The University holds and processes various types of data to carry out its operations. It is essential that university data is assigned the appropriate sensitivity category and the minimum-security controls necessary to keep it safe from unauthorized or unintentional access, mishandling, or misuse.

The purpose of this policy is to establish a data governance process to maintain the confidentiality and integrity of university data from the time of creation or collection to disposal.

Information Handling: These are the practices for handling data securely based on its sensitivity.

Data Classification

All data held and used by the university will be classified under the following:

Restricted
Internal
Public

These classifications are governed by various data privacy legislation which the university is required to comply with. These include the following:

Legislation

Identify Protection Act:

This act sets out the requirements for protecting the confidentiality of Social Security Numbers (SSNs) by requiring state and government agencies to implement policies and procedures for maintaining the confidentiality and integrity of SSNs and to train employees who handle SSNs. Learn how the University complies with the act.

Payment Card Industry Data Security Standards (PCI DSS):

PCI DSS sets out the requirements to safeguard the privacy of payment card information or cardholder