Information Technology

Table of Contents

Policy Title: **Information Security Policy**
Policy Number: **7.0**

Purpose:
This Information Security Policy (this **Policy**) defines the role of information security in supporting the College's mission, while fostering an environment to protect the College community from all internal, external, deliberate, or accidental information security threats that may compromise the confidentiality, privacy, and integrity of Institutional Resources.

This Information Security Policy provides the basis for defining and regulating the management of information systems and other information assets. Adhering to these principles is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, privacy, and integrity that would otherwise occur.

Definitions:

1. **Authorized Users** means anyone who is authorized to access and use Institutional Resources.
2. **College** or **EWC** means Eastern Wyoming College and all campuses, departments, offices, and units affiliated with Eastern Wyoming College.
3. **Confidential (Level 2)** has its meaning set forth in Administrative Regulation 7.0.1 Information Classification.
4. **Contractor** means a person officially attached or connected to the College who is not a student or Personnel (e.g., contractors, consultants, vendors, interns, temporary staffing).
5. **Highly-Sensitive (Level 3)** has its meaning set forth in the Administrative Regulation 7.0.1 Information Classification**.**
6. **Information Technology Resources** or **IT Resources** means any information technology resources owned or managed by the College, or hosted or managed on behalf of the College, including without limitation, networks, servers, websites, applications, and machines.
7. **Institutional Data** means any information or data, personal or non-personal, regardless of format or location, that is (1) substantive and relevant to the planning, managing, operating, documenting, staffing, or auditing of one or more functions of the College; (2) subject to a legal obligation requiring the College to secure the data; (3) clinical data or research data of the College or its personnel; or (4) used to derive any data element that meets the above criteria.
8. **Institutional Resources** means all information assets of the College, including IT Resources and Institutional Data.
9. **Mission Critical Systems** means Institutional Resources that are essential to the operation of the College.
10. **Non-Public** means any Institutional Data or Institutional Resource that is not classified as Public (Level 1) according to Administrative Regulation 7.0.1 Information Classification.
11. **Personally Identifiable Information** or **PII** means any data or information that alone or in combination with other information can identify, or be used to reasonably identify, an individual.
12. **Personnel** means any individual who works for or on behalf of the College, including, without limitation, faculty, academic advisors, staff, and advisors.
13. **Public (Level 1)** has the meaning set forth in Administrative Regulation 7.0.1 Information Classification.

14. **Visitor** is defined as anyone not enrolled at or employed by the College and can include, but are not limited to, non-registered students, friends, spouses, children, guest speakers and College sanctioned event participants.

Scope:

The College's Information Security Policy encompasses the following policies:

- Board Policy 7.0 Information Security
- Board Policy 7.1 Graham-Leach-Bliley Act (GLBA)
- Board Policy 7.2 Accessibility
- Board Policy 7.3 Acceptable Use
- Board Policy 7.4 Visitor - Use of Institutional Resources
- Board Policy 7.5 Security Awareness Training
- Board Policy 7.6 Electronic Communications
- Board Policy 7.7 Emergency Notification
- Board Policy 7.8 Enforcement
- Board Policy 5.7 Family Education Rights and Privacy Act (FERPA)

The College's Information Security Policy encompasses the following administrative regulations:

- Administrative Regulation 7.0.1 Information Classification
- Administrative Regulation 7.0.2 Business Continuity and Disaster Recovery
- Administrative Regulation 7.1.1 Risk Management
- Administrative Regulation 7.1.2 Vulnerability Management
- Administrative Regulation 7.1.3 Data Backup
- Administrative Regulation 7.1.4 Authentication and Access Control
- Administrative Regulation 7.1.5 Monitoring and Logging
- Administrative Regulation 7.1.6 Incident Response

This Information Security Policy, which encompasses the GLBA Policy and FERPA Policy, lists a set of policies and administrative regulations, which together constitute the Information Security Program of the College. If any inconsistency is found between this overarching Policy and any of the referenced policies or administrative regulations, the overarching Policy will take precedence. Each of the administrative regulations contains high-level descriptions of requirements and principles. The administrative regulations do not and are not intended to include detailed descriptions of regulation implementation. Such details will, where necessary, be supplied in the form of separate procedural documents.

Within the College's IT environment, additional regulations may apply to specific computers, computer systems or facilities, software applications, databases and data sources, data types, or networks, and to the uses thereof, or to local workplaces or specific types of activities (collectively, **Local Regulations**). Local Regulations must be consistent with policies and administrative regulations, but also may impose additional or more specific requirements or responsibilities on users.

Policy:

The Board of Trustees mandates the College to adhere to the establishment of its information security policies and administrative regulations in conformance with various applicable regulations and laws. To ensure an effective information security program is maintained, compliance with the policies, administrative regulations, and laws is mandatory. All Personnel, Contractors, students, and Visitors are expected to comply with all federal, state, and local laws pertaining to the protection of Non-Public

information, as well as campus policies and administrative regulations meant to protect the security of information systems.

Institutional Resources are available to College Personnel, students and, in a limited number of cases, Contractors, Visitors, and the public. Use of all such Institutional Resources are subject to the standards set forth in College policies and administrative regulations.

In general, every individual is responsible for:

- Being aware of and practicing safe computer hygiene, including maintaining the confidentiality of username and passwords, ensuring browsing occurs on protected networks, and properly disposing of physical and electronic documents containing Non-Public information.
- Paying attention to unexplained system behavior and unsolicited requests for information.
- Watching for inappropriate conduct from all employees and Visitors.

Governance:
Responsibility for the production, maintenance, and communication of this overarching Policy and all related policies and administrative regulations resides with the EWC President who may delegate that duty to the College's Chief Information Officer (**CIO**).

The College establishes, publishes, maintains, and disseminates this Policy to all relevant Personnel, Contractors, students, vendors, and other partners of the College. The Policy is reviewed at least annually, and updates are made, as applicable, based on changes to the College's environment or applicable laws, regulations, or industry standards.

- The College may audit networks and systems on a more frequent basis to ensure compliance with this Policy. Instances of non-compliance are presented to, reviewed, and approved by the CIO.
- All breaches of information security, actual or suspected, must be reported to and investigated by the CIO and/or his designee as set forth in the Incident Response Administrative Regulation.

Enforcement:
Those who violate this Policy, whether knowingly or unknowingly, may be subject to the following enforcement actions:

1. Forced compliance with the Policy
2. Disciplinary action, including termination of employment, if a Contractor or Personnel;
3. Disciplinary action, including expulsion from the College, if a student;
4. Suspension or termination of rights to access Institutional Resources;
5. Termination of vendor contract and or service agreement;
6. Prosecution to the fullest extent of the law; and
7. Other actions deemed appropriate by the College.

References: Federal Education Rights and Privacy Act (FERPA), §20 U.S.C. § 1232g; 34 CFR Part 99
National Institute of Standards and Technology (NIST), Special Publication 800-171, Rev. 2
Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809, §§ 6821-6827

Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Administrative Regulation Title: **Information Classification**
Regulation Number: **7.0.1**

Purpose:
This Information Classification Administrative Regulation (this "**Admin Reg**") establishes a framework for classifying and managing Institutional Data. Data is classified as public, confidential, and highly-sensitive based on applicable law, the sensitivity of the data, and how critical the data is to the College's operations. This criteria aids in developing and implementing security controls, which are proportionate to the classification of the data, to ensure confidentiality, integrity, and availability of data are maintained. In the event of a security incident, data classification is a vital component in prioritization of remediation efforts and allocation of resources. Institutional Data is a vital asset to the College; therefore, proper data classification and management are essential to the mission and operation of the College.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

Scope:
This Admin Reg applies to all persons or entities that have access to Institutional Data and to all Institutional Data collected, stored, or maintained by administrative, academic, or other units, Personnel, or agents of the College, regardless of its source, where it resides, or whether it is in digital or non-digital form (except as otherwise permitted or required by statute or contractual obligations).

Classification Levels:
All Institutional Data are classified into three categories: Public (Level 1), Confidential (Level 2), or Highly Sensitive (Level 3). The level of classification is determined by the impact to the individual and/or to the College if such data is compromised, whether by unauthorized disclosure, modification, or destruction of the data or loss of access to data or systems. Descriptions and examples related to each classification level are provided in the chart below.

