INFORMATION SECURITY PLAN

INFORMATION SECURITY PLAN

SUMMARY

An Information Security Plan provides direction for managing and protecting the confidentiality, integrity, and availability of information resources, particularly highly sensitive or critical data. The plan contains administrative, technical, and physical safeguards to protect information assets. Controls include policies, processes, procedures, standards, guidelines, organizational structures, and supporting technology.

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 defines the requirements of the Information Security Plan, roles and responsibilities, and adoption of appropriate security controls. This Plan also is intended to comply with the federal Safeguards Rule.

This document establishes the purpose, scope, authority, organizational responsibilities, and foundational elements of the Information Security Plan for Kilgore College.

Table of Contents

INTRODUCTION

This document establishes Kilgore College's Information Security Plan and outlines objectives for managing, operating, and controlling information security activities. Where applicable, policies, procedures, standards, guidelines, and controls will be established to support and maintain the Information Security Plan. Policies serve as overarching rules for the use, management, and implementation of information security. Procedures, standards, and guidelines serve to define the methods for the protection of information assets. Defined controls provide a system of checks and balances intended to identify irregularities and prevent abuse.

The Information Security Plan contains administrative, technical, and physical safeguards to protect KC information resources. Measures shall be taken to protect these resources against accidental or unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, authenticity, and confidentiality of information.

GOAL

The purpose of the KC Information Security Plan is to provide the college community with a description of the strategic plan to achieve compliance with information security related laws and regulations. The framework is designed to:

1. Ensure the confidentiality, integrity, and availability of KC data.
2. Establish the governance and responsibilities for information security at KC.
3. Establish periodic risk assessments and develop risk mitigation plans.
4. Classify information and establish controls for each classification type.
5. Establish an ongoing security awareness education program for all users starting with new employees during onboarding process.
6. Establish strategies to protect high-impact information resources.
7. Facilitate the development of policies, standards, and procedures that include controls for:
    a. Data security risk management.
    b. Mitigation of information security risks to levels acceptable to College leadership.
    c. Information security throughout the life cycle of the information resource.
8. Develop processes to:

a. Plan, implement, evaluate, and document remedial action to address any deficiencies in the information security policies, procedures, and practices.

b. Justify, grant, and document any exceptions to specific program requirements in accordance with requirements and processes.

The Information Security Plan combines multiple security elements into a management framework that supports the objectives of confidentiality, integrity, and availability.

SCOPE

This program applies equally to any person/entity granted access to Kilgore College information resources including:

- All users employed by KC, contractors, vendors, or any other person with access to KC information technology resources.
- Non-KC-owned computing devices that may store protected KC information.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and 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 ROLES AND RESPONSIBILITIES

The following roles are defined with appropriate responsibilities and authorities regarding information security:

Information Resource Manager (IRM)

The Director of Information Technology (John Colville) is designated as the College's Information Resource Manager and is responsible for management of the College's information resources. The IRM is designated through appointment by the President. The IRM provides strategic direction, ensures objectives are achieved, ascertains that risks are managed appropriately, and verifies information resources are used responsibly. The IRM reports to the President, and is the designated representative for the College's information resources.

Information Security Officer (ISO)

The IT Report Writer (Larry Brooks) is designated as the College's Information Security Officer (ISO). The ISO reports to the Information Resource Manager. The ISO administers the College's Information Security Plan.

It shall be the responsibility of the Information Security Officer to:

- Develop, recommend, and maintain a campus-wide Information Security Plan.
- Develop and maintain information security policies and procedures that address security regulations and the College's information security risks.
- Work with the business and technical resources to ensure that controls are utilized to address all applicable security regulations and the College's information security risks.
- Provide guidance and assistance to College leadership, information owners, information custodians, and end users concerning their responsibilities.
- Ensure that annual information security risk assessments are performed and documented by information-owners.
- Develop and recommend policies and establish procedures and practices, in cooperation with the IRM, information owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.
- Coordinate the review of the data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data.
- Verify that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data.
- Report annually the status and effectiveness of security controls; and inform the campus departments, data owners, and data custodians in the event of noncompliance with Kilgore College's information security policies.
- Issue exceptions to information security requirements or controls with the approval of the IRM.

- Justify, document, and communicate any such exceptions as part of the risk assessment process.

Information Owner / Data Owner

A data owner is defined as an individual with statutory or operational authority for specific information or information resources. The data owner or designee is responsible for and authorized to:

- Classify information under their authority, with the approval of the IRM or designee, in accordance with KC's established information classification categories.
- Approve access and formally assign custody of information or an information resource.
- Specify data security control requirements and convey them to users and custodians.
- Confirm that controls are in place to ensure the confidentiality, integrity, and availability of data.
- Assign custody of information resources and provide appropriate authority to implement security controls and procedures.
- Periodically review access lists based on documented risk management decisions.
- Approve, justify, document, and be accountable for exceptions to security controls with the ISO.
- Participate in risk assessments.

Information Custodian / Data Custodian

An information custodian is defined as an individual, a department, agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource.

Data custodians shall:

- Implement controls required to protect information and information resources based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the Information Security Plan.
- Provide owners with information to evaluate the cost-effectiveness of controls and monitoring.

- Adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents.
- Provide information necessary for appropriate information security training to employees.
- Ensure information is recoverable in accordance with risk management decisions.

User / Information User / Authorized User

An information user is defined as an individual, process, or automated application authorized to access an information resource in accordance with federal and state laws, College policies, and the information owner's procedures and rules. The user of an information resource has the responsibility to:

- Use the resource only for the purpose specified by the institution or information owner.
- Comply with information security controls and College policies to prevent unauthorized or accidental disclosure, modification, or destruction.
- Formally acknowledge that they will comply with the security policies and procedures of Kilgore College.

Information Security Plan Reviewer

The Information Security Plan is reviewed by individual(s) designated by the Information Resource Manager that are independent of the program. The review is to be conducted biennially for compliance with applicable standards based on business risk management decisions. Outcomes of the review provide the basis for corrective action plans and the development of policies, procedures, and processes.

PROGRAM 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 should be reviewed and updated consistent with changing business environment and/or regulations.

Responsibility and Accountability

Data owners and their selected data custodians will be reviewed on an annual basis by the ISO. The data owners will review/identify the related data stored on their system and identify the categories of data stored as confidential, protected, or public according to the data classification standards found in **Appendix A**. Data owners will also review the list of authorized users for each system and implement required changes using the least privileged model.

The ISO will review and approve information ownership and responsibilities including personnel, equipment, hardware, and software, as well as define information classification categories.

Activity Description	Assigned Responsibility
Inventory of systems, data owners, and data custodians	ISO
Periodic review of access and authorization granted	Data owners
Implement controls	Data custodians
Respond to audits and inquiries	Data owners and custodians
Acknowledge policies and confidentiality	Authorized users

Risk Management

Risk management is the process of aligning information resource risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures. The risk management cycle includes assessment, review, mitigation, and reporting.

- Risk assessment is the process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls. Risk assessment also provides the documentation for evaluating and granting exemptions from security control requirements.

- Risk review is the process of evaluating the results of risk assessments and recommending activities to mitigate the risks.

- Risk mitigations are technical and/or procedural activities designed to reduce or eliminate the risks identified during assessment and review.

- Risk reporting is the process of reporting residual risks to the IRM and executive leadership.

Activity Description	Assigned Responsibility

Coordinate risk assessment activities	IRM or designee (IT Compliance)
Participate in risk assessment	Data owners and data custodians
Review assessment results and recommend remediation requirements	ISO
Mitigate identified risks	Data custodians
Grant exemptions to controls requirements based on risk assessments	ISO
Residual risk report	ISO

Security Awareness

Security awareness is a critical component of an Information Security Plan. All employees with access to KC information resources must participate annually in information security awareness training. Training promotes awareness of:

- KC information security policies, standards, procedures, and guidelines.
- Potential threats against college protected data and information resources.
- Appropriate controls and procedures to protect confidentiality, integrity, and availability of protected data and information resources.

New employees will sign a non-disclosure agreement and will be provided individual access to the Information Security Awareness Training Program. Employees are expected to complete training within 30 days of receiving the program, and then annually. Department heads and college leadership will be provided status of training compliance.

The ISO will maintain and operate an ongoing security awareness program as well as coordinate development and effective maintenance of communication and internal marketing strategies for information security awareness.

Business Continuity Plan

Business Continuity Plans (BCP) are developed and maintained with the objective of mitigating against loss and ensuring critical business and academic functions are sustained in the event that facilities, technologies, and/or other resources are unavailable due to an unforeseen disruption or event. It is crucial that KC formally develop an organizational Business Continuity Plan. The BCP ensures that the effects of a disaster will be minimized, and KC will be able to either maintain or quickly resume mission-critical functions.

Elements of a BCP specifically for information resources shall include:

- Business Impact Analysis including:
  - Mission Critical Information Resources
  - Disruption impacts and allowable outage times
  - Recovery priorities

- Risk Assessment.

- Implementation, testing, and maintenance management program for the plan.

- Disaster Recovery Plan.

Activity Description	Assigned Responsibility
Develop and maintain BCP (for IT)	IRM or designee (IT Compliance)
Develop and maintain applicable policy, process and procedures (for IT)	IRM or designee (IT Compliance)
Coordinate distribution of BCP (for IT)	IRM or designee (IT Compliance)
Implement and test of BCP (for IT)	IRM or designee

Information Security Incident Response

An information security incident is defined as an event that impacts or has the potential to impact the confidentiality, availability, or integrity of KC information resources. Having an effective incident response plan is essential in mitigating damage and loss. Proper handling of such incidents protects KC's information resources from future unauthorized access, misuse, or damage.

Activity Description	Assigned Responsibility
Develop and maintain incident response policy	ISO
Coordinate incident response activities	ISO
Develop and maintain incident response plan	ISO
Develop and maintain incident response procedures for: • Incident management • User reporting • State reportingISO	ISO

Physical Security

Physical security controls and secure areas are used to minimize unauthorized access, damage, and interference to information resources. Physical security includes providing environmental safeguards and controlling physical access to equipment and data.

Activity Description	Assigned Responsibility
Develop and maintain physical security policies	IRM or designee
Implement physical security procedures	Data custodians

Digital Data Disposition

The secure disposal of KC's digital data is a significant part of the information security posture. KC data can be stored on both printed media and on digital format. It is vital both these forms of data are disposed of securely to ensure confidentiality. In order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality, specific disposition methods for digital data must be adhered to.

Activity Description	Assigned Responsibility
Develop and maintain data disposition policy and standards	ISO
Implement data disposition standards	Data custodians

Enforcement

The ISO is authorized by the President to ensure that the appropriate processes to administer this program are in place, and are communicated to, and followed by the College community.

Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines, and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the ISO. Approved requests will be reviewed annually to determine if an exception is still warranted.

KC reserves the right to temporarily or permanently suspend, block, or restrict electronic access to college information resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of KC information resources; to protect KC from liability; or to enforce this policy and its related standards and practices.

Failure to adhere to the provisions of this policy statement or the appropriate use policy statement 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/or
- civil or criminal prosecution

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

The Information Resource Manager or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate College officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Third-party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to KC.

Appeals of College actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for KC students and employees.

APPENDIX A

Classification of Data

Information classification (data classification) is required to determine the relative sensitivity and criticality of information resources. This provides the basis for protection efforts and access control.

Kilgore College adopts a four-category classification: regulated, confidential, sensitive, and public. Although all data require some level of protection, particular data classifications are considered more sensitive and require tighter controls. The level of security required depends in part on the effect that unauthorized access or disclosure of data would have on operations, functions, reputation, assets, or privacy of individual members of the KC community.

The Data Classification Standard outlines the minimum controls for protection of classified KC information. Additional controls may be required under applicable laws, regulations, or standards governing specific types of data (e.g., health or financial information, credit card data).

Activity Description	Assigned Responsibility
Develop and maintain data classification policy and standard	ISO
Develop and maintain applicable control standards	ISO
Classify data	Data owners
Implement controls	Data custodians

APPENDIX B

Compliance References

Kilgore College Information Security Plan and practices must comply with several federal and state laws, as well as Kilgore College policies. While it is not possible to list all potentially applicable laws and regulations, this list references the most relevant ones that must be complied.

1. The Federal Family Educational Rights and Privacy Act (FERPA).
2. Health Insurance Portability and Accountability Act (HIPAA).
3. Gramm-Leach-Bliley Act (GLBA).
4. Texas Administrative Code, Title 1, part 10, Chapter 202, Subchapter C (pending).
5. Texas Medical Records Privacy Act.
6. Texas Government Code, Chapter 2054 - Information Resources.
7. Texas Government Code, Chapter 2059 - Texas Computer Network Security System.

APPENDIX C

Definitions

Availability – Ensuring that information systems and the necessary data are accessible for use when required.

Business Continuity Plan – A plan to ensure that the essential business functions of the organization are able to continue (or restart) in the event of unforeseen circumstances.

Confidentiality – Assurance that information is shared only among authorized persons or organizations.

Disaster Recovery Plan – Assurance that a documented process or set of procedures to recover and protect a business IT infrastructure is in place in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster.

Information Resource – Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors. Information Resources of Kilgore College include, but are not limited to the following:

- All components of the Kilgore College information network, both physical and logical.
- Any device owned by Kilgore College or used to connect to the Kilgore College network. These devices include computers (both stationary and mobile), printers, and communication devices.
- All software purchased by or used to support Kilgore College.
- All electronic data, including email, and the storage media on which the data resides (both stationary and mobile).
- Kilgore College credentials used to access licensed external resources.

Information Security – The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction.

Information Security Plan – Plan that contains administrative, technical, and physical safeguards to protect information resources.

Integrity –Accuracy and consistency of data over the entire life–cycle.

Mitigate – An effort to reduce loss by making a deficiency less severe and lessening the impact of potential damages.

Remediate – The act or process of correcting a fault or deficiency.

Risk – The likelihood that something will occur and cause harm to, or loss of, an information asset.

Risk Assessment – A systematic process of evaluating potential risk and impact from disruption of information resources.

Security Incident – A computer, network, or paper based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

Threat – Anything that has the potential to cause harm.

Vulnerability – A weakness that could be exploited to endanger or cause harm to an information resource.

Vulnerability Assessment – The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.