

**UNIVERSITY OF OKLAHOMA**  
**Information Technology**  
**Security Policy**

**Subject:** Data Classification Policy

**Coverage:** OU Health Science Center and Health Care Components

**Policy number:** Information Security P-5.2

**Draft Date:** 11-14-2005

**Regulation:** HIPAA, FERPA, GLB, PCI DSS, State of Okla. ISPPG

**Approved:** 11-16-2005

**Effective:** 11-16-2005

**Revised:**

**Purpose:**

The purpose of this *Data Classification* policy is to provide a framework for protecting OU information resources. Information resources are assets of the University and must be classified by the sensitivity and associated risks to confidentiality, availability, and integrity. Data with the highest sensitivity and risk need the greatest amount of protection. Consistent use of this classification system will facilitate business activities that apply appropriate levels of protection.

**Policy:**

In order to protect information from unauthorized disclosure, use, modification or deletion, all OU Health Sciences Center and Health Care Components must use the designated information classification system.

- Category A – Highest level, most sensitive
- Category B – Moderate level of sensitivity
- Category C – Very low, but still some sensitivity
- Category D – Not sensitive

Data in Category A or B will be designated as “*Sensitive*”.

Use criteria in the [Data Classification Standard](#) to determine which data category is appropriate for a particular information or infrastructure system.

**Scope/Applicability:**

This policy is applicable to the OU Health Sciences Center and OU Health Care Components.

**Regulatory Reference:**

- 45 CFR 164.308(a)(1)(i) [HIPAA Security rule: administrative: security management process]
- 34 CFR Part 99 [Family Educational Rights and Privacy Act]
- 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (“GLB Act”)]
- PCI DSS requirement 12.1 (Payment Card Industry Data Security Standard)
- State of Oklahoma Information Security, Policy Procedures Guidelines

**Definitions:**

See separate Definitions document

**Responsible Department:**

Each department that maintains information systems and electronic media is responsible for complying with this policy.

**Policy Authority/ Enforcement:**

The University’s Internal Auditing department will periodically assess departmental compliance.

**Related Documents:**

Data Classification Standard, Data Protection Standard, Data Disposal and Reuse Policy, Risk Assessment Policy, Risk Management Policy, PHI Server Consolidation Policy