Based upon how the data are classified, certain data management standards and security controls will need to be taken for the secure handling of such data. Director/Department Heads, under guidance of the Chief Information Officer, are responsible for determining which classification applies to specific data. If it is unclear which classification is appropriate, (Default level for data classification is Level 3.), then the highest classification of those being considered will apply. Derivative data shall have the same classification level as the data on which it is derived, unless the creator of the derivative data can show that the aggregated and anonymized derivative data presents a lower degree of risk in the event such data is made public.

Classification Levels			
Criteria	**Public (Level 1)**	**Confidential (Level 2)**	**Highly Sensitive (Level 3)**
Level of Impact if Compromised	Low adverse effects on the College or individuals	Moderate adverse effects on the College or individuals	Serious adverse effects on the College or individuals
Data that Generally Fall into the Classification	Information that may or must be open to the public and is not restricted by local, state, national, or international regulations regarding use or disclosure	Information whose access must be guarded due to proprietary, ethical, or privacy considerations and that is not intended for public dissemination, but whose disclosure is not restricted by law	Information protected by law, including, without limitation, the Family Educational Rights and Privacy Act ("**FERPA**"), Health Insurance Portability and Accountability Act ("**HIPAA**"), Gramm-Leach-Bliley Act ("**GLBA**"), Payment Card Industry Data Security Standard ("**PCI DSS**"), and Wyo. Stat. § 40-12-502(d)(iii) & (iv)
Potential Impacts of Loss of Confidentiality, Integrity, or Availability	• No or very limited degradation in or loss of mission capability – the College is able to perform its primary functions, but the effectiveness of the functions may be reduced • No or very minor damage to College assets • No direct financial damages or fines • Insignificant indirect financial damages • Insignificant harm or inconveniences to individuals • Possible negative impact on College's reputation, generally dependent on the visibility of the loss of confidentiality,	• Limited degradation in or loss of mission capability – the College is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced • Minor damage to College assets • Minor direct financial damages and/or fines • Minor indirect financial damages • Minor harm to individuals • Minor negative impact on the College's reputation	• Severe degradation in or loss of mission capability to an extent and duration that the College is not able to perform one or more of its primary functions • Major damage to College assets • Major direct financial damages and/or fines • Major indirect financial damages • Significant harm to individuals • Major negative impact on the College's reputation

	integrity or availability		
Examples of Data	• Published "white pages" • Directory information • Maps • Departmental websites • Lists of email addresses • Academic course descriptions • Other information readily published and provided to the public at large	• Student grades maintained by an instructor • Class lists • Lists of students in a major in a department • Internal memos • Financial records • Email communications • Other documents not intended for public distribution that are not otherwise Level 3 data	• Credit card numbers • Social security numbers • Driver's license numbers • Health records • Student transcripts • Financial aid data • Human subject research data that identify an individual • Credentials used as passwords, passphrases, or fingerprints and the data stored to allow self-service reset of the credentials

Management and Security:
Data is managed based on its classification level. This Admin Reg, and those policies, regulations, and procedures referenced in the Information Security Policy, make up the College's overall information security framework, which provides guidance on how Institutional Data is collected, handled, stored, and destroyed.

This Admin Reg will be reviewed and, if applicable, updated at least annually.

References:
Information Security Policy

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Administrative Regulation Title: **Business Continuity and Disaster Recovery**
Regulation Number: **7.0.2**

Purpose:
This Business Continuity and Disaster Recovery ("**BC/DR**") Administrative Regulation (this "**Admin Reg**") ensures the College is prepared to restore mission critical systems in the case of a disaster to minimize disruption to business operations. BC/DR planning ensures that system dependencies have been identified and accounted for when developing the recovery prioritization, establishing recovery time and recovery point objectives, and documenting the roles of supporting Personnel.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

"**Business Continuity**" means an organization's ability to continue essential operations and services in the face of disruptive events by implementing measures such as viable backup and recovery procedures.
"**Disaster Recovery**" means the ability to restore an organization's critical systems and services to return the entity to an acceptable operating condition following a catastrophic event by activating a Disaster Recovery Plan. Disaster recovery is a subset of business continuity planning.
"**Recovery Point Objective**" or "**RPO**" means the maximum amount of data loss acceptable due to a disaster, expressed as a period of time. RPOs for each confidentiality classification are listed in Table 1.
"Recovery Time Objective" or **"RTO"** means the maximum time period in which critical business operations must be restored in order to avoid unacceptable consequences associated with a break in service. RTOs for each confidentiality classification are listed in Table 1.

Scope:
This Admin Reg applies to all Institutional Resources and Personnel who have responsibilities related to the availability of Institutional Resources.

Roles and Responsibilities:
Preparation for, response to, and recovery from a disaster affecting administrative functions require the cooperative efforts of many functions of the College. In conjunction with functional leads of departments throughout the College, the Office of Information Technology ("**OIT**") is responsible for maintenance of BC/DR plans. College leadership is accountable for ensuring plans are adequate and effectively carried out in the case of disaster.

Standards:
The College will develop and maintain a BC/DR process that identifies Institutional Resources and will implement, at minimum:

- Documented BC/DR plans for Institutional Resources;
- Storage of BC/DR plans in multiple secure and geographically diverse locations, when possible, ensuring their availability and resilience during disruptive disaster events;
- Briefing of Personnel on their roles and responsibilities related to BC/DR plans, including developing, updating, and testing plans, conducted by team leads that maintain, and are responsible for, Institutional Resources; and
- Requirements that team leads who manage Institutional Resources ensure sufficient financial, personnel, and other resources are available to maintain technological BC/DR plans.

The College will review the BC/DR process annually.

The following recovery maintenance activities must be conducted at minimum annually, when a significant change to Institutional Resources occurs, or when a new Institutional Resource is implemented:

- Review the BC/DR objectives and strategy;
- Update/create BC/DR plans;
- Update/create the internal and external contacts lists;
- Conduct recovery test(s);
- Verify the alternate site(s), if applicable; and
- Verify the hardware platform, applications, and operating system requirements, if applicable.
- (Optional) Conduct BC/DR simulation/tabletop exercise(s).

BC/DR plans should reference and incorporate related College information security policies and administrative regulations, including, without limitation:

- Data Backup: This Admin Reg ensures data that is lost or compromised can be restored.
- Information Classification: This Admin Reg provides the framework used to classify information based on criticality. The classifications should be used to guide the development of related business continuity and disaster recovery plans.
- Incident Response: This Admin Reg outlines how the College responds to security incidents and should work hand-in-hand with business continuity and disaster recovery plans.

Table 1: Disaster Recovery Performance Objectives by Information Confidentiality Classification

Level	RPO	RTO	Performance Objective
Highly Sensitive (Level 3)	24 hours	8 hours	Best possible performance, required robust real-time transaction speed monitoring
Confidential (Level 2)	24 hours	24–48 hours	Better performance, some transaction monitoring
Public (Level 1)	1–7 days	7–30 days	No performance targets, not monitored

References:
Information Security Policy
Data Backup Administrative Regulation
Information Classification Administrative Regulation
Incident Response Administrative Regulation

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Policy Title: **Graham-Leach-Bliley Act (GLBA) Policy**
Policy Number: **7.1**

Purpose:
This GLBA Policy (this **Policy**) summarizes the College's comprehensive written information security program (the Program) mandated by the Federal Trade Commission's (FTC) Safeguards Rule and the Gramm-Leach-Bliley Act (GLBA).

In particular, this Policy describes the Program elements by which the College (i) ensures the confidentiality, integrity, and availability of covered records; (ii) protects against anticipated threats or hazards to the security of such records; and (iii) protects against the unauthorized access or use of such records that could result in substantial harm or inconvenience to the College or associated individuals. The Program incorporates by reference the College's policies and administrative regulations enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, the Family Educational Rights and Privacy Act (FERPA).

Definitions
Capitalized terms not defined in this Policy have the meaning set forth in the Board Policy 7.0 Information Security.

1. **Customer Information**
   Means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, which is handled or maintained by or on behalf of you or your affiliates. In the case of the College, students are considered "customers."

2. **Encryption**
   Means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

3. **Information Security Program**
   Means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Customer Information.

