

UNIVERSITY OF OKLAHOMA
Information Technology
Security Standard

Subject: Data Classification Standard

Coverage: OU Health Science Center and Health Care Components

Standard number: Information Security S-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 Standard* is to provide a framework for classifying and protecting OU information resources.

Classification table:

	Category A Highest most sensitive	Category B Moderate sensitivity	Category C Very low, but still some sensitivity
Legal requirement	Protection of data is required by law or contract	OU has an obligation to protect the data	Minimal
Reputation risk	High	Medium	Low
Other Institutional Risks	Information which provides access to resources, physical or virtual	Information whose loss or compromise impairs regular business operations	
Examples (this is not an exhaustive list)	<ul style="list-style-type: none"> • Credit card numbers • SSN • Passwords • Medical • Student • Prospective student • Personnel • Donor or prospect • Financial • Contract • Confidential agreements • See list of specific HIPAA, GLB, and FERPA data elements in the <i>Definitions</i> document) 	<ul style="list-style-type: none"> • Research detail or results that are not Category-A • Financial transactions which do not include Category-A data (e.g., telephone billing) • Physical plant detail • Certain management information 	<ul style="list-style-type: none"> • Personal directory data (e.g., internal phone lists and email addresses) • Internal training material
Category D - Not Sensitive			

Related Documents:

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