# Data Classification Policy

## Section 1. PURPOSE AND SCOPE

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.

## Section 2. PROCEDURES AND ENFORCEMENT

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:

- Confidential - Data which is legally regulated and data that would provide access to confidential or restricted data.
- Restricted - Data which the Data Managers have decided NOT to publish or make public and data protected by contractual obligations.
- 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. Click here to view the Table of Classification Criteria.

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

**Section 3. 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 Regulations

Appropriate Use of Clark's Information Technology System

Clark University Data Access Policy

## History/Revision Information

**Responsible Office/ Division: ITS**

**Effective Date**: February 25, 2009
**Last Amended Date**: March 5, 2024
**Next Review Date:** June 6, 2024