4. **Information System**
   Means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing Customer Information or connected to a system containing Customer Information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains Customer Information or that is connected to a system that contains Customer Information.

5. **Multi-factor Authentication**
   Means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics.

6. **Nonpublic Personal Information**
   Means: (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

7. **Penetration Testing**
   Means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside College Information Systems.

8. **Security Event**
   Means an event resulting in unauthorized access to, or disruption or misuse of, and Information System, information stored on such Information System, or Customer Information held in physical form.

9. **Service Provider**
   Means any person or entity that receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services directly to a financial institution that is subject to this part.

Scope:
The Program applies to Nonpublic Personal Information about a customer of the College contained in any record, whether in paper, electronic, or other form, which is handled or maintained by or on behalf of the College or its affiliates. For these purposes, the term Nonpublic Personal Information shall mean any information: (i) a student provides in order to obtain a financial service from EWC, (ii) about a student or other third party resulting from any transaction with EWC involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Policy:
The College will protect, to the extent reasonably possible, the privacy, security, and confidentiality of personally identifiable financial records and information. This Policy applies to all personally identifiable financial records and information and covers Personnel, Contractors, and all other individuals or entities using these records and information for any reason. This Policy also establishes an expectation that members of the College community act in accordance with this Policy, relevant laws, contractual obligations, and the highest standards of ethics.

Elements of the Program:
1. **Designation of Representatives**: EWC's Chief Information Officer (CIO) is designated as the Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of EWC to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his/her designees.

2. **Risk Identification and Assessment**. EWC recognizes that it is exposed to both internal and external risks including, but not limited to:
   - Misuse or unauthorized access of Nonpublic Personal Information

- Compromised system security
- Interception of data during transmission
- Loss of data and data integrity

EWC, as part of the Program, will undertake to identify and assess reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of Nonpublic Personal Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and assess the sufficiency of safeguards in place to control those risks. The risk assessment will be written and will include criteria for evaluating risks and threats. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of EWC's operations.

The Program Officer shall periodically perform risk assessments that reexamine the reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of nonpublic personal information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and reassess the sufficiency of any safeguards in place to control those risks.

1. **Design and Implement Safeguards**. The risk assessment and analysis described above shall apply to all methods of handling or disposing of Nonpublic Personal Information, whether in electronic, paper or other form. The Program Officer will, on a regular basis, design and implement safeguards to control the risks identified through such assessments by:

    a. Implementing and periodically reviewing access controls. EWC will determine and periodically reevaluate who has access to Customer Information and whether such authorized user has a legitimate business need for it.

    b. Knowing what EWC has and where it is. EWC will conduct a periodic inventory of data, noting where it's collected, stored, or transmitted.

    c. Encrypting Nonpublic Personal Information in transit and at rest. EWC will protect data classified as confidential and highly sensitive as defined in the Information Classification Administrative Regulation by encrypting it in transit and at rest.

    d. Assessing applications. EWC will, to the extent applicable, adopt secure development practices for developing its own applications to store, access, or transmit Nonpublic Personal Information and implement procedures for evaluating the security of third-party applications EWC utilizes to transmit, access, or store Nonpublic Personal Information.

    e. Implementing Multi-factor Authentication for users authorized to access Nonpublic Personal information on the College's system.

    f. Disposing of Nonpublic Personal Information securely. EWC will dispose of Nonpublic Personal Information no later than two years after the most recent use of it to serve the customer, in compliance with the State of Wyoming Document Retention Schedule, or as required by applicable law. The Program Officer or his/her designee will periodically review EWC's data retention schedule to minimize the unnecessary retention of data.

g. Anticipating and evaluating changes to EWC's system or network. EWC's change management procedure is designed to provide a safe and orderly process for making changes that may affect EWC's systems and networks.

h. Maintaining a log of Authorized User's activity and detecting unauthorized access. EWC will implement procedures and controls to monitor when Authorized Users are accessing systems that contain Nonpublic Personal Information and detect unauthorized access.

2. **Monitor and Test Safeguards**. EWC will regularly test its procedures for detecting actual and attempted attacks.

   For Information Systems, testing may be accomplished through continuous monitoring of the system and/or through annual Penetration Testing, as well as vulnerability assessments, including system-wide scans every six (6) months designed to test for publicly known security vulnerabilities.

   In addition, EWC will conduct testing of its environment whenever there are material changes to its operations or business arrangements and whenever there are circumstances EWC knows or has reason to know may have a material impact on the College's Program.

3. **Train Staff**. EWC will ensure its staff are able to enact its Program by:
   a. Providing security awareness training that is updated as necessary to reflect risks identified by the risk assessment; (Security Awareness Training Policy)
   b. Utilizing qualified information security personnel either employed by EWC or an affiliate or Service Provider sufficient to manage its security risks and to perform or oversee the Information Security Program;
   c. Providing information security personnel with security updates and training sufficient to address relevant security risks; and
   d. Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

   Oversee Service Providers. Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that EWC determines not to provide on its own.

   The Program Officer will coordinate with those responsible for the third-party service procurement activities among the IT Department and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those Service Providers that are capable of maintaining appropriate safeguards for Nonpublic Personal Information of students and other third parties to which they will have access.

   In addition, the Program Officer will work with EWC's legal counsel and/or other designated institutional officials to develop and incorporate standard, contractual protections applicable to third-party Service Providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of EWC legal counsel and/or other designated institutional official.

The Program Officer will periodically assess third-party Service Providers based on the risk they present and the continued adequacy of these safeguards.

4. **Adjustments to Program**. The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the EWC's operations or other circumstances that may have a material impact on the Program.

5. **Create a Written Incident Response Plan**. The Program Officer shall oversee the development of a written incident response plan designed to promptly respond to and recover from, any security event potentially resulting in unauthorized access to or misuse of information stored on EWC's system or maintained in physical form.

   The incident response plan will address the following areas:

   a. The goals of the plan;
   b. The internal processes for responding to a security event;
   c. Clear roles, responsibilities, and levels of decision-making authority;
   d. Communications and information sharing both inside and outside EWC;
   e. A process to fix any identified weaknesses in EWC's systems and controls;
   f. Procedures for documenting and reporting security events and EWC's response; and
   g. The evaluation of the security event and a revision of the incident response plan and Program based on what is learned.

6. **Program Officer to report to Board of Trustees**. The Program Officer will at least annually provide a written report to the EWC Board of Trustees that will include: 1) an overall assessment of EWC's compliance with its Information Security Program, and 2) specific topics related to the Program, including risk assessment, risk management and control decisions, Service Provider arrangements, test results, Security Events and how EWC responded, and recommendations for changes in the Information Security Program.

References:
Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809, §§ 6821-6827 Federal Education Rights and Privacy Act (FERPA), §20 U.S.C. § 1232g; 34 CFR Part 99

Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Administrative Regulation Title: **Risk Management**
Regulation Number: **7.1.1**

Purpose:
This Risk Management Administrative Regulation (this "**Admin Reg**") sets forth the information security risk management standards of the College (the "**Risk Management Program**"). Identifying, assessing, and mitigating risks are essential for safeguarding Institutional Resources. The Information Security Policy requires all departments in the College to follow the Risk Management Program in their management, use, and maintenance of Institutional Resources. The Risk Management Program allows for identified risks to be assigned a numerical score based on the impact of such risk and the probability such risk will occur.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

Scope:
This Admin Reg applies to all Institutional Resources and the Personnel involved in management and maintenance of such resources.

Roles and Responsibilities:
The College's Chief Information Officer ("**CIO**") is responsible for creating and managing the Risk Management Program, and coordinating the development and maintenance of program policies, procedures, and standards, including the risk assessment methodology ("**RAM**"). Personnel who manage and maintain Institutional Resources are responsible for following the established risk management standards.

Overview of Risk Management Standards:
The Office of Information Technology ("**OIT**") will work with Personnel to periodically assess the risk to the College and its assets resulting from the operation of IT Resources and processing, storage, or transfer of Institutional Data. Assessments will include analysis of the threats to and vulnerabilities of Institutional Resources, likelihood that such threats or vulnerabilities will be exploited, and potential impact of any such exploitation. Analysis will consider threats and vulnerabilities related to internal assets and entities as well as external entities (i.e., service providers, others acting on behalf of the College, etc.). Risk assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to the College, and the results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls to protect against such risks.

Risk Management Program:
Risk management is an ongoing lifecycle that includes the following steps

Step 1. Categorize
Categorize the IT Resource and/or Institutional Data processed, stored, and transmitted by that resource based on sensitivity and risk of harm to individuals and the College if the information is subject to a breach or unauthorized disclosure, in accordance with the Information Classification Administrative Regulation.

All IT Resources that create, process, store, or transmit Confidential (Level 2) or Highly Sensitive (Level 3) data must be assessed for risk to the College that results from threats to the integrity, availability, and confidentiality of the data. Within the NIST framework, security controls are added or removed based on the data classification level.

Step 2. Select
Select an initial set of baseline security controls based on the classification levels.

Step 3. Assess
Assess the extent to which security controls are correctly implemented, operating as intended, and producing the desired outcome.
The core elements of a risk assessment (utilizing the RAM or other approved methodology) include:

- Scope of assessment;
- Current state of security control implementation;
- Documentation of identified threats, vulnerabilities, and risks associated with the resource; and
- Mitigation recommendations to reduce risks and threat potential to the resource.

Risk assessments for IT Resources that create, store, process, or transmit Confidential (Level 2) or Highly Sensitive (Level 3) data are required to be conducted under the following circumstances:

- After a major architectural change to the resource;
- Soon after a serious IT security incident is reported; and/or
- When required by regulation or law.

OIT may prioritize assessment schedules based upon data classification, institutional priorities, compliance requirements, or contractual obligations.

The chart below summarizes requirements for risk assessments by classification level:

Data Classification Level	Required or recommended	Risk Assessment Frequency
Highly Sensitive (Level 3)	Required	As defined by regulation
Confidential (Level 2)	Required	As defined by regulation, after new system implementation, or after major system change
Public (Level 1)	Recommended	After new system implementation or after major system change

Assessment Outcomes:
All risk assessment outcomes must be provided to OIT. Once a risk has been identified, using the Risk Matrix in Appendix A, OIT will work with relevant Personnel to assign the threat an impact category and likelihood score that are used to determine the threat's risk matrix score. The risk matrix score allows for all risks to be evaluated equally in order to appropriately assign resources for mitigation. OIT and relevant Personnel will then work together to develop and implement risk mitigation actions and

strategies to reduce the risk to acceptable levels. Risk Treatment Plans (described below) provide the structure for actively managing identified risks.

Risk assessments are considered IT security data classified as Confidential (Level 2) and should be maintained as confidential records and made available only to designated Personnel and others with job-related responsibilities.

Step 4. Implement

Implement the appropriate risk-reducing controls as identified by the risk assessment process.
A Risk Treatment Plan is provided as soon as possible after completing the risk assessment (within two weeks wherever possible). This is an action plan that requires the assessed area to review all security control recommendations and either: (a) agree to mitigate as stated; or (b) propose alternative or revision to specific control recommendation(s). Plans must be reviewed and accepted by applicable leadership within two months after receipt of the plan.

Components of risk treatment plans include:

- Applicable risk matrix score(s);
- Description of security control recommendation(s);
- Primary Personnel responsibility for each recommendation;
- Estimated financial costs, time, and staffing resources to carry out identified mitigation recommendations, including estimated start and completion dates; and
- Metrics to evaluate progress and success.

In general, risks identified by a risk assessment and included in a Risk Treatment Plan must be mitigated or accepted on a priority basis within the following timeframes:

- 60 days to create remediation plan; and
- 180 days to address findings, with timeframes running concurrently.

Non-trivial changes to Risk Treatment Plans, once adopted, must be documented and approved by applicable leadership.

Identified risks must be addressed by one of the following:

- Implementing identified control(s) (information security risk mitigation);
- Sharing or shifting the risk to another party (information security risk transference); or
- Assuming or accepting the identified risk (information security risk acceptance).

Step 5. Evaluate

Evaluate whether an identified but unmitigated risk is acceptable.
In general, Personnel may not unilaterally accept any information security and compliance risk that results in the College's vulnerability to cyber risks. Specifically:

- Risks that are given a risk matrix score of 15 (See Appendix A), but not mitigated in an established timeframe may only be accepted on behalf of the College by applicable leadership with the acknowledgement of the CIO, in writing.
- Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance on behalf of the College cannot be delegated.

Step 6. Monitor and Follow-up
OIT will follow up with departments and Personnel on an ongoing basis to ensure and track progress of open Risk Treatment Plan items.

References:
Information Classification Administrative Regulation
Information Security Policy

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Appendix A: Risk Matrix

Impact Category				
1 - Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
• Brief disruption to service delivery • IT services not available for less than 2 hours • Data loss isolated to one or a very small group of people affected • Financial implications are negligible	• Some disruption to service delivery of up to 24 hours • IT services not available for up to 8 hours • Small to medium group of people affected by data loss • Some financial implications	• Disruption to service delivery of up to 48 hours • IT services not available for up to 48 hours • Large group of people affected by data loss • Moderate financial implications	• Unable to deliver services for more than one week • IT services not available for more than one week • Significant group of people affected by data loss • High financial implications	• Rebuilding of foundational systems required • IT services not available for more than one month • Very high financial implications • Brand tarnished to the extent that re-branding may be necessary

Likelihood Score	1	2	3	4	5
Probability	Rare	Unlikely	Possible	Likely	Certain
Frequency	Expected no more than once every other year	Expected every year	Expected every month	Expected weekly	Expected daily

Risk Matrix Score					
Impact	Likelihood				
	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Certain
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	8	12	15
2 Minor	2	4	6	8	10
1 Insignificant	1	2	3	4	5

Administrative Regulation Title: **Vulnerability Management**
Regulation Number: **7.1.2**

Purpose:
This Vulnerability Management Administrative Regulation (this "**Admin Reg**") outlines the framework for identifying, assessing, and remediating vulnerabilities on devices connected to the College's networks. Vulnerabilities within networks, software applications, and operating systems, whether due to server or software misconfigurations, improper file settings, or outdated software versions, are an ever-present threat. Vulnerability management is a critical component of the College's information security program and is essential to help reduce the College's potential financial, reputational, and regulatory risks.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

Scope:
This Admin Reg applies to all College-owned and managed networks (public and private) and all devices that connect to or access those networks, including, but not limited to, computer workstations and servers, network switches and routers, networked printers, scanners, copiers, digital telecommunications, and personally owned devices.

Vulnerability scanning is limited to reviewing IT system and application configuration and does not open or review content found in emails or digital documents.

Roles and Responsibilities:
The Office of Information Technology ("**OIT**") works with Personnel who manage Institutional Resources throughout the College to determine appropriate vulnerability scanning and remediation.

The Chief Information Officer ("**CIO**") is authorized by the College's executive officers to take action, as needed, to ensure that unremediated systems or applications do not pose a threat to Institutional Resources. When a critical vulnerability is not remediated within a required timeframe or is improperly remediated, the CIO may temporarily block the system or application from the network until such time as the remediation is effectively completed.

Vulnerability Management Standards:
Vulnerability scanning is a task that identifies software vulnerabilities, missing system patches, and improper configurations. Regular vulnerability scanning along with the timely and consistent application of vendor-supplied security patches or other mitigation of a reported vulnerability are critical components in protecting Institutional Resources from damage or loss and in meeting regulatory and compliance requirements.

Vulnerability assessment provides visibility into the vulnerability of systems and hosted applications deployed on the College's network. Used effectively, vulnerability management helps to ensure that software, settings, and security configurations are kept up-to-date. Further, systemic weaknesses or deficiencies can be detected by patterns or trends identified in scans of the College's network.

Vulnerability Scanning:
College systems and applications will be scanned for vulnerabilities periodically and when new vulnerabilities affecting those systems and applications are identified. Vulnerability assessments will be conducted no less than every six months, and penetration testing will be conducted no less than annually.

OIT will determine the required vulnerability scanning for all system components (including potential sources of vulnerabilities such as networked printers, scanners, and copiers) and hosted applications. Vulnerabilities to be scanned will be readily updated as new vulnerabilities are discovered and announced and scanning methods are developed. Vulnerability scanning processes shall ensure that potential vulnerabilities are identified and addressed as quickly as possible.

