Panola College
Policy Compliance

PURPOSE

The purpose of this policy is to ensure an information technology infrastructure that promotes the mission of the college. Panola College (PC) information services network has been established for the use and benefit of PC in the conduct of its academic, business, and other operations. This document provides direction and support for the PC Information Security Program and the Information Technology Policies.

This framework of IT security policies collectively represents the basis of the institutional Information Security program and on the aggregate whole meet the objectives as articulated by Texas Administrative Code Chapter 202 (TAC§202), Texas Higher Education Coordinating Board (THECB) and the associated guidelines.

This policy promotes the following goals:

- To ensure the integrity, reliability, availability, and performance of PC information technology resources;
- To ensure that use of PC information technology resources is consistent with the principles and values that governs PC as a whole;
- To ensure that information technology resources are used for their intended purposes; and
- To ensure all individuals granted access privileges to PC information technology resources have a clear understanding of what is expected during use and the consequences of violating PC policies.

SCOPE

This program applies equally to all individuals granted access privileges to any Panola College (PC) information technology resources.

POLICY STATEMENT

Information technology resources play an integral part in the fulfillment of the primary mission of the college. Users of Panola's information technology resources have a responsibility to protect and respect those resources, and are responsible for knowing the regulations and policies that apply to appropriate use of the college's information technology resources.

Users must understand the expectation that if needed PC information technology resources may be limited and/or regulated by PC 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 the College's information resources expressly consents to monitoring of the network by the college at any time and for any purpose, including but not necessarily limited to, evidence of possible criminal activity, violations of law, contract, copyright or patent infringement, and/or violation of any college policy, rule, or regulation.

A review of the institution's information security program for compliance with these standards will be performed at least biennially, 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 his or her designated representative(s).TAC 202.76(c)

NON-CONSENSUAL ACCESS

Panola College cannot absolutely guarantee the privacy or confidentiality of electronic documents. Consequently, persons that use these PC-owned resources, or any personally owned device that may be connected to an PC resource, have no right to privacy in their use of these resources and devices. However, PC will take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons that PC 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 statutes, laws or regulations;
- Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;
- Protect the integrity of Panola College's information technology resources, and the rights and other property of PC;
- Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergency situations; or
- Protect the rights of individuals working in collaborative situations where information and files are shared.

VIOLATIONS

Failure to adhere to the provisions of the information technology security policies may result in:

- suspension or loss of access to institutional information technology resources
- appropriate disciplinary action under existing procedures applicable to students, faculty and staff, and
- civil or criminal prosecution

Potential violations will be investigated in a manner consistent with applicable laws and regulations, and Panola College policies, standards, guidelines and practices.

EXCEPTIONS TO POLICY

Exceptions are granted on a case-by-case basis and must be reviewed and approved by the College. The Director of Information Technology Services will mandate the documentation and additional administrative approvals required for consideration of each policy exception request.

REFERENCE

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State College Systems Rules and Regulations, Policy Guideline TSUS IT.02.01, Information Security Policy. The primary applicable references are listed below.

DIR Security Controls Catalog Control Group

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202)
- National Institute of Standards and Technology, Special Publication 800-171
  (NIST 800-171)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- 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 Electro-technical Commission (IEC)
- Texas Department of Information Resources (DIR) Practices for Protecting Information Resources Assets