Eastern Wyoming College

(EWC)

Privacy and Security Policies Manual

2021

Table of Contents

1.0 Overview and Introduction

This document serves as a directory for rules and regulations for successfully and properly utilizing Critical Information and Assets at Eastern Wyoming College (EWC). Careful consideration should be taken to verify that one's actions fall within the authorized parameters for access, utilization, distribution, and modification of EWC's technology resources set forth within this document to ensure proper steps are taken when using EWC IT Services.

EWC Information Technology (IT) Department to provide these policies and procedures in order to address potential situations and to provide steps to take during these situations. However, not all situations can ever be addressed so it is up to each individual employee and affiliate to use these policies and procedures for an example of what type of actions to take.

All individuals using EWC IT resources ("Users"), regardless of affiliation and irrespective of whether these resources are accessed from EWC's campus or from remote locations.

EWC leadership and management expects EWC employees and associates to utilize caution should a potential risk, threat, issue, or questionable request or action present itself that is not discussed herein. Each employee or associate of EWC are encouraged to utilize EWC IT Department's open-door policy and ask for assistance or clarification.

Any misuse, misappropriation, negligence, or deliberate disobedience concerning these policies and procedures will result in EWC action regarding employment or affiliation. Each individual employee and affiliate of EWC shall be familiar with the policies and procedures set forth herein prior to signing the agreement form included in this manual. The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.0 Scope and Change Management

2.1 Scope of Controlled Unclassified Information

The policies described in this manual are applicable to all departments and users of resources and assets that collect, process, store, transmit, or provide security protection for the College's Controlled Unclassified Information (CUI) including, but not limited to:

- EWC-owned technology resources. These resources can include, but are not limited to, the following equipment:
    - Computers that include desktop computers, mobile devices, servers, etc.
    - Network Equipment that include switches, routers, network and communications cabling, wall plates, wireless antennas, wireless bridge devices, fiber optic lines, fiber optic equipment, VoIP phones, etc.
    - Audio/Video Equipment that include video codecs, HDTVs, document cameras, projectors, security cameras, miscellaneous cabling, digital cameras and camcorders, printers, copiers, fax machines, etc.
    - Software that includes operating systems, application software, etc.
    - Resources that include group drive file storage, website file storage, email accounts, social networking accounts, etc.

2.2 Applicable Standards and Regulations

Applicable rules and regulations, include and are not limited to:

- Compliance_matrix.xlsx
- 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

Within EWC's IT environment, additional rules 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 to specific types of activities (collectively, "local rules"). Local rules must be consistent with Policies, but also may impose additional or more specific requirements or responsibilities on Users.

2.3 Data and Information Classification

2.3.1 PII Definition

This section establishes EWC's definition of Personally Identifiable Information (PII) and indicates what information may be shared, if any, with third-party entities. It is important to note that information should never be shared without cause or requirement, unless dictated by state or federal government regulations such as annual reporting guidelines and statistical reporting data, in the course of preset institutional operations or vendor agreements, or due to the request of EWC's President or designee. PII is the type of information that should be kept safe using the highest level of security. PII is described as information about an individual that identifies, links, relates, or is unique to, or describes him or her. PII may include:

- Name
- SSN
- Address(es)
- Phone Number(s)
- SSN
- Birth date
- Birthplace
- Mother's maiden name
- Family names
- Other family data such as addresses, contact information, etc.
- Financial information such as bank account information, account balances, etc.
- Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have a personal knowledge of the relevant circumstances, to identify the student with a reasonable certainty
- Information requested by a person who the educational agency or institution believes knows the identity of the student to whom the educational record directly relates.

Under no circumstances should PII be transported off-campus. On-campus storage of PII should meet other policy requirements as dictated herein. Off-campus use of this type of data may be facilitated via the EWC IT Department's Remote Access Policy.

2.3.1 Data Classification

Eastern Wyoming College Data Classification approach categorizes information collected, stored, and managed by the College community. These data classifications will be used internally and referenced by other policies to improve the College's ability to prevent, deter, detect, respond to, and recover from internal and external compromises to its electronic information resources.

This approach applies to all persons or entities that have access to College data. It applies to all data utilized by the College community for the purpose of carrying out the institutional mission of research, teaching, outreach, and data used in the execution of required business functions, limited by any overriding contractual or statutory requirements.

