Subject: Information System Telework Policy

Policy #: Information Security-P#11.7.2

Regulation: HIPAA, GLB, State of Oklahoma

Effective: 05/09/07

Coverage: OUHSC

Version: 2.0

Approved: 05/09/07

Revised/Reviewed: 11/20/2014

Policy Summary:
Procedures must be in place to ensure all computing devices used to work remotely (telework) and access University’s sensitive information system resources and data are appropriately secured.

Purpose:
This policy reflects our commitment to identify and implement security controls which will keep risks to information system resources at reasonable and appropriate levels.

Policy:
Procedures must be in place to ensure all computing devices used to telework and access sensitive University’s information system resources and data remotely are secured in a manner equivalent to on-site workstations and in a manner commensurate with the risks of the telework environment to protect the confidentiality, integrity, and availability of the data contained on or accessed through these workstations.

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 OUHSC.

Regulatory Reference:
HIPAA 45 CFR 164.308(a)(1)(ii)(B)
Payment Card Industry Data Security Standard (PCI DSS)

Definitions:
See the Information Security Policy Definitions document for definitions

Responsible Department:
Each organizational unit within the University of Oklahoma that has work force members who telework 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.