KILGORE COLLEGE

Information Security

Information Security Policy

Approved by and date:

Board of Trustees	*06/17/2019*
Executive Leadership Team	*06/05/2019*

Policy:

Kilgore College's Information Security is governed by several federal and state laws. *Texas Administrative Code (TAC) 202 subchapter C* defines information security standards for institutions of higher education. TAC 202 requires that the College develop an Information Security Plan. The KC Information Security Plan also is intended to comply with the federal *Safeguards Rule*.

In accordance with this over-arching Information Security policy, where applicable, subject specific policies, procedures, standards, guidelines and controls will be established to support and maintain the Information Security Plan.

Procedures:

Approved by and date:

Executive Leadership Team	*06/05/2019*

Information Security Plan

Kilgore College takes data privacy and security seriously and has systems in place to protect its data. The Kilgore College Information Security Plan combines multiple security elements into a management framework that supports the objectives of confidentiality, integrity, and availability. The KC Information Security Plan is a living document that provides a strategic plan to achieve compliance with information security related laws and regulations.

The framework of the Plan is designed to:

a. Ensure the confidentiality, integrity, and availability of KC data.
b. Establish the governance and responsibilities for information security at KC.
c. Establish periodic risk assessments and develop risk mitigation plans.
d. Classify information and establish controls for each classification type.
e. Establish an ongoing security awareness education program for all users starting with new employees during the onboarding process.
f. Establish strategies to protect high-impact information resources.
g. Facilitate the development of policies, standards and procedures that include controls for:

    1) Data security risk management.
    2) Mitigation of information security risks to levels acceptable to College leadership.
    3) Information security throughout the life cycle of the information resource.

h. Develop processes to:

    1) Plan, implement, evaluate, and document remedial action to address any deficiencies in the information security policies, procedures, and practices.
    2) Justify, grant and document any exceptions to specific program requirements in accordance with requirements and processes.

Scope of the Information Security Plan

The Information Security Plan applies equally to any person granted access to Kilgore College information resources including:

a. All users employed by KC, contractors, vendors, or any other person with access to KC information technology resources.
b. Non-KC-owned computing devices that may store protected KC information.
c. All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
d. Information technology facilities, applications, hardware systems, network resources owned or managed by KC. This includes third party service providers' systems that access or store KC protected information.

   NOTE: Auxiliary organizations, external businesses and organizations that use college information technology resources must operate those assets in conformity with the KC Information Security Plan.

Information Security Plan Framework

The foundational elements that follow create a framework for the Information Security Plan that ensure continuity, performance and security of KC's information systems. A review of KC's Information Security Plan for compliance with required standards will be performed at least biennially based on business risk management decisions by individuals(s) independent of the Information Security Plan.

The elements outlined here will ensure appropriate safeguards are applied to KC's information systems and will be regularly reviewed and updated consistent with changing business environment and/or regulations.

a. Responsibility and Accountability.
b. Risk Management.
c. Security Awareness.
d. Business Continuity Plan.
e. Information Security Incident Response.
f. Physical Security.
g. Digital Data Disposition.
h. Enforcement.