POLICY 08:13:00
INFORMATION SECURITY MANAGEMENT SYSTEMS
(ISMS)

I. Purpose

The purpose of this policy is to define and describe the College's Information Security Management System (ISMS), including related policies and procedures.

II. Scope and Applicability

The ISMS is designed to protect the College's data, networks and information systems from all internal or external threats, whether deliberate or accidental. It also should ensure the confidentiality, integrity, and availability of technology and data. The ISMS is accomplished through the development and implementation of policies, procedures and actions based on compliance standards which address security requirements and expectations. These standards will follow industry-defined effective practices in securing technology and data.

This policy applies to all individuals using or attempting to use any computer or information technology resource of the College. Use of a computer or information technology resource or system signifies the following:

- The user agrees to comply all applicable College and Tennessee Board of Regents (TBR) policies.
- The user accepts that failure to comply with this policy may result in temporary or permanent denial of access to computer or information technologies, or in some cases may result in college disciplinary action or legal action.

III. Definitions

Availability – providing data access to authorized users when it is needed

College information – College related data that can take many forms including data stored on computers and servers, transmitted across networks, printed out or written on paper, sent by fax, or stored on physical media
Confidentiality - protecting information from being accessed by unauthorized parties
Integrity –consistency, accuracy, and trustworthiness of data over its entire life cycle

IV. Policy and Responsibilities

Pellissippi State will ensure that appropriate information, data and network resources are made available with integrity and minimal disruption to staff and the public. Systems will be maintained and updated regularly following Tennessee Board of Regents Policy 1.08.01.00 (formerly G-50) Enterprise Information Systems Updates and departmental procedures. The confidentiality of college information will be protected through documented access controls as required by business process or role with the college.

Information security is managed through Pellissippi State's Information Security Management System (ISMS) framework.

Information will be classified and protected in accordance to Policy 08:13:13 Data Classification and all regulatory and legislative requirements will be met.

An Information Technology Disaster Recovery Plan shall be in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. A Cyber Incident Response Plan shall be in place to respond to real or assumed cyber threats and breaches. All breaches of information security, actual or suspected, will be reported to, and investigated by the Incident Response Team as identified in the Cyber Incident Response Plan. The Information Technology Disaster Recovery and Cyber Incident Response plans should be maintained and tested, as appropriate, on a regular basis.

Information security awareness education and training will be made available to all employees. Training may be required for continued account access and privileges. Account owners and other users of information technology resources provided or supported by the College must comply with the appropriate college policies including, but not limited to, 08:04:05 Information Technology Resources, 08:13:01 Information Technology Acceptable Use, 08:13:02 Computer Account; and Tennessee Board of Regents (TBR) Policies:1.08.00.00 Information Technology Resources, 1.08.04.00 (formerly G-053) Personally Identifiable Information (PII), 1.08.05.00 (formerly G-054) IT Acceptable Uses.

Appropriate access control will be maintained according to the related college policies including 08:13:08 Electronic Account Access, 08:13:09 Wireless Network, 08:13:10 Remote Access, and 08:13:12 Data Access Management as well as Tennessee Board of Regents (TBR) Policy 1.08.03.00 (formerly G-051 & G-052) Access Control.

A. Responsibilities

Information Services has direct responsibility for maintaining the ISMS and writing and/or managing the development of relevant policies, procedures and guidelines regarding the use of information technology including, but not limited to, information security.

All managers are directly responsible for implementing the ISMS within their units, and for adherence by their staff.

All employees are directly responsible for adhering to the ISMS requirements for their role at the college.

Information Services will work closely with other departments and vendors to establish appropriate information security standards including the continual review of risk evaluation criteria, which may impact information security. Policy 08:13:14 Cloud Computing must be followed for any cloud-based vendor.

Approved: Executive Council, March 4, 1991
Executive Council, August 13, 1991
Editorial Changes, May 4, 1993
Executive Council, May 27, 1993
Reviewed/Recommended: President's Council, April 29, 1996
Approved: President Allen G. Edwards, May 1, 1996
Approved: President Allen G. Edwards, November 12, 1997
Approved: President Allen G. Edwards, August 5, 2002
Reviewed/Recommended: President's Staff, March 26, 2007
Approved: President Allen G. Edwards, March 26, 2007
Reviewed/Recommended: President's Staff, May 9, 2011
Approved: President Allen G. Edwards, May 9, 2011
Reviewed/Recommended: President's Staff, June 6, 2011
Approved: President Allen G. Edwards, June 6, 2011
Reviewed/Recommended: President's Council, September 26, 2016
Approved: President L. Anthony Wise, Jr., September 26, 2016
Policy 08:13:00 was formally titled Network and Technical Service Department-
Title changed to Information Security Management Systems (ISMS), September 9, 2019
Reviewed/Recommended, President's Council, September 9, 2019
Approved: President L. Anthony Wise, Jr., September 9, 2019