MERCER UNIVERSITY

UNIVERSITY POLICIES

Title:	Data Security Policy
Effective Date:	June 5, 2025
Issuing Authority:	Senior Vice President for Administration and Finance
Policy Contact:	Assistant VP of Information Technology and Chief Information Officer helpdesk@mercer.edu, 478-301-7000

Purpose

The purpose of this policy is to ensure the security of administrative information (Data) which is processed, stored, maintained, or transmitted on computing systems (Systems) and networks centrally managed by Information Technology and to protect the confidentiality of that data. This policy is designed to protect data from unauthorized change, destruction, or disclosure, whether intentional or accidental.

Scope

This policy applies to any Information Technology staff who have access to data. It regulates the use of the systems and applies to all computer programs used to access data, as well as the computers and terminals that run those programs, including workstations to which the data has been downloaded.

Exclusions

None

Definitions

As used in this policy, the following term(s) have the meaning specified below:

Custodian of the Data: the entity or office that is delegated by the data owner the responsibility of performing management functions for the data.

Data: administrative information which is processed, stored, maintained, or transmitted on computing systems and networks centrally managed by IT.

Data Owner: the entity or office that is authorized to collect and manage the data as official record.

Staff: any IT employees (permanent or temporary) who have access to data.

Systems: all IT maintained central administrative systems which provide access to data.

Policy Statement

It is the responsibility of IT staff to protect data from unauthorized change, destruction or disclosure according to University, campus, or local guidelines, as well as any other regulations or laws that may apply. This policy governs all IT-maintained central administrative systems that provide access to data and outlines the responsibilities of staff who maintain or use these systems. It should be noted that, in general, IT is not the Data Owner, but is the Custodian of the Data. It is the owner who has the authority to grant or revoke access to data or systems that use data. It is IT's responsibility to implement specific procedures that enforce access authority and establish guidelines and standards for systems and data security under this policy. It is also IT's responsibility to develop and promulgate procedures for the dissemination of this policy. Each individual is responsible for carrying out his or her responsibilities under this policy.

Violations of this policy include but are not limited to: accessing data or systems to which the individual has not been specifically given access; enabling unauthorized individuals to access the data; disclosing data in a way which violates applicable policy, procedure or other relevant regulations or laws; or inappropriately modifying or destroying data. Violations may result in access revocation, corrective action up to and including dismissal, and/or civil or criminal prosecution under applicable law. Recourse under this policy is available under the appropriate section of the employee's personnel policy or contract, or by pursuing applicable legal action.

Website Address

Information Technology: https://it.mercer.edu/student/index.htm

History

Approved by the Executive Vice President of Administration and Finance on December 1, 2008
Revised June 5, 2025