Vulnerability scanning will include:

- scanning for patch levels;
- scanning for functions, ports, protocols, and services that should not be accessible to users or devices;
- scanning for improperly configured or incorrectly operating information flow control mechanisms; and
- scanning of custom software applications using source code reviews and/or static analysis tools, web-based application scanners, binary analyzers, and/or other analysis approaches, as appropriate.

Vulnerability scanning will be completed by individuals with privileged access authorization to the selected system components and the sensitivity of the information contained therein.

Vulnerability Remediation:
Remediation of discovered vulnerabilities will be prioritized with consideration of the related assessment of risk and the level of effort to be expended in the remediation for specific vulnerabilities.

Vulnerability severity is determined by the rating provided by NIST's Common Vulnerability Scoring System ("**CVSS**") version 3.0 ratings. On the CVSS scale, 7-8.9 is considered "high" severity and 9-10 is considered "critical" severity. All validated high and critical vulnerabilities should be remediated as defined in the table 1 below. Vulnerabilities with less severity can be resolved based on availability of staff resources to address them.

AR 7.1.2 Table 1

Priority Level	Remediation Plan to Be Developed Within	Vulnerability to Be Resolved Within
Critical (CVSS 9-10)	2 weeks	1 month
High (CVSS 7-8.9)	1 month	3 months

After a vulnerability is detected, and a fix is available, the timeline for remediation begins. Vulnerabilities that potentially put Confidential (Level 2) or Highly Sensitive (Level 3) data or Mission Critical Systems at risk have the shortest remediation timeframe.

Remediation plans should:

- validate that the vulnerability is properly identified and prioritized;
- provide action-oriented descriptions of the steps that will be taken to mitigate the vulnerability;
- ensure that appropriate resources are or will be available to resolve the vulnerability;
- identify milestones necessary to fully address and resolve the vulnerability; and
- ensure that the schedule for resolving the vulnerability is achievable.

References:
Information Security Policy

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Administrative Regulation Title: **Data Backup**
Regulation Number: **7.1.3**

Purpose:
This Data Backup Administrative Regulation (this "**Admin Reg**") outlines the data backup practices of the College. Regularly backing up data protects against data loss in the event of a physical disaster, database corruption, cybersecurity incident, hardware or software failure, or other incident which may lead to the loss or unavailability of data. Standardized backup practices facilitate the College's goal of ensuring the integrity and availability of Institutional Resources and allow College functions to resume in an acceptable timeframe following incidents.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

Scope:
This Admin Reg applies to all Institutional Resources.

Backup Overview:
Data backup is the practice of saving data in a manner that is logically and physically separated from the production system for the purpose of preventing unplanned data loss in the event of equipment failure or destruction. Backup practices discussed in this Admin Reg represent the minimum backup standards for all Institutional Resources. Specific backup standards for systems and resources throughout the College will be determined by the Chief Information Officer, taking into account the criticality and restoration requirements associated with the data. Backup standards are determined using the College's Information Classification and Disaster Recovery standards.

Backup Requirements and Practices:
Data backups are:

- *Required* for all Mission Critical Systems and for any Institutional Resource that creates, processes, maintains, or stores data classified as Highly Sensitive (Level 3).
- *Recommended* for Confidential (Level 2) data, and for data that cannot be recreated in a timeframe satisfactory to the owner.
- *Optional* for all other Institutional Resources.

Data intended to be temporary in nature (i.e., work or scratch files), which can readily be recreated from source data in a timely manner, may be excluded from backup requirements provided that the original source data is backed up.

To facilitate appropriate data backups, the Office of Information Technology ("**OIT**") will work with College departments and Personnel to:

- Identify primary responsibility within the unit or program for data backup and appropriately define roles and responsibilities to ensure timeliness and accountability related to backups;
- Classify Institutional Data and determine the backup method best suited to their classification level;

- Ensure that backups containing data classified as Highly Sensitive (Level 3) are encrypted both in transit and at rest and determine whether encryption is necessary for backups containing Confidential (Level 2) data; and
- Determine appropriate backup location (data must be backed up to College approved and managed devices or servers).

Third-Party Vendors:
Contracts with vendors that maintain, protect, or provide access to the College's Mission Critical Systems or Highly Sensitive (Level 3) data—whether on-premise or cloud-based—must include appropriate data backup provisions.

References:
Business Continuity and Disaster Recovery Administrative Regulation
Data Retention
Information Classification Administrative Regulation
Information Security Policy

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Administrative Regulation Title: **Authentication and Access Control**
Regulation Number: **7.1.4**

Purpose:
This Authentication and Access Control Administrative Regulation (this "**Admin Reg"**) outlines the identification and authentication standards that enable the College to manage access to Institutional Resources. Limiting access to Institutional Resources to only Authorized Users helps ensure the confidentiality, integrity, and availability of Institutional Data are maintained. Institutional Resources are vital assets to the College and limiting access to those with a legitimate business purpose is essential to the mission and operation of the College.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

Scope:
This Admin Reg applies to all accounts, persons, or entities that provide or have access to Non-Public Institutional Resources.

Roles and Responsibilities:
The Office of Information Technology ("**OIT**") manages and executes the identification, authentication, and access control practices of the College, in conjunction with applicable Personnel, including the Human Resources Department.

Authentication:
Authentication is the verification process of ensuring the identification of a user, document, or credential is genuine. Authentication is performed when users provide a username and password. Multi-factor authentication is the process of requiring the user to verify their identity by performing different methods of authentication, such as password authentication and SMS text one-time passcode.
The College will implement and maintain an authentication process that complies with applicable law or at minimum:

- Requires user accounts to use a password with the following complexity requirements:
    - Contains 10 or more characters;
    - Does not contain specific patterns, such as 3 or more repeating characters;
    - Has not been used in the previous twenty-four (24) password changes;
- Requires multi-factor authentication for access to Institutional Resources (Level 2 and Level 3), through verification of at least two of the following types of authentication factors:
    - Knowledge factors, such as a password;
    - Possession factors, such as a token; or
    - Inherence factors, such as biometric characteristics; and
- Limits unsuccessful logon attempts.

Access Control:
Access to Institutional Resources is granted on the principle of least privilege access, which means access rights to Institutional Resources are limited to only that which is necessary for the Authorized

User to perform their job/task. The College will implement, maintain, and review a process for granting access to user accounts that includes, at minimum:

- Limiting Authorized Users' system access to the types of transactions and functions that are required based on the role the Authorized User performs;
- Segregating Institutional Resources behind access control checkpoints that is proportionate to the confidentiality and sensitivity of the resource;
- Periodically reviewing access control parameters to ensure access to resources is limited only to those accounts that continue to require such access;
- Offboarding Authorized Users upon their separation from the College and de-credentialing the account to prevent the exploitation of the account;
- Monitoring and logging of system activities, in accordance with the Monitoring and Logging Administrative Regulation, to detect misuse of accounts and ensure access remains properly limited;
- Utilizing session locks and automatic session termination to prevent access to and viewing of data after periods of inactivity and other defined conditions;
- Monitoring and controlling remote access sessions to ensure such sessions, and the data accessed, remain appropriately secure and confidential; and
- Ensuring individuals who have been provided any level of authorized access to Institutional Resources are made aware of relevant policies and procedures applicable to their access to and use of such resources, including, but not limited to, the Acceptable Use Policy.

Identification:
The College will maintain a set of linked records, or credentials, identifying all Authorized Users who use Institutional Resources and the permission associated with such Authorized User. The College will implement and maintain identification practices that include, at minimum:

- Clearly defined account types and privileges, roles, and memberships associated with accounts;
- Establishing change management procedures to identify when accounts, or their related privileges, roles, or memberships, should be created, modified, or removed;
- Upon approval of account creation by appropriate Personnel, as applicable, providing appropriate credentials to individuals; and
- Ensuring individuals are not assigned more than one unique identifier and unique identifiers are never reassigned to individuals other than the initial assignee.

