UNIVERSITY OF OKLAHOMA
Information Technology
Security Standard

Subject: Facility Security Plan Standard
Standard number: Information Security S-
Regulation: HIPAA, FERPA, GLB, PCI DSS, State of Okla. ISPPG
Effective: 06/07/2005
Coverage: OU Health Sciences Center
Version: 1.2
Reviewed/Revised: 02/1/2013

Purpose:

The purpose of this *Facility Security Plan Standard* is to provide a framework for developing a Facility Security Plan for the protection of Sensitive Data.

Standard:

The Facility Security Plan must include appropriate safeguards for all equipment containing Sensitive Data. Such equipment includes, but is not limited to, workstations, servers, portable computing devices and biomedical devices (e.g., MRI).

The Facility Security Plan must be based on a risk assessment, conducted at least annually, that assesses the risks to the facilities and the information systems resources contained within.

At a minimum, the University Facility Security Plan must address the following:

- Identification of information system resources to be protected from unauthorized physical access, tampering, and theft.
- Identification of processes and controls used to protect information system resources from unauthorized physical access, tampering, and theft.
- Actions to be taken if unauthorized physical access, tampering, or theft attempts are made against information system resources.
- Identification and definition of OUHSC workforce member responsibilities.
- Notification and reporting procedures
- A maintenance schedule that specifies how and when the plan will be tested, as well as the process for maintaining the plan.

All appropriate OUHSC workforce members must have a current copy of the plan. An appropriate number of current copies of the plan must be maintained off-site.

Related Documents: