UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information System Resource and Data Recovery Policy	**Coverage:** OUHSC
Policy #: Information Security-P#	**Version:** 2.0
Regulation: HIPAA, GLB, State of Oklahoma	**Approved:** 04/11/07
Effective: 04/11/07	**Revised/Reviewed:** 11/18/2014

Policy Summary:

Information System Resource and Data Owners must ensure all sensitive information system resources and data are identified and covered by recovery plans and procedures to ensure business continuity and the ability to restore any loss of sensitive information system resources and data.

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:

Information System Resource and Data Owners must establish, test and revise, and implement, as needed, resource and data recovery plans and procedures to ensure business continuity and the ability to restore any loss of sensitive information system resources or data.

At a minimum, these recovery plans must include:

- The conditions for activating the plan or procedure.
- Business, infrastructure, and resource requirements.
- Identification and definition of employee roles and responsibilities (primary and secondary) and contact information.
- Identification of dependencies on external entities for restoration and any requirements and/or agreements for/with these entities.
- Procedures (manual and automated) that identify recovery locations and describe the actions to be taken to resume normal operations within required time frames.
- The order in which information systems or data must be recovered.
- Allowable down times.
- Notification and reporting procedures.
- Procedures for allowing appropriate physical access to the facilities and information systems.
- Procedures for obtaining sensitive data when normal access is unavailable for business continuity.

Information System Resource and Data Owners must create and document a disaster recovery plan and procedures to recover information systems, resources, and data in the event of a disaster.

Information System Resource and Data Owners must create and document contingency plans and procedures for responding to an emergency or other incident that may occur (for example: vandalism, theft, system or power failure) during a disaster or as a random event.

Information System Resource and Data Owners must create and document an emergency operations plan and procedures for the protection of sensitive data during a disaster, emergency or other occurrence that may impact the protection of sensitive data. The emergency operations plan must reasonably ensure all sensitive data is protected prior to, during, and after the implementation/completion of any recovery plan or procedure.

	Information System Resource and Data Owners must establish a data backup plan and procedures to ensure exact copies of sensitive data are created, maintained, and available for the restoration of any loss. A testing and revision plan must be established and implemented to ensure the periodic testing of recovery plans and related procedures. This plan will define the cycle and scope of the tests, training of those involved, and the type of tests performed (exercise or real operational scenario). Employees must receive regular training on these plans and procedures and have access to a current copy of the plans and procedures at all times. An appropriate number of copies of the plans and procedures must be kept off-site.
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 Information System Resource and Data Owners.
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 (‘‘G–L–B Act’’) State of Oklahoma Information Security, Policy Procedures Guidelines
Definitions:	See the Information Security Policy Definitions document for definitions
Responsible Department:	Each organizational unit within the University of Oklahoma 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 enforcement of 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.