References:
Acceptable Use Policy
Information Security Policy
Monitoring and Logging Administrative Regulation

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Administrative Regulation: **Monitoring and Logging**
Regulation Number: **7.1.5**

Purpose:
This Monitoring and Logging Administrative Regulation (the "Admin Reg") outlines College practices and procedures regarding the monitoring and logging of events related to Institutional Resources. Standardized monitoring and logging procedures ensure the College is able to readily identify suspicious incidents and effectively protect the confidentiality, integrity, and availability of Institutional Resources.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

Scope:
This Admin Reg applies to all Institutional Resources. Responsibilities identified in this Admin Reg apply to IT or other Personnel tasked with monitoring system events.

Log Content:
Where technically possible, and not in conflict with regulatory or contractual requirements, systems will record and retain log records of the following events. Log records will be made regardless of whether attempted activities are failed or successful.

- User login attempts;
- File or database access attempts;
- Use of privileged accounts with administrative access;
- Use of privileged access or operations (e.g., adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, user password changes, etc.);
- Act of switching to or acting as a different user account
- Accept an incoming network service request;
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
- Server-based application process startup, shutdown, restart, or abnormal end;
- Activation and deactivation of protection systems such as anti-virus, intrusion detection, and file integrity systems; and
- Alarms and/or detection of suspicious or malicious activity provided by an information security system, such as an Intrusion Detection or Prevention System (IDS/IPS), file integrity monitor, anti-virus system, or anti-malware system.

Log records will capture sufficient information to provide the following:

- Identification of the activity performed;
- Identification of the person or entity that performed the activity (e.g., username or other ID, source address, destination address);
- Object the activity was performed against;
- Date and time stamp of the activity; and
- Status, outcome, and/or result of the activity.

Log Storage and Retention:
IT Resources will be configured to support formatting and storage of logs that ensure the integrity and availability of log information. Log information will be retained for a minimum of three (3) months for immediately available analysis. Logs will be subject to the College's Data Backup Administrative Reg.

Log Monitoring and Review:
Logs will be reviewed regularly by authorized IT personnel to ensure College resources remain secure. Frequency of log reviews will be determined based on the criticality of the Institutional Resources related to the logs, based on the College's Information Classification Administrative Reg.

Alerts based on thresholds and triggering events will be incorporated into logging practices to facilitate monitoring of logs and flagging of suspicious activity. Detection of suspicious activity will be reported and handled in accordance with the College's Incident Response Administrative Reg.

Controls will be in place to ensure logs are not improperly accessed or modified and logging is not improperly halted.

References:
Data Backup Administrative Regulation
Incident Response Administrative Regulation
Information Classification Administrative Regulation
Information Security Policy

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Administrative Regulation: **Incident Response**
Regulation Number: **7.1.6**

Purpose:
This Incident Response Administrative Regulation (this "**Admin Reg**") outlines the process for responding to potential or actual information security incidents at the College. This Admin Reg defines roles, responsibilities, and procedures related to incident identification, investigation, remediation, and reporting. Standardization of incident response plans aids the College in effectively containing and resolving incidents to ensure confidentiality, integrity, and availability of Institutional Resources are maintained.

Definitions:
Capitalized terms not defined in this Admin Reg have the meaning set forth in the Information Security Policy.

Scope:
This Admin Reg applies to all Institutional Resources and any person, entity, or device that gains or attempts to gain access to Institutional Resources.

Information Security Incidents:
Information security incidents are events that have the potential to compromise the confidentiality, integrity, or availability of Institutional Resources.
The Incident Response Plan should be followed when the following types of events occur:

- Any unauthorized access to Institutional Resources, including any potential data breach;
- Any such incident involving a member of the College community, including, but not limited to, students, faculty, staff, guests, volunteers, partners, and visitors; and/or
- Any such incident involving services provided by third parties to the College, such as contracted vendors, partner institutions, etc.

If it is not clear whether a specific situation constitutes an information security incident, report the situation and the Office of Information Technology ("**OIT**") will make the determination.

Reporting:
All Authorized Users are responsible for reporting any event that might compromise information security to OIT and/or the Authorized User's direct supervisor.

- Call IT Helpdesk at 307-532-8002 or log a Halo ticket through MyEWC portal
- Report an incident in person at the IT Office (AC 105)- lower-level Activities Center

Other means, such as automatic detection tools and logs kept pursuant to the Monitoring and Logging Administrative Regulation, also enable monitoring and reporting of suspicious activity.

Incident Response:
The College responds to incidents in accordance with the following phases. The phases outlined below are only meant to serve as a general overview of the incident response, as OIT and system owners and administrators work together to develop detailed plans specific to various Institutional Resources.

1. **Preparation**

   Effective incident response is facilitated by proactive planning for the possibility of incidents. Pursuant to the Information Security Policy and this Admin Reg, the College maintains, and works to continuously improve internal processes, procedures, and tools, with the goal of enabling immediate and effective response should an incident be detected across any IT Resource. OIT and President's Executive Team will work together to prepare and evaluate incident response plans.

2. **Detection and Analysis**

   Once an incident has been reported to OIT, OIT is charged with coordination for the duration of the incident, except in situations where OIT determines the specifics of the incident warrant law enforcement involvement. Once a determination has been made that an incident has occurred, investigation of the incident and/or forensic analysis related to the incident must be initiated by and coordinated through OIT.

   Once a potential incident is detected, the following actions will be taken:

   a. The College President assigns an Incident Coordinator who will be the primary point of contact for the duration of the response and recovery effort. In the absence of the College President, the Vice President of Administrative Services shall make the assignment.
   b. The Chief Information Officer ("CIO"), in conjunction with OIT and any other appropriate Personnel, will review the known details of the incident and classify and prioritize the incident based on relevant factors (i.e., functional impact, information impact, recoverability, etc.).
   c. If the incident involves Confidential (Level 2) or Highly Sensitive (Level 3) data, the Incident Coordinator will assemble an Incident Response Team ("IRT") as set forth below.
   d. The Incident Coordinator, in consultation with the College President and legal counsel, will initiate notifications required by law or contract and as necessary to initiate additional incident response activities. Depending on the circumstances, notifications may be made to the following:
      - Local law enforcement (Torrington PD, 307-532-7001) (Douglas PD, 307-358-3311)
      - Homeland Security (307-777-4663)
      - FBI (Cheyenne Office, 307-632-6224)
      - Cyber Insurance Company
      - Wyoming Community College Commission (307-777-7763)
      - Wyoming Department of Enterprise Technology Services (307-777-5840)
      - Federal Student Aid (support@cpssaid.ed.gov)
      - Federal Trade Commission (www.ftc.gov)

3. **Assemble an Incident Response Team**

   If applicable, under the guidance of the CIO, the Incident Coordinator will assemble an IRT that will be responsible for mitigation, investigation, and remediation of the incident. The makeup of this team will vary depending on the classification of the incident, the type of incident, and the Institutional Resources impacted by the incident.

4. **Containment**
   The goal of the containment phase is to prevent any further damage or incidents associated with the initial incident. OIT will work to identify, and isolate or otherwise mitigate, the affected system(s) or resource(s) to "contain the spread" as effectively as possible.

5. **Eradication**
   All vulnerabilities that were exploited will be identified and mitigated. Any malware or other inappropriate materials or components will be removed. Investigation of the incident will remain on-going, and if additional systems or resources are determined to be affected, the detection, analysis, containment, and eradication activities will be completed for the affected systems or resources.

6. **Recovery**
   Systems or resources will be returned to their operational state, and tests will be completed to ensure all systems and resources are functioning normally. Additional monitoring mechanisms will be implemented, as necessary, to facilitate detection of future related activity.

7. **Incident Documentation**
   The IRT will complete an incident report to document details of the incident and the investigation. Each incident report must minimally contain:
   - A description of the incident;
   - Information about the results of the investigation (attacker, cause, etc.);
   - Impact on service, financial damage, violation of privacy, and other related effects;
   - Actions taken;
   - Notification decisions and completed notifications; and
   - Remediation plan information.

8. **Debriefing/Notification**
   Meetings with relevant stakeholders will be held to discuss the incident report and any takeaways. Incident response plans and other policies and procedures (e.g., Risk Management and Vulnerability Management) will be updated, as applicable, to facilitate ongoing security and future incident response capabilities. Additionally, stakeholders should opine on whether applicable law requires any external parties to be notified of the incident.