Eastern Wyoming College is bound by laws and regulations as it relates to the handling of data that is collected, maintained, and used by the institution. Those would include Federal Educational Rights and

Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Wyo. Stat. § 40-12-502(d)(iii) & (iv), Payment Card Industry Data Security Standard (PCI DSS), other contractual obligations and any other regulations that may be put into force by federal and state governing authorities. Any changes and/or additions to regulations may override the data definitions below and thus this policy should be reviewed annually for recent changes.

2.3.2 Classification Levels

College data are essential to the operations of the College and its quality and safety must be ensured to comply with legal, regulatory, and administrative requirements. Information will be classified according to the risk of unauthorized exposure and the resulting impact. College data shall be classified as Level I (public - low potential impact), Level II (moderate potential impact), or Level III (private - high potential impact). Unless otherwise classified by a Data Custodian or policy, all College data shall be classified as Level II.

College data will be classified into three levels, where level I requires the least security and level III requires the highest security. Data must be consistently protected throughout its life cycle in a manner commensurate with its sensitivity regardless of where it resides or what purpose(s) it serves. Extracts of data shall have the same classification level and utilize the same protective measures as the same data in the system of record. Data Custodians may utilize the negative potential impacts listed below to evaluate data under their purview if the data does not clearly fall under the laws, regulations, or examples listed. The highest negative impact rating received shall classify data within that category. Data that has no negative impacts to the College but may cause significant harm to individuals must be categorized as Level III.

Level I: Public -Low Potential Impact

Level I data may or must be open to the public. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Access is available to the public but may need to be granted by the Data Custodian. The loss of confidentiality of Level I data should be expected to have limited adverse effects on College operations, College assets, or individuals. A loss of integrity or availability of Level I data may have limited adverse effects on College operations, College assets, or individuals. The loss of confidentiality of Level I data may result in some of the following:

- No loss of mission capability, but inconveniences may be experienced by some individuals
- No damage to College assets
- No financial damages and/or fines

Insignificant harm to individuals 5. Little, if any, negative impact on the College's reputation The loss of availability or integrity of Level I data may result in some of the following: 1. Limited degradation in or loss of mission capability to an extent and duration that the College is able to perform its primary functions, but the effectiveness of the functions may be noticeably reduced. 2. No or very minor damage to College assets 3. No direct financial damages and no fines 4. Insignificant indirect financial damages 5. Insignificant harm to individuals 6. Possible negative impact on the College's reputation, generally dependent on the visibility of loss of integrity or availability to the community Examples include published "white pages," directory information, maps, departmental websites, lists of email addresses, academic course descriptions, and other information readily published and provided to the public at large.

Level II: Private - Moderate Potential Impact

Level II data are information whose access must be guarded due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a statute requiring this protection. This information is not intended for public dissemination, but its disclosure is not restricted by Federal or state law. Unless otherwise classified by a Data Custodian or policy, all College data shall be classified as Level II. The loss of confidentiality, integrity, or availability of Level II data should be expected to have moderate adverse effects on College operations, College assets, or individuals. The loss of confidentiality, integrity, or availability of Level II data may result in some of the following: 1. Limited degradation in or loss of mission capability to an extent and duration that the College is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced. 2. Minor damage to College assets 3. Minor direct financial damages and/or fines 4. Minor indirect financial damages 5. Minor harm to individuals 6. Minor negative impact on the College's reputation Examples includes student grades maintained by an instructor, class lists, lists of students in a major in a department, internal memos, financial records, email communications, and other documents not intended for public distribution that are not otherwise Level III data.

Level III: Legally Protected -High Potential Impact

Level III data include all data protected by federal or state law, including, but not limited to FERPA, HIPAA, GLBA, Iowa Code Chapter 715C, PCI DSS and other contractual obligations. The loss of confidentiality, integrity, or availability of Level III data should be expected to have serious adverse effects on College operations, College assets, or individuals. The loss of confidentiality, integrity, or availability of Level III data may result in some of the following: 1. 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 2. Major damage to College assets 3. Major direct financial damages and/or fines 4. Major indirect financial damages 5. Significant harm to individuals 6. Major negative impact on the College's reputation Examples include credit card numbers, social security numbers, driver's license numbers, health records, student transcripts, financial aid data, and human subject research data that identify an individual. Other examples include credentials used as passwords, passphrases, or fingerprints as well as the data stored to allow self-service reset of the credentials.

Intermingling of Data Classifications

Multiple classifications of data may reside together in the same document, database, or electronic record. A document, database, or electronic record containing multiple classifications of data shall be classified according to the highest level of any single data element contained therein. Adequate redaction or removal of data elements will cause a document, database, or electronic record to be reclassified according to its new contents.

3.0 Access Control Policy

3.1 Policy Statements

IT Staff shall comply with the following Basic Security Requirements:

1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
2. Control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems.
3. Clearly define account types for privileged and unprivileged accounts.
4. Identify and select information system accounts to support organizational missions and business functions for all users including, but not limited to: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.
5. Assign account managers for information system accounts. System administrators shall manage unprivileged user accounts.
6. Establish conditions for group and role membership.
7. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
8. Require approvals by system owners for requests to create information system accounts.
9. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.
10. Monitor the use of information system accounts.
11. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.
12. Authorize access to the information system based on a valid access authorization or intended system usage.

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

1. Define access privileges and other attributes by account, account type, and other factors. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of- origin. In defining other account attributes, system-related requirements (e.g., system upgrades scheduled maintenance) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements) may be considered.
2. Establish system account types to include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary.
3. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

The IT Department shall comply with the following Derived Security Requirements:

3.1.3 Control the flow of CUI in accordance with approved authorizations.

1. Regulate where information can travel within a system and between systems without regard to subsequent accesses to that information.
2. Restrict the following information flows: keeping export- controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within

the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.
3. Control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems.
4. Control the flow based upon characteristics of the information or the information path.
5. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. Enforcement shall occur in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet- filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics).
6. Consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) as well as the guidance of information owners or stewards at designated policy enforcement points between interconnected systems in controlling the flow of CUI.
7. Prohibit information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
1. Separate duties of individuals as necessary to prevent the potential for abuse of unauthorized privileges.
2. Document the separation of duties of individuals.
3. Separation of duties may include dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions.
4. Define information system access authorizations across systems and application domains to support this Policy Statement.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.
1. Apply least privilege to the development, implementation, and operation of organizational systems.
2. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
3. Create additional processes, roles, and system accounts to achieve least privilege, as necessary.
4. Complete security functions including establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).
5. Restrict privileged accounts on the information system to [entity defined personnel or roles].

6. Differentiate in the application of this Policy Statement between allowed privileges for local accounts and for domain accounts provided the Department retains the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

3.1.6 Use non-privileged accounts or roles when accessing non-security functions.

1. Require that users of information system accounts, or roles, with access to [entity defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing non-security functions.

3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

1. Authorize explicit access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.
2. Ensure that the information system audits the execution of privileged functions including establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities.
3. Ensure that the information system prevents non-privileged users from executing privileged functions such as disabling, circumventing, or altering implemented security safeguards/countermeasures. Privileged functions that require protection from non-privileged users include, but aren't limited to, circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms.
4. Ensure the use of privileged functions are logged in order to detect misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

3.1.8 Limit unsuccessful logon attempts.

1. Enforce a limit of consecutive invalid logon attempts by a user during a [entity defined frequency]. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.
2. Lock the account/node automatically for [entity defined frequency] or until released by an administrator when the maximum number of unsuccessful attempts is exceeded. If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components.
3. Apply this Policy Statement regardless of whether the logon occurs via a local or network connection.

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

1. Ensure the system displays an approved system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:
    1.1. Users are accessing a [entity] information system.
    1.2. Information system usage may be monitored, recorded, and subject to audit.
    1.3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
    1.4. Use of the information system indicates consent to monitoring and recording.
    1.5. There are no rights to privacy.

2. Ensure the system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit action to log on to or further access the information system.
3. For publicly accessible systems, ensure that the information system:
    3.1. Displays system use information, but before granting further access.
    3.2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
    3.3. Includes a description of the authorized uses of the system.
4. The Department may consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon based on a risk assessment.
5. Where necessary, use posters or other printed materials in lieu of an automated system banner.
6. Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
7. Prevent further access to the system by initiating a session lock after [entity defined frequency] of inactivity or upon receiving a request from a user.
8. Retain the session lock until the user reestablishes access using established identification and authentication procedures.
9. Implement session locks where session activities can be determined, typically at the operating system level (but can also be at the application level).
10. Do not use session locks as a substitute for logging out of the system.
11. Use pattern-hiding displays, which may include static or dynamic images such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.

3.1.11 Terminate (automatically) a user session after a defined condition.

1. Ensure the information system automatically terminates a user-initiated logical session. A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.
2. Ensure session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.
3. Conditions or trigger events requiring automatic session termination may include organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

3.1.12 Monitor and control remote access sessions.

1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed, including, but not limited to: dial-up, broadband, wireless, and encrypted virtual private networks (VPNs).
2. Authorize remote access to the information system prior to allowing such connections.
3. Ensure that the information system monitors and controls remote access methods.
4. Document the rationale for such access in the security plan for the information system.
5. Provide for automated monitoring and control of remote access sessions to allow the Department to detect cyber- attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of

system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). See NIST SP 800-46, SP 800-77, and SP 800-113 for guidance on secure remote access and virtual private networks.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

1. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
2. Ensure that the information system routes all remote accesses through [entity defined number] managed network access control points to reduce the risk for external attacks. (VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.)
3. Authorize the execution of privileged commands and access to security-relevant information via remote access only for [entity defined needs].
4. Employ cryptographic standards including FIPS-validated cryptography and NSA-approved cryptography. See NIST CRYPTO; NIST CAVP; NIST CMVP; National Security Agency Cryptographic Standards.

3.1.14 Route remote access via managed access control points.

1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
2. Route remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.
3. Authorize wireless access to the information system prior to allowing such connections.
4. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

1. Allow for the execution of privileged commands on a system for the control, monitoring, and administration of the system including security functions and associated security-relevant information.
2. Provide for access from remote locations to help ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems.

3.1.16 Authorize wireless access prior to allowing such connections.

1. Establish usage restrictions and configuration and/or connection requirements for wireless access to the system to support wireless access authorization decisions and reduce the susceptibility to unauthorized access to the system through wireless technologies.
2. Leverage wireless networks' authentication protocols to provide credential protection and mutual authentication. See
   NIST, SP 800-97 for guidance on secure wireless networks.

3.1.17 Protect wireless access using authentication and encryption.

1. Authenticate individuals and devices to help protect wireless access to the system.
2. Consider the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See NIST CRYPTO.

3.1.18 Control connection of mobile devices.

1. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

2. Authorize the connection of mobile devices to organizational information systems.

3.1.20 Verify and control/limit connections to and use of external systems.

3.1.20.1. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems.
2. Process, store, or transmit organization-controlled information using external information systems.

3.1.20.2. Ensure that terms and conditions address, at a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

3.1.20.3. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

1. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

3.1.20.4. Establish that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

3.1.20.5. Control and/or limit external systems including personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This Policy Statement also addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems. Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

3.1.21 Limit use of portable storage devices on external systems.

1. Limit the use of organization-controlled portable storage devices in external systems. Such limits may include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

3.1.22 Control CUI posted or processed on publicly accessible systems.

2. Designate individuals authorized to post information onto a publicly accessible information system.
3. Train authorized individuals to ensure that individuals understand that the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication.

4. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.
5. Review the content on the publicly accessible information system for nonpublic information [entity defined frequency] and remove such information, if discovered.

Password protection

1. Enforce access control mechanisms, such as strong password requirements, MFA, and regular password changes.
2. All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 120 days.
4. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
5. Passwords must NOT be inserted into email messages or other forms of electronic communication.
6. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
7. All user-level and system-level passwords must conform to the guidelines described below. Passwords are used for various purposes at EWC. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every EWC employee should know how to select strong passwords. Poor, weak passwords have the following characteristics:
8. The password contains less than eight characters
9. The password or a subset of the password is a word found in a dictionary (English or foreign)
10. The password is a common usage word such as: o Names of family, pets, friends, co-workers, fantasy characters, etc.
11. Computer terms and names, commands, sites, companies, hardware, software
12. The words "EWC", "lancers", "community", “college” or any derivation
13. Birthdays and other personal information such as addresses and phone numbers
14. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
15. Any of the above spelled backwards o Any of the above preceded or followed by a digit (e.g., secret1, 1secret) Strong passwords have the following characteristics:
16. Contain between 8 and 32 characters
17. Contain both upper and lower case characters (e.g., a-z, A-Z)
18. Contain at least one number (e.g., 0-9)
19. Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
20. Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
21. Does not contain personal information, names of family, etc.
22. Review accounts for compliance with account management requirements based on the bulleted list above.

23. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
24. Employ automated mechanisms to support the management of information system accounts.
25. Ensure that the information system automatically disables temporary and emergency accounts after usage.
26. Ensure that the information system automatically disables inactive accounts based on password and audit requirements.
27. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

4.0 Training and Awareness

4.1 Policy Statements

The College and the IT Department (as appropriate) shall comply with the following Basic Security Requirements:

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

3.2.1.1 The College shall schedule security awareness training as part of initial training for new users:

1. Schedule security awareness training when required by information system changes and then requirements for each system thereafter.
2. Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
3. Retain individual training records for training based on system requirements and archiving requirements.

3.2.1.2 The IT Department shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

1. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
2. Address awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

3.2.2.1 The IT Department shall provide role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties.
2. When required by information system changes and on a routine basis thereafter.
3. Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.
4. Provide comprehensive role-based training that addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined.
5. Provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.
6. Provide training to system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and other personnel having access to system-level software, security-related technical training specifically tailored for their assigned duties

3.2.2.2 The IT Department shall provide initial and ongoing training in the employment and operation of physical security controls:

1. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.
2. Provide physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).

3.2.2.3 The IT Department shall provide practical exercises in security training that reinforce training objectives:

a. Practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives.
b. Practical exercises should help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

The IT Department shall comply with the following Derived Security Requirements:

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

3.2.3.1 Provide training on recognizing and reporting potential indicators of insider threat.

3.2.3.2 Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

3.2.3.3 Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations.

3.2.3.4 Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

3.2.3.5 The IT Department may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

5.0 Audit and Accountability

5.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

5.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

3.3.1.1 The information system shall generate audit records containing the following content:

1. NIST-suggested content including: time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked.
2. Event outcomes may include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred).

3.3.1.2 Information systems owners shall create and retain audit logs and records to support the monitoring, analysis, investigation, and reporting of audit events, including the following:

1. Identify event types that are significant and relevant to the security of systems and the environments in which those systems operate.
2. Log events as necessary to cover related events when defining event types appropriate for each security requirement, including the steps in distributed, transaction-based processes (e.g. processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud- based architecture including Password changes, failed logons or failed access related to systems, administrative privilege usage, and third party credential usage.
3. Select the appropriate level of abstraction for each audit logging capability such that a root cause may be sufficiently identified.
4. Balance monitoring and auditing requirements with other system needs.
5. Coordinate the security audit function with other organizational entities requiring audit.

3.3.1.3 Stakeholders shall review, analyze, and update audited events as often as needed for indications of [entity defined inappropriate or unusual activity] and to provide important information to the College to facilitate risk-based decision making, but at a minimum annually..

3.3.1.4 Findings shall be reported to the CIO and the EWC President.

The College and its Stakeholders shall comply with the following Derived Security Requirements:

3.3.3 Review and update logged events.

1. Event types that are logged shall be periodically re-evaluated and may change over time.

3.3.4 Alert in the event of an audit logging process failure.

1. The audit and monitoring tool shall provide an alert on a predefined basis when the following audit failure events occur:

2. The auditing or oversight third party shall take the following actions in the event of a audit logging process failure:
    a. Alert CIO within one to two business days, depending on the criticality.
3. The information system shall provide a warning to the EWC CIO within one to two business days when allocated audit record storage volume reaches 75%, 80%, 85%, 90%, 95%, and 99% of repository maximum audit record storage capacity.
4. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

1. Information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
2. The information system owner shall ensure analysis and correlation of audit records across different repositories to gain situational awareness collectively across the organization. Correlation may be applied at the system level or at the organization level across all systems, as appropriate.

