Panola College
Security Incident Management Policy

PURPOSE:

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

The purpose of this Incident Response Policy is to establish a framework for identifying, containing, mitigating, and reporting privacy and security incidents in accordance with the Texas Administrative Code, Title 1, Chapter 202. This document sets forth the policy for incident management within Panola College (PC).

SCOPE:

- This policy applies to and must be complied with by all Panola College users.
- The user agrees to abide by this policy while employed or contracted with the College.
- Roles and responsibilities of each function pertaining to the protection of PC-owned systems and data are documented in PC policy via the Incident Response Team (IRT) Redbook.
- The user is responsible for understanding the terms and conditions of this policy. This policy is subject to change.
- This policy applies to any computing device owned or provided by PC. It also applies to any computing device regardless of ownership, which either is used to store PC-owned confidential or PC sensitive data or

that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data disclosure.

POLICY STATEMENT:

The Information Security Officer (ISO) is responsible for overseeing incident investigations in coordination with the Incident Response Team (IRT). The ISO shall recommend the IRT members to the Executive Council, via the Vice President of Instruction, for approval. (TAC§202.76)

The highest priority of the ISO and IRT shall be to identify, contain, mitigate, and report privacy or security incidents that fall under one or the following categories:

- Propagation to external systems
- Violation of applicable federal and/or state laws which will require involvement from law enforcement
- Potential modification or disclosure of confidential information as defined in the Data Classification policy.

The Panola College ISO shall notify appropriate individuals (which must include the State CISO and the State Cybersecurity Coordinator) within 48 hours if it is believed that personal information owned by PC has been used or disclosed by or for unauthorized persons or purposes. (TGC§2054.1125, TBC §521.053)

The ISO shall establish an Incident Criticality matrix (see page 4). This matrix will define each level of escalation, detail the appropriate response for various incidents, and establish the appropriate team participants. (TAC§202.71-72)

The ISO shall establish and document appropriate procedures, standards, and guidelines regarding incidents. (TAC§202.71)

The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation. Any electronic device containing data owned by PC may be subject to seizure and retention by the ISO.

The PC Chief of Police, Information Security Officer, or PC's General Counsel (as appropriate) will work directly with law enforcement regarding any incidents that may have violated federal or state laws. If an incident is determined to be the result of a privacy violation by a user, the ISO shall notify the user's supervisor and Human Resources of the violation(s), or the Inspector General's Office, as applicable, for appropriate action.

The ISO shall provide a summary report for each valid security incident to Executive Council within five business days after the incident has been closed.

DISCIPLINARY ACTION:

Management reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts the normal operation of agency information systems or violates state or federal law.

Any user who has violated PC security policies may be subject to disciplinary action, up to and including termination of employment or contract.

PC will cooperate with appropriate law enforcement if any user may have violated federal or state law.

PANOLA COLLEGE

INCIDENT CRITICALITY MATRIX

		Impact		
		High-System Wide Business Unit, Department, Location	**Medium-Multiple Users** Number of Users	**Low-Single User** Single User
Urgency	**High** Can no longer perform primary work functions	**Critical**	**High**	**Moderate**
	Medium Work functions impaired, the workaround in place	**High**	**Moderate**	**Low**
	Low Inconvenient	**Moderate**	**Low**	**Low**