The College is bound by laws and regulations as it relates to the handling of data that is collected, maintained, and used by the College. Those include the Family Educational Rights and Privacy Act ("**FERPA**"), the Health Insurance Portability and Accountability Act ("**HIPAA**"), the Gramm-Leach-Bliley Act ("**GLBA**"), Wyo. Stat. § 40-12-502(d)(iii) & (iv), the Payment Card Industry Data Security Standard ("**PCI DSS**"), contractual obligations, and any other regulations that may be put into force by federal or state governing authorities. Any changes and/or additions to regulations may override the above-referenced acts, and this Admin Reg will be reviewed annually for recent changes.

References:
Information Security Policy
Information Classification Administrative Regulation
Monitoring and Logging Administrative Regulation
Risk Management Administrative Regulation

Vulnerability Management Administrative Regulation

Revision History:
Original Adoption Date: 1/29/24
Revision Date(s):
Date Reviewed, no change:

Policy Title: **Accessibility in Electronic and Information Technology Design**
Policy Number: **7.2**

Purpose:
This Accessibility Policy (this **Policy**) outlines the College's accessibility practices related to Institutional Resources. The College complies with the Americans with Disabilities Act, the Rehabilitation Act, and other federal, state, and local laws regarding disabilities and is committed to maintaining an inclusive community by striving to provide accessible electronic information, communication, and technology.

Definitions:
Capitalized terms not defined in this Policy have the meaning set forth in the Board Policy 7.0 Information Security.

1. **Accessible**
   Means a person with a disability is afforded the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services as a person without a disability in an equally effective and equally integrated manner, with substantially equivalent ease of use. The person with a disability must be able to obtain the information as fully, equally, and independently as a person without a disability, according to the U.S. Department of Education Office for Civil Rights.

2. **Digital Content**
   Includes anything on College websites and within the learning management system, Student Information System, including, but not limited to, audio, video, images, tables, forms, documents (in any format, including, .docx and .pdf), registration forms, surveys, and HTML.

3. **Effective Alternative Access**
   Means equally effective alternate access to the same information or services offered by an IT Resource that does not meet the College's accessibility standards.

4. **Web-based Application**
   Means a web-based program created to carry out or facilitate a task on a computing device.

Scope:
This Policy applies to all Digital Content or services that are acquired, developed, distributed, used, purchased, or implemented by or for the College and used within the context of teaching, learning, research, service, employment, and other official functions of the College. This includes any web pages, Web-based Applications, electronic documents, and multimedia. It also includes any third-party applications used to create and/or disseminate digital content (i.e., web-based content creation, textbook supplemental materials, or mobile applications).

Policy:
Ensuring accessibility of Digital Content is a shared responsibility for all members of the College community who create, obtain, share, utilize, and publish Digital Content. Each member of the College community (i.e., Personnel, students, Contractors, etc.) who obtains, designs, develops, recommends, procures, or manages Digital Content, Web-based Applications, or other technology-based resources is subject to and has responsibilities under this Policy.

Accessibility Standards:
The accessibility of online content and functionality will be measured according to the W3C's Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. Web Content Accessibility Guidelines (WCAG) 2.1 (w3.org)

Effective Alternative Access:

- Consistent with applicable laws, the College will follow WCAG 2.1 Level AA for all web-based electronic information, communication, and technology unless doing so (1) fundamentally alters a program, service, or activity; or (2) creates an undue administrative or financial burden.
- For all aspects of this Policy for which the College determines an undue administrative or financial burden exists, or that require a fundamental alteration of a program or service or activity, the College will provide affected individuals with Effective Alternative Access.
- In providing Effective Alternative Access, EWC will take actions that do not impose any undue administrative or financial burden on the College and that do not require a fundamental alteration of any program or service or activity. Further, in providing Effective Alternative Access, the College will ensure that, to the maximum extent possible, individuals with disabilities receive the same benefits or services as their nondisabled peers.
- Effective Alternative Access alternatives are not required to produce the identical result or level of achievement for persons with disabilities, but they must afford persons with disabilities an equal opportunity to obtain the same result, to gain the same benefit, or to reach the same level of achievement, in the most integrated setting appropriate to the person's needs.

Procurement/Purchases:
The College will have purchasing protocols in place to ensure that Web-based Applications, Digital Content, and other electronic products and solutions including, but not limited to, software, operating systems, video, and multimedia meet or exceed the above accessibility standards. The College recommends that all requests for proposals and contracts with vendors include language that outlines this requirement and provides stipulations for how the vendor is expected to demonstrate compliance.

Training:
The EWC President shall designate the CIO to ensure all Personnel and Contractors have received training on the requirements of this Policy.

References:
682Americans with Disabilities Act of 1991, 42 U.S.C. § 12101 *et seq*. (**ADA**)
Sections 504, 508 of the Rehabilitation Act of 1973, 29 U.S.C. 794 § *et seq*.
Requirements for Accessible Electronic and Information Technology (E&IT) Design
https://www2.ed.gov/about/offices/list/ocr/frontpage/pro-students/issues/dis-issue06.htm

Revision History
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Policy Title: **Acceptable Use Policy**
Policy Number: **7.3**

Purpose:
This Acceptable Use Policy (this **Policy**) protects the confidentiality, integrity, and availability of institutional Resources, by setting expectations for all Authorized Users, including Personnel, Contractors, and students, regarding accessibility to technology resources for the College's academic community and the prohibition of using Institutional Resources inappropriately.

Definitions:
Capitalized terms not defined in this Policy have the meaning set forth in the Board Policy 7.0 Information Security.

Policy:
Institutional Resources are reserved for the educational, instructional, research, and administrative computing needs of Authorized Users.

Access to Institutional Resources is a privilege, and therefore, it is essential that all Authorized Users exercise responsible, ethical behavior when using these resources. Authorized Users are expected to read, understand, and comply with this Policy.

Acceptable Use:
Institutional Resources are intended to be used for educational purposes and to carry out the legitimate business of the College. Users are expected to:

- use only those resources that they have been authorized to use, and use them only in the manner and to the extent authorized;
- protect their user ID, password, and system from unauthorized use;
- be considerate in the use of shared resources; and
- comply with local, state, and federal law, including copyright law and College policies and administrative Regulations.

Incidental personal use of Institutional Resources by Personnel is permitted if the personal use does not interfere with the execution of job duties, does not incur cost on behalf of the College, and is not considered "unacceptable" as outlined in the "Unacceptable Use" section below. Incidental personal uses that inaccurately create the appearance that the College is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

Unacceptable Use:
Personnel, including students acting as employees, and Contractors are prohibited from the following actions when using Institutional Resources:

- Unauthorized use for commercial purposes or personal gain; and
- Transmitting commercial or personal advertisements, solicitations, or promotions.

All users are prohibited from using Institutional Resources in a manner that results in a violation of law or policy or potentially adversely affects network service performance. Examples of unacceptable use include, but are not limited to, the following:

- Activity that violates federal, state, or local law;
- Activity that violates any College policy or administrative regulation;
- Activities that lead to the destruction or damage of equipment, software, or data belonging to others or the College;
- Circumventing information security controls of Institutional Resources;
- Releasing malware;
- Intentionally installing malicious software;
- Impeding or disrupting the legitimate computing activities of others;
- Unauthorized use of accounts, access codes, passwords, or identification numbers;
- Unauthorized use of systems and networks; and
- Unauthorized monitoring of communications.

This list is not complete or exhaustive. It provides examples of prohibited actions. Any user in doubt about the acceptable use of Institutional Resources should contact the Chief Information Officer for further clarification and assistance.

Enforcement and Penalties:
The College reserves the right to monitor activity of users. While the College does not routinely monitor the activity of users for violation of this Policy, situations may arise where the College may have the need to view information or email or monitor user activity on the network. This may include, but are not limited to, the health or safety of individuals or property or actual or suspected violations of College policies or administrative regulations or local, state, or federal laws.

Violations of this Policy may result in disciplinary action, including suspension or dismissal from employment, probation, suspension or expulsion from further study, and/or termination or suspension of network privileges. The College also reserves the right to notify appropriate legal authorities if Institutional Resources are used in a manner that constitutes a violation of any local, state, or federal law.

The College is not liable for the actions of anyone in their use of, access to, or connection to the Internet through Institutional Resources. All users will assume full liability, legal, financial or otherwise, for their actions when accessing or using Institutional Resources.

