TALLAHASSEE STATE COLLEGE

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

Introduction

The Tallahassee State College (TSC) Information Security Plan describes the policies, procedures and standards employed by TSC to safeguard both the information systems in use by the College and the data stored on those systems. This security plan is intended to comply with regulations and policies set by the State of Florida as well as other state and federal agencies.

Scope

The policies, procedures and standards contained in the TSC Information Security Plan apply to all information systems maintained by the College.

Objective

The objective of the TSC Information Security Plan is to provide a framework by which the College can protect both the electronic systems and electronic data that is in the care, custody and control of the College. This not only means protecting the systems and data from unauthorized access but also to helping those with authorized access understand their roles with respect to data security, privacy, integrity and confidentiality.

Roles and Responsibilities

Vice President for Information Technology (VP for IT): responsible for setting the vision and strategic direction for technology and technology related policies and procedures at the College. Responsible for managing the Information Technology department.

Director, Enterprise Systems: reporting to the VP for IT, the Director of Enterprise Systems supports all of the centralized systems and software in use at the College including all centralized databases, software applications, and software development activities. The Director of Enterprise Systems also serves as the Chief Information Security Officer (CISO) for the College.

Director, IT Infrastructure: reporting to the VP for IT, the Director of IT Infrastructure is responsible for the physical and virtual servers and systems in use by the College as well as for the data, voice and video networks at the College.

Director, User Services: reporting to the VP for IT, the Director of User Services is responsible for supporting all of the end-user technology at the College, including desktop, tablet and mobile technologies, as well as providing technology training and front-line support for the College for

technology and technology-related issues.

Network Administrator: reporting to the Director, IT Infrastructure, the Network Administrator and their staff are responsible for maintaining and securing the data, voice and video networks at the College.

Manager, Server Administration: reporting to the Director, IT Infrastructure, the Server Manager and heir staff are responsible for maintaining and securing the servers, both physical and virtual, and networked storage devices at the College.

Client Support Manager: reporting to the Director, User Services, the Client Support Manager is responsible for the security of all desktop computers, laptop computers and mobile devices owned by the College.

Incident Response Team: the group within IT that responds to IT security related incidents. Led by the Director of Enterprise Systems acting in their role as CISO, the team includes the Director, IT Infrastructure; Director, User Services; Network Administrator; Server Manager; Client Support Manager; VP for IT and other members of IT and the campus community as needed.

Data Custodian: members of the TSC community who have primary responsibility for the management of specific pieces of information.

Policies

TSC Policy 7540: INFORMATION
TECHNOLOGY TSC Policy 8305:
INFORMATION SECURITY
TSC Policy 8315: INFORMATION MANAGEMENT

Passwords

NIST Special Publication 800-63B "Digital Identity Guidelines: Authentication and Lifecycle Management," published in June 2017, sets the current standards for authentication. The rules proposed below meet the NIST guidelines and have been endorsed by the Gartner Group, an IT Consulting company.

- Passwords must be at least 10 characters and can be as long as 64 characters.
- There is no requirement to use a mixture of uppercase, lowercase, digits and special symbols, although those are all permitted.
- All proposed passwords will be verified against a "blacklist" of known bad (or non-secure) passwords. The blacklist will consist of dictionary words, words with special meaning to TSC (such as "eagles" or "FPSI"), and passwords that are available on the "dark web" due

to a data breach. If the proposed password is on the blacklist the user will be told to choose another password.
- Passwords will not have an expiration date. However, passwords will be required to be changed if the user falls victim and enters data as a result of a real or simulated phishing attempt, forgets their password, or has been the victim of a hacking attempt.
- Multifactor authentication is required
- The use of SMS messaging for multifactor authentication will be discouraged due to SIM swapping. The use of authenticator apps will be encouraged instead.
- The multifactor authentication will be good for 28 days.

Data Security Training

Annual data security training is required for all employees of the College. Any employee who fails to complete the annual training within the allotted time will lose access to online resources and their supervisor will be notified.

In addition, the College conducts simulated phishing email attacks on all employees on a monthly basis. The goal is to continue to encourage employees to pay attention to the warning signs of phishing email messages, to never open suspicious attachments, to not click on links in such messages and to never provide personal information, including usernames and passwords, on web sites linked in phishing email messages.

Procedure for Failing Phishing Tests or Falling Victim to Actual Phishing Attack

The following procedure describes the College's approach to employees who fall victim to both simulated and real phishing attacks. This procedure was developed by the Technology and Innovation Committee of the College and approved by the College's Executive team. Questions about this procedure should be directed to the Vice President for Information Technology.

When someone clicks on a link or attachment in a simulated or real phishing email…
…for the first time:

- A notice will be sent to the employee, including notice of increasing penalties should it happen again
- A notice will be sent to the employees' supervisor
- The employee will be required to take additional data security training (online)
- The employee must read material describing the impact of data breaches and ransomware

…for the second time, or for the first time if they entered data in a simulated or real phishing email…

- All of the items listed under "…for the first time" above, plus:

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

- The employee will need to attend a meeting with VP for IT, CISO, or their designee
    - for contingent workers working outside of the immediate 3-county area this meeting will be done via audio or video conference
- The employee will be locked out of most systems until meeting with VP for IT, CISO, or their designee

...for the third time, or for the second time if they entered data in a simulated or real phishing email...

- All of the items listed under "...for the second time..." above, plus:
- The employee will need to attend a meeting with their VP
- The employee will be locked out of most systems until meeting with their VP
- A formal letter, jointly from their VP and VP for IT, will be placed in their employment file
- This and any subsequent violations will be turned over to HR for possible further action

Note for contingent workers: notices to their supervisor will also include notices to the appropriate TSC program director, and "their VP" will refer to the appropriate TSC organizational reporting VP.

Personally Identifiable Information

Personally identifiable information (PII) is information that is defined in Florida Statute 501.171 "Security of confidential personal information," The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) as well as other local, state and federal statutes and regulations. It is the responsibility of the Data Custodians to determine which members of the campus community shall have access to the PII that is under their responsibility. Such access shall be reviewed by each Data Custodian on an annual basis.

Network Security Monitoring

Through our membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC), the College is participating in the Albert service. The Albert service consists of an Intrusion Detection System (IDS) sensor placed within the College's network that collects network data and sends it to the MS-ISAC for analysis. MS-ISAC then notifies the College in real time about any malicious activity they detect.

Vulnerability Management Program

Through the College's in MS-ISAC the College receives a monthly domain profiling report on out-of-date and vulnerable software including server software, web programming languages

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

and content management systems. The monthly report also includes an IP address profiling report.

Security Breach

A security breach is defined in Florida Statute 501.171 "Security of confidential personal information." Should the College become aware of a security breach the Incident Response Team will be convened to respond to the breach. Depending on the nature of the security breach we may also seek the assistance of the MS-ISAC Computer Emergency Response Team (CERT), as service that we have access to through our membership in MS-ISAC.

Criminal Justice Information and Criminal Justice Information Services

The Tallahassee State College Police Department (TSC PD) is responsible for safeguarding criminal justice information (CJI) and access to criminal justice information services (CJIS). The TSC PD maintains a Criminal Justice Use Agreement (CJUA) with the Florida Department of Law Enforcement (FDLE) and acts in compliance with the Federal Bureau of Investigation Criminal Justice Information Services Security Policy (FBI CSP). The TSC PD also maintains a "Memorandum of Agreement" with the TSC IT Department in support of these efforts.