Collin College Technology Services (CC-TS)
Computer Compliance – Information Security Procedure (ISP)

PURPOSE

This ISP aims to ensure a Technology Services infrastructure that promotes the College's mission. CC's Technology Services network has been established for the use and benefit of CC in its academic, business, and other operations. This document provides direction and support for the CC Information Security Plan and the CC-TS ISPs.

The framework of this CC-TS ISP collectively represents the basis of the institutional Information Security program and, on the aggregate whole, meets the objectives as articulated by the applicable rules of the Texas Administrative Code Chapter 202 (TAC§202), Texas Higher Education Coordinating Board (THECB) and the associated guidelines.

This ISP promotes the following goals:

- To ensure the integrity, reliability, availability, and performance of CC Technology Services resources
- To ensure that the use of CC-TS resources is consistent with the laws and policies that govern CC as a whole and the needs of the College
- To ensure that Technology Services resources are used for their intended purposes
- To ensure all individuals granted access privileges to CC-TS resources have a clear understanding of what is expected during use and the consequences of violating CC policies or ISPs

SCOPE

This program applies equally to all individuals granted access privileges to any CC-TS resources.

STATEMENT

Technology Services resources play an integral part in the fulfillment of the primary mission of the College. Users of CC-TS resources have a responsibility to protect and respect those resources and know the regulations, policies, and ISPs that apply to the appropriate use of the College's Technology Services resources.

Users must understand the expectation that if needed, CC-TS resources may be limited or regulated by CC to fulfill the primary mission of the College. Usage may be constrained as required to assure adequate capacity, optimal performance, and appropriate security of those resources.

Anyone using CC's information resources expressly consents to monitoring of the network by the College at any time and for any purpose, including but not limited to evidence of possible criminal activity, violations of applicable law, contract, copyright or patent infringement, or violation of any college policy, ISP, or rule.

A review of the institution's information security program for compliance with these standards will be performed at least annually, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or the designated representative(s). TAC 202.76(c)

NON-CONSENSUAL ACCESS

CC cannot guarantee the privacy or confidentiality of electronic documents. Consequently, persons that use these CC-owned resources, or any personally owned device connected to a CC resource, have no right to or expectation of privacy in their use of these resources and devices. However, CC will take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons that CC will not seek access to their electronic messages or documents without their prior consent except where necessary to:

- Satisfy the requirements of the Texas Public Information Act, or other applicable laws or regulations
- Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity
- Protect the integrity of CC-TS resources, and the rights and other property of CC
- Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergencies
- Protect the rights of individuals working in collaborative situations where information and files are shared
- Comply with law enforcement investigations, subpoenas, or court orders
- Comply with any other authorized business, financial, or legal purpose or requirements

To appropriately preserve the privacy of electronic documents and allow authorized individuals to perform their assigned duties, specific college staff and law enforcement will sign a CC Non-Consensual Access to Electronic Information Resources Request Form annually and submit the form to the Office of the Information Resources Manager (IRM). At the beginning of each fiscal year, the IRM will resubmit, review, and approve or deny non-consensual access requests.

Individuals may request non-consensual access to specific data by initiating the Non-Consensual Access to Electronic Information Resources Request Form, obtaining the approval of their organizational head, and submitting the form to the Office of the Information Resources Manager (IRM). If the request appears compliant with college ISPs, the IRM or designee will coordinate with the Chief Information Security Officer (CISO) as necessary to satisfy the request.

VIOLATIONS

Failure to adhere to the provisions of the Technology Services security policy and ISPs may result in the following:

- Suspension or loss of access to institutional Technology Services resources
- Appropriate disciplinary action under existing procedures applicable to students, faculty, and staff, and
- Civil or criminal prosecution

Potential violations will be investigated consistent with applicable laws, regulations, and CC policies, standards, guidelines, and practices.

EXCEPTIONS TO ISP

Exceptions are granted on a case-by-case basis and must be reviewed and approved by the College designated IRM. The required ISP Exception Form and procedures can be found at https://www.collin.edu/security The IRM will mandate the documentation and additional administrative approvals required for consideration of each ISP exception request.

REFERENCE

Many individual laws, regulations, and policies establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the primarily applicable references are listed below.

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act of 2002 (FISMA)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Government Code, Title 5, Subtitle A, Chapter 552
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, § 37.10, Tampering with Governmental Record
- United States Code, Title 18, § 1030, Computer Fraud and Related Activity of 1986
- Copyright Act of 1976

- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B, 2054.075(b)
- Computer Software Rental Amendments Act of 1990
- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Texas Department of Information Resources (DIR) Practices for Protecting Information Resources Assets

Implementation Information

Review Frequency:	Annually
Responsible Person:	SVP – Campus Operations
Approved By:	Abe Johnson, Ed. D.
Approval Date:	02/09/2022

Revision History

Version:	Date:	Description:
1.0	02/09/2022	Initial document
1.1	10/28/2022	Annual Review – No Changes required.
1.1	11/07/2023	Annual Review – Minor Grammatical edits.