References:

Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Policy Title: **Visitor - Use of Institutional IT Resources**
Policy Number: **7.4**

Purpose:
This Visitor - Use of Institutional IT Resources Policy (this **Policy**) outlines the parameters under which Visitors of the College may access and use IT Institutional Resources. The College maintains an atmosphere that is open and allows visitors access to certain resources, as long as such access does not compromise the integrity of the systems or information contained within the campus and does not introduce malicious software or intent to harm the internal network and/or Institutional Resources.

Definitions:
Capitalized terms not defined in this Policy have the meaning set forth in Board Policy 7.0 Information Security.

1. **Internal Access:**
   Means access to systems or applications that are not publicly accessible, without relevant internal permissions, and may include access to:
   a. Wireless VLANs (i.e., campus, employees, and Lancers);
   b. Singular or multiple file access; or
   c. System access, such as Canvas Learning Management System, Colleague Student Information System, ID Card System, email system, etc.

2. **Visitor** is defined as anyone not enrolled at or employed by the College and can include, but are not limited to: community members, non-registered students, friends, spouses, children, guest speakers, consultants, and College sanctioned event participants.

Policy:
Visitor's access may be classified as:
1. Standard Access – Access granted to internet resources, to include Wi-Fi access, and public Institutional Resources located online; and
2. Special Access – Standard Access plus any Internal Access as requested by an individual with the authority to do so from the Vice President for Administrative Services or Vice President of Student and Academic Services, and the President, and Chief Information Officer, or other designee deemed necessary by the President.

Under no circumstances should Visitors be given Special Access unless permission has been obtained from the appropriate administrative personnel (i.e., signatures from personnel above) along with a detailed description of access and the need thereof.

To obtain Special Access, users should contact the College IT Department with their requested system access requirements.

References:
Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Policy Title: **Security Awareness Training Policy**
Policy Number: **7.5**

Purpose:
This Security Awareness Training Policy (this **Policy**) ensures all Personnel and Contractors with access to Institutional Resources are provided with education and training opportunities to gain an understanding of the importance of securing the Institutional Data.

Definitions:
Capitalized terms not defined in this Policy have the meaning set forth in the Board Policy 7.0 Information Security.

1. **Security Awareness Training** is a formal process for educating employees about the Internet and computer security. A good security awareness program should educate employees about institutional policies and procedures for working with information technology (IT).

Scope:
This Policy applies to all College Personnel and Contractors. Exceptions are Personnel and Contractors who do not have access to computers and/or personally identifiable information (PII). Any other exceptions must be approved by the Chief Information Officer.

Policy:
The College will implement and maintain a Security Awareness Training program that is designed to educate Personnel and Contractors on their obligations with respect to the security of their accounts, Institutional Resources, and other information assets that could impact the College. The College requires Personnel and Contractors to appropriately protect College-owned and personal computers that store, access, or use Institutional Resources. The College also requires specific training based on the classification level of data, as set forth in Administrative Regulation 7.0.1 Information Classification, the Personnel or Contractor has access to and the role the Personnel or Contractor fills.

Personnel are required to attend Security Awareness Training within the first sixty (60) days of employment or the new hire will be deemed non-compliant with this Policy. Personnel and Contractors with access to PII are required to complete Security Awareness Training on a yearly basis. All part-time, temporary employees, and Contractors with access to PII must undergo Security Awareness Training before accessing any Institutional Resources.

The Security Awareness Training program will be reviewed annually and updated, as applicable, based on changes to the information security environment.

Enforcement:
Personnel and Contractors that do not comply with this Policy will have network access rights suspended until they comply.

References: Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809, §§ 6821-6827
Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Policy Title: **Electronic Communications**
Policy Number: **7.6**

Purpose:
Electronic communication is necessary to fulfill multiple roles and activities here at EWC. Because of the varying types of electronic communication, focus is on those used primarily at EWC:

1. Email
2. VoIP
3. Videoconferencing
4. Digital Signage

Regardless of the type of technology being used, electronic communication is meant to serve the needs of the college by sharing information with students, employees, vendors, other state agencies, campus visitors, and other individuals. Because of the unique capabilities of each system, it is important to realize that each type of communication method contains unique issues that must be addressed on a case-by- case basis; however, general rules can be set forth to ensure that any communication method is used wisely and according to its intended purpose. In general, EWC's electronic communication mechanisms are to be used to share information with students, employees, vendors, other state agencies, campus visitors, and other individuals. EWC is to adequately convey the appropriate knowledge so that the College mission is not hindered but enhanced.

This information is always to be distributed under the following assumptions:

1. is always understood to represent an official statement from the institution
2. shall never be used for the creation or distribution of any information that meets the following criteria: such as Disruptive or Offensive or Derogatory or Specific comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin or any information that could be used to sabotage institutional progress or any personally identifiable information
3. shall not be used for personal gain
4. shall not be used extensively for personal use
5. shall not be used to distribute malicious or harmful software or information

Email:
Email is the official method of communication at EWC, both for students and employees. Business is conducted every day via email. Since email has both positive and negative connotations, it is imperative that we recognize that the positive aspects greatly outweigh the negative aspects. However, we must also realize that the negative aspects exist and ensure that this method of communication is used effectively, efficiently, and for its intended purpose.

VoIP Phone Communication:
EWC's VoIP phone system is used to transmit and receive audio/video within the institution to facilitate direct communication amongst employees and departments. It is also used to transmit and receive audio outside the institution to facilitate direct communication with vendors, students, other institutions, and other third-party entities. Because of this capability, we must ensure that it is used for work purposes.

Videoconference Systems:
Videoconferencing equipment is used primarily for instructional classrooms requiring connectivity to other EWC locations and to service area high schools. Videoconferencing equipment is also used to facilitate conferences and meetings with other institutions, state agencies, or other third-party entities. Since this type of communication conveys not only audio, but video as well, it is particularly important for it to be used for its intended purposes.

Digital Signage:
Digital signage is used on campus to convey student activities, important academic dates, campus events, and other information to students, employees, and visitors. Since this is also a visual and auditory communication mechanism, it is also important to ensure it is used for its intended purpose as well.

Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Policy Title: **Emergency Notification**
Policy Number: **7.7**

Purpose:
EWC maintains an emergency notification system that is used to notify students and employees who have opted in to the service via the CodeRed on the EWC website. This system is updated daily to reflect the current student data available so that any notification message will be delivered to the required student and employee list.

Use of CodeRed:
The EWC Emergency Notification System is to be used, at all times, for emergency purposes or purposes deemed necessary by the President or designee only. The notification system is to be used to send messages via text to email addresses and mobile phones, via voice to office phones, personal phones, and mobile devices, and via applications to desktops and office phones.

At no time shall this system be used for normal messaging, notifications, or otherwise standard contact as this would compromise the importance of these messages and may create an environment where students and employees are able to overlook these types of messages because of the frequency with which they could occur. Tests of this system shall be conducted once a semester at minimum to ensure the system is functioning properly. Additional tests may be conducted but are not required; however, more than four tests per semester may be too many to retain the importance of such messages when an actual emergency arises requiring the system to be operational.

Only users defined below shall be able to send emergency notification messages via this system:

- Director of College Relations
- Director of Housing
- Vice President of the Douglas Campus
- Vice President of Student and Academic Services
- Other designee deemed necessary by the President

Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change:

Policy Title: **Enforcement**
Policy Number: **7.8**

Purpose:
This policy is to establish enforcement guidelines to ensure that all EWC IT Department policies and procedures are adhered to and observed by all departments and individuals at EWC including students, employees, visitors, vendors, etc. Anyone using technology resources at EWC will be required to operate within the parameters described in this document or the following enforcement options may be administered.

Actions:
All policies herein are applicable to any and all users of technology resources at EWC. If it is found that any individual, department, or external entity disobeys the policies and procedures set forth within this document, whether knowingly or unknowingly, then the enforcement of such policy may include, but may not be limited to:

- Forced compliance with the policy
- Disciplinary action including termination of employment, if an employee
- Disciplinary action including expulsion from the College, if a student
- Termination of vendor contract and or service agreement
- Prosecution to the fullest extent of the law

Revision History:
Original Adoption Date: 11/09/21
Revision Date(s): 12/12/23
Date Reviewed, no change: