TSC
TALLAHASSEE
STATE COLLEGE

444 Appleyard Dr.
Tallahassee, FL 32304
(850) 201-6200 | tsc.fl.edu

March 23, 2026

MEMORANDUM

TO: Jim Murdaugh, Ph.D.
President

FROM: Barbara Wills, Ph.D.
Vice President for Administrative Services and Chief Business Officer

SUBJECT: Policy Manual Changes

Item Description
This item requests Board approval of Policy Manual changes in chapter 8000 – Operations.

Overview and Background
The College brings forth a request to modify the College’s Policy Manual: creation of Policy 8820.1 – Acceptable Use for Technology Resources and Artificial Intelligence will provide standards for ethical, legal, and responsible use of the College’s technology resources.

Funding/ Financial Implications
N/A

Past Actions by the Board
The Board approved previous revisions to the College’s Policy Manual in November 2025.

Recommended Action
Approve revision of College policies as presented.

Book	Policy Manual
Section	8000 Operations
Title	ACCEPTABLE USE FOR TECHNOLOGY RESOURCES AND ARTIFICIAL INTELLIGENCE_New
Code	po8820.1
Status	
Legal	F.S. 775.0847 F.S. 827.071 (4), (5) F.S. 1001.64 F.S. 1001.65 Computer Fraud and Abuse Act 18, 1030 Electronic Communications Privacy Act 18 USC, 2510-2522 Florida Computer Crimes Act Chapter 815

8820.1 - **ACCEPTABLE USE FOR TECHNOLOGY RESOURCES AND ARTIFICIAL INTELLIGENCE**

This policy supplements Policy 8820 - Information Technology. In the event of any inconsistency, Policy 8820 shall prevail.

The College is dedicated to leveraging technology in ways that elevate the quality of learning and strengthen the efficiency of its operations.

This Acceptable Use Policy (AUP) establishes the standards for ethical, legal, and responsible use of the College's technology resources, including networks, computers, information systems, and Artificial Intelligence (AI) technologies. The policy is designed to safeguard the integrity, security, and privacy of all the College's technology assets, support academic and administrative missions, and ensure compliance with all applicable laws and regulations.

This policy applies to all individuals who access or use the College's technology resources, including but not limited to students, employees, contractors, consultants, volunteers, and visitors, in both academic and administrative settings.

Definitions

Technology Resources: All hardware, software, networks, cloud services, and information systems owned, operated, or maintained by the College.

AI Systems: Computer programs or platforms designed to perform tasks requiring human intelligence, such as data processing, learning, adaptation, and autonomous or semi-autonomous operations.

Network: The interconnected system of digital communication channels and devices managed by the College.

Information Systems: Organized collections of hardware, software, data, and procedures supporting the College.

Personally Identifiable Information (PII): Any information that can identify an individual, including but not limited to names, addresses, social security numbers, and academic records.

Acceptable Use

All users must utilize the College's technology resources in a manner that is ethical, legal, and aligned with the College’s mission. Acceptable use includes activities that support teaching, learning, research, and administrative functions. Users are responsible for:

Accessing only systems and data for which they have explicit authorization;

Protecting credentials and preventing unauthorized access to accounts or devices;

Respecting intellectual property rights;

Using AI exclusively in accordance with the College's Human-centered AI Governance, the Safe Harbor Principle, and faculty or administrative guidelines; and

Maintaining the confidentiality of sensitive information and complying with all privacy policies.

Prohibited activities include, but are not limited to:

Unauthorized access, use, or disclosure of data, systems, or accounts;

Introduction or distribution of malware, viruses, or other harmful software;

Plagiarism, cheating, or data fabrication in academic or administrative work;

Use of non-College-approved AI tools, including personal AI accounts, to process Restricted or Internal data;

Illegal downloads, distribution of copyrighted material without permission, or violation of licensing agreements;

Uploading Internal or Restricted data into any unvetted application or third-party system without an approved IT Security Review; and

Use, download, or access of any application identified as prohibited by the Florida Department of Management Services (DMS) on College owned or controlled technology is forbidden. Employees must comply with removal timelines and waiver processes described in Policy 8820.

Privacy and Security

Users must safeguard all personal, confidential, and College data. Sensitive information, including PII, FERPA-protected records, and Criminal Justice Information (CJIS), must only be handled using College-approved systems and tools.

The following requirements apply:

Do not share or upload protected data to external or public platforms without explicit approval and contractual safeguards;

Any system or tool, AI or otherwise, that processes Restricted data requires IT Security Review and approval under the Technology Acquisition & Security Compliance process; and

Comply with all federal and state data protection laws, including Florida Statutes and applicable privacy regulations.

AI-Specific Guidelines

The College recognizes the opportunities and risks associated with AI technologies.

The following rules apply to all AI use:

AI initiatives must support the College's academic and administrative objectives and adhere to principles of fairness, transparency, accountability, and privacy;

Substantive AI contributions to academic or official work must be acknowledged; presenting AI-generated content as original work is prohibited;

Users are 100% responsible for verifying AI-generated outputs before use; AI can produce errors or fabricated information (often referred to as "hallucinations");

Faculty must clearly communicate course-specific AI policies in course syllabi;

All AI systems must undergo the IT Security Review and Delta Assessment processes to ensure compliance with NIST 800-171, FERPA, and Florida public records requirements;

AI must not be used for automated decisions affecting students, employees, or research subjects without substantive human oversight or formal approval by Information Technology and the applicable data custodians;

Research and academic AI projects require ethical review by the appropriate College committee; and

Uploading non-public data into AI systems is prohibited unless specifically authorized.

Reporting AI-Related Security Incidents

Because AI technology is rapidly evolving, users may encounter unique security or integrity issues. To protect the College community, users must immediately report the following specific incidents to the IT Help Desk:

If you inadvertently upload Restricted Data—such as Social Security numbers, student grades, or financial records—into a public or unverified AI tool;

If you discover that an AI tool used for College business is consistently producing fabricated facts, false legal citations, or biased outputs that could lead to harmful decisions or academic integrity violations;

If you notice an AI tool, internal or external, is accessing or requesting information that seems beyond its "need to know" or intended purpose;

If you become aware of AI being used for "automated decision-making" (e.g., grading, admissions, or personnel evaluations) without the required substantive human oversight.

The College maintains a "no-fault" reporting culture for accidental AI data exposure. Our primary objective is the containment of risk and the protection of College data. A quick report allows the IT Security Team to coordinate with vendors to delete "spilled" data from training sets, flag unreliable tools for the campus community, and adjust security filters to prevent future occurrences.