including but not limited to malicious software, hacker activities, and other intentional or inadvertent actions. To ensure the highest level of security, the University will identify and respond to potential threats and investigate, document, and remediate any breaches of security.
Policy:	Legal Counsel and the Vice-President of Information Technology, have the authority to initiate investigations of all incidents related to possible breaches of security or exposure of sensitive information on information technology assets. Such investigations will be conducted by Information Technology in connection with appropriate University officials. The University has established a Computer Security Incident Response Team (CSIRT) to conduct and document investigations and coordinate recovery efforts and a Breach Assessment Committee to review findings and approve actions. All information systems, records, or data related to an incident including sensitive information under the authority, custody, control or possession of the University, must be made available to the Office of Legal Counsel or designee upon request. University workforce members including but not limited to employees, affiliates, or other users of University information systems shall assist in investigative efforts as requested by CSIRT members. Information Technology (IT) employees and workforce members must isolate and safeguard affected information systems in their current state, ensuring the system remains powered on so that the system state is preserved to the greatest extent possible. At no time will IT or other workforce members proactively modify or disturb the system by wiping the hard drive, reinstalling the operating system, or similar acts unless directed to do so by CSIRT.
Scope/Applicability:	This policy is applicable to all OUHSC and all OU Health Care Component workforce members, and those performing services for OUHSC and OU Health Care Components
Regulatory Reference:	Health Information Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Payment Card Industry Data Security Standards (PCI-DSS), Higher Education Opportunity Act, The Digital Millennium Copyright Act (DMCA), University Copyright policy, University Acceptable Use of Information Systems Policy.
Definitions:	See the Information Security Policy Definitions document for definitions

Responsible Department:	Managers and supervisors will ensure workforce members comply with policy. Upon being notified of non-compliance, CSIRT members will document the failure to follow the policy and report as necessary.
Enforcement/Audit:	This policy is authorized and approved by the Office of the General Council and OUHSC Dean's Council and Provost.
Procedures:	Data or Resource Owners or a delegate must formally document and maintain the processes and related procedures for compliance with this policy.
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.