Data Classification Policy

Purpose/Statement

A data classification policy is necessary to provide a framework for securing data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal. This policy outlines measures and responsibilities required for securing data resources. It shall be carried out in conformity with state and federal law.

Reason for the Policy

Clark must maintain and protect its institutional assets and comply with applicable state and federal regulations.

Entities Effected by this Policy

This policy applies to all University administrative data, all user-developed data sets and systems that may access these data, regardless of the environment where the data reside (including systems, servers, personal computers, laptops, portable devices, etc.). The policy applies regardless of the media on which data reside (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.).

Clark also expects all employees, partners, consultants and vendors to abide by Clark's information security policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by Clark's information security policies.

Who Should Read this Policy

All faculty, staff and student employees as well as third-party contractors should be aware of the policy.

Overview

Clark takes seriously its commitment to respect and protect the privacy of its students, alumni, faculty, staff, parents and friends, as well as to protect the confidentiality of information important to the University's academic and research mission. The University recognizes that the value of its data resources lies in their appropriate and widespread use. It is not the purpose of this policy to create unnecessary restrictions to data access or use for those individuals who use the data in support of University business or academic pursuits.

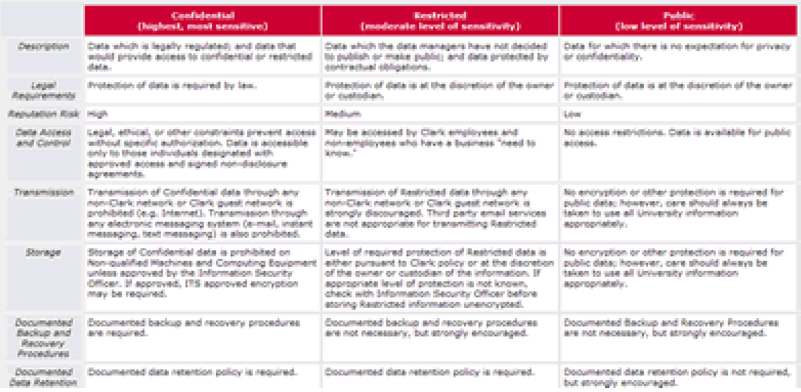
Procedures

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk. To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data,

data should be classified into one of the following categories:

1. Confidential - Data which is legally regulated and data that would provide access to confidential or restricted data.
2. Restricted - Data which the Data Managers have decided NOT to publish or make public and data protected by contractual obligations.
3. Public - Data which there is no expectation for privacy or confidentiality.

Confidential data and Restricted data will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business or research functions of the University, result in financial loss, or violate law, policy or University contracts. Security measures for data are set by the Data Custodian, working in cooperation with the Information Security Officer, Information Technology Services and the respective Data Managers. The table below outlines the criteria used to determine which data classification is appropriate for a particular piece of data or information system.



	Confidential (highest, most sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
Description	Data which is legally regulated; and data that would provide access to confidential or restricted data.	Data which the data managers have not decided to publish or make public; and data protected by contractual obligations.	Data for which there is no expectation for privacy or confidentiality.
Legal Requirements	Protection of data is required by law.	Protection of data is at the discretion of the owner or custodian.	Protection of data is at the discretion of the owner or custodian.
Reputation Risk	High	Medium	Low
Data Access and Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements.	May be accessed by Clark employees and non-employees who have a business "need to know."	No access restrictions. Data is available for public access.
Transmission	Transmission of Confidential data through any non-Clark network or Clark guest network is prohibited (e.g. Internet). Transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is also prohibited.	Transmission of Restricted data through any non-Clark network or Clark guest network is strongly discouraged. Third party email services are not appropriate for transmitting Restricted data.	No encryption or other protection is required for public data; however, care should always be taken to use all University information appropriately.
Storage	Storage of Confidential data is prohibited on Non-qualified Machines and Computing Equipment unless approved by the Information Security Officer. If approved, ITS approved encryption may be required.	Level of required protection of Restricted data is either pursuant to Clark policy or at the discretion of the owner or custodian of the information. If appropriate level of protection is not known, check with Information Security Officer before storing Restricted information unencrypted.	No encryption or other protection is required for public data; however, care should always be taken to use all University information appropriately.
Documented Backup and Recovery Procedures	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.	Documented Backup and Recovery Procedures are not necessary, but strongly encouraged.
Documented Data Retention	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is not required, but strongly encouraged.

Click to View Table of Classification Criteria

Responsible Organization/Party

This policy will be re-evaluated on or about the first day of each calendar year to determine whether all aspects of the program are up to date and applicable in the current business environments, and revised as necessary. The Information Security Officer is responsible for this policy.

Enforcement

The Information Security Officer will investigate suspected violations, and may recommend disciplinary action in accordance with University codes of conduct, policies, or applicable laws. Sanctions may include one or more of the following:

- Suspension or termination of access
- Disciplinary action up to and including termination of employment
- Student discipline in accordance with applicable University policy
- Civil or criminal penalties
- Or any combination of the above

Reporting Violations

Report suspected violations of this policy to the Information Security Officer, the appropriate Data Manager or the Responsible Organization/Party. Reports of violations are considered Restricted data until otherwise classified.

Related Policies and Resources

- Appropriate Use of Clark's Information Technology System

Date of Creation: February 25, 2009
Date of Last Revision: October 14, 2009