6.0 Configuration Management

6.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

6.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.1.1. The IT System Owner shall:

1. Develop, document, and maintain under configuration control, a baseline configuration reflecting agreed-upon specifications for systems or configuration items within the Colleges' enterprise architecture.
2. Review and continually update the baseline configuration as necessary throughout the respective system development life cycles as an integral part of future builds, releases, upgrades, and changes to systems based on security risks and deviations from the established baseline configuration,
3. Formally review and update the baseline configuration of the information system on a routine basis.
4. Retain one previous version of baseline configurations of information systems to support rollback.

3.4.1.2. Baseline configurations shall include the information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture.

3.4.1.3. If implementing centralized system component inventories that include components from multiple organizational systems, the resulting inventories include system-specific information required for proper component accountability including:

1. System association;
2. System owner;
3. Hardware inventory specifications;
4. Software license information;
5. Software version numbers;

1. Component owners;
2. machine names and network addresses for networked components or devices; and
3. Inventory specifications including manufacturer, device type, model, serial number, and physical location.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

3.4.2.1 IT System Owner shall:

1. Establish and document configuration settings for hardware, software, or firmware components of the system that affect the security posture or functionality of the system using common secure configurations that reflect the most restrictive mode consistent with operational requirements.
2. Identify, document, and approve any deviations from established configuration settings for critical and high priority systems.
3. Ensure the configuration settings are implemented and enforced.
4. Monitor and control changes to the configuration settings in accordance with policies and procedures.

1.1. Develop, document, and implement a configuration management plan for the information system that:

1.1.1. Defines the configuration items for the information system and places the configuration items under configuration management.

1.1.2. Addresses configuration management roles and responsibilities.

1.1.3. Defines detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level.

1.1.4. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

1.1.5. Establishes procedures that protect the configuration management plan from unauthorized disclosure and modification.

3.4.2.2 Common secure configurations may be developed by a variety of organizations including information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors.

3.4.2.3 Common secure configurations shall provide recognized, standardized, and established benchmarks that stipulate secure configuration settings and configuration instructions for the Colleges' information technology platforms/products including, but not limited to:

3.1. Mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers),

3.2. Network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), and

3.3. Operating systems, middleware, and applications.

3.4.2.4 Common secure configurations shall address security parameters for the following:

4.1. Registry settings; account, file, directory permission settings;

4.2. Settings for functions, ports, protocols, and remote connections; and

4.3. Specific configuration settings for systems derived from organization-wide configuration settings.

3.4.2.5 Established settings shall become part of the systems' configuration baseline.

The College and its Stakeholders shall comply with the following Derived Security Requirements:

3.4.4 Analyze the security impact of changes prior to implementation.

3.4.4.1 Prior to change implementation, the IT System Owner shall, together with College personnel with information security responsibilities (e.g., system administrators, system

security officers, system security managers, and systems security engineers) who conduct security impact analyses, analyze changes to the information system to determine potential security impacts.

3.4.4.2 Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls.

3.4.4.3 Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

3.4.4.4 Unless doing so inhibits the core functions of these systems or is otherwise not technically feasible, the IT System Stakeholders shall ensure:

1. The initial setup, software installation, and security configuration of new systems are performed in a secure environment isolated from other operational systems with minimal communication protocols enabled.
2. Changes to configurations are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation in accordance with the change management procedures.
3. A configuration monitoring process is in place to identify undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

3.4.5.1 The IT System Owner shall define, document, approve, and enforce physical access restrictions associated with:

1. Changes to the information system, including software libraries, physical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems); and
2. Change windows (e.g., changes occur only during certain specified times).

3.4.5.2 Only qualified and authorized individuals shall be permitted to access systems for purposes of initiating changes, including upgrades and modifications.

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

3.4.6.1. Where feasible, component functionality shall be limited to a single function per component and configured to provide only essential capabilities.

3.4.6.2. The IT System Owner and its Stakeholders shall ensure:

1. The information system is reviewed quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.
2. Disable unused or unnecessary functions, physical and logical ports and protocols, and services within the information system to prevent unauthorized connection of devices, transfer of information, and tunneling.
3. Prevent program execution in accordance with policies regarding software program usage, restrictions, and rules authorizing the terms and conditions of software program usage.

3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

1. The College shall make a security-based determination by defining essential ports, protocols and services. The College will define nonessential ports and these ports will be restricted, disabled, or prevented as defined.

3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

3.4.8.1 The IT System Owner shall employ processes to identify software programs authorized to execute on College Information Systems to prohibit the execution of unauthorized software programs including:

1.1. Identifying software programs not authorized to execute on information systems and apply a blacklisting (eg deny-all, allow-by-exception) policy.

1.2. Identifying software programs that are authorized to execute on systems and apply a whitelisting (eg allow-all, deny-by-exception) policy

1.3. Consider using cryptographic checksums, digital signatures, or hash functions to verify the integrity of whitelisted software programs.

1.4. Review and update the list of unauthorized software programs annually.

3.4.9 Control and monitor user-installed software

3.4.9.1. The IT System Owner shall maintain control over its software as follows:

1.1. Establish policies governing the installation of software, updates and security patches by users.

1.2. Enforce software installation policies through procedural and/or automated methods (e.g. controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting).

3.4.9.2. Monitor compliance of its software installation practices.

7.0 Identification and Authentication

7.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

7.1 Identify system users, processes acting on behalf of users, and devices.

3.5.1.1 The IT System Owners shall:
- 1.1. Uniquely identify users and processes acting on behalf of users, whether or not they are associated with system accounts.
- 1.2. Identify devices and define by type and/or device.

3.5.1.2 Select and assign a unique identifier to identify an individual, group, role, or device.

3.5.1.3 Ensure that the College manages information system identifiers by receiving authorization from the IT Department to assign an individual, group, role, or device identifier.

7.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

3.5.2.1 The IT System Owner shall:
- 1.1. Establish initial authenticator content for authenticators defined by the organization.
- 1.2. Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication
- 1.3. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
- 1.4. Require that the registration process to receive IT assets] be conducted in person or by a trusted third party before with authorization by the CIO.
- 1.5. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
- 1.6. Enforce authorized access to the corresponding private key.
- 1.7. Change default content of authenticators prior to information system installation.

3.5.2.2 The information system shall:
- 2.1. Support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication.
- 2.2. Issue and revoke, when no longer needed, authenticators for temporary access such as that required for remote maintenance, and device authenticators including certificates and passwords.
- 2.3. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.

2.4. For PKI-based authentication, validate certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
2.5. Map the authenticated identity to the account of the individual or group.
2.6. Leverage a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

The College and its stakeholders shall comply with the following Derived Security Requirements:

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

3.5.3.1 Information Systems shall require multi factor authentication at the system level (i.e., at logon) in the following scenarios:
1.1. for network access to privileged accounts.
1.2. for network access to non-privileged accounts.
1.3. local access to privileged accounts.
1.4. for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

3.5.3.2 Physical authenticators shall be required for hardware authenticators providing time-based or challenge-response authenticators and smart cards.

3.5.3.3 The Information System may employ authentication mechanisms at the application level, when necessary, to provide increased information security.

3.5.3.4 The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.

3.5.3.5 Commercially available tokens and biometrics, including those that may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials may be used.

3.5.3.6 Information systems shall accept and electronically verify Personal Identity Verification (PIV) credentials.

3.5.3.7 Information Systems shall employ only FICAM-approved information system components in EWC] to accept third-party credentials.

3.5.3.8 The IT System Owner shall ensure that information systems:
8.1. Uniquely identify and authenticate all devices before establishing a network connection.
8.2. Identify and authenticate non-entity users or processes acting on behalf of non-entity users.
8.3. Accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.
8.4. Accept only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

3.5.7.1 The IT System's password-based authenticators shall have the following minimum password requirements:

1.1. Passwords shall not contain the user's entire Account Name value or entire Full Name value.

1.2. Passwords shall contain characters from three of the following five categories:

1.2.1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);

1.2.2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);

1.2.3. Base 10 digits (0 through 9);

1.2.4. Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/; and

1.2.5. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

1.3. Passwords shall have a minimum length of 8 characters.

3.5.7.2 The IT System shall require at least one changed character when new passwords are created.

3.5.8 Prohibit password reuse for a specified number of generations.

3.5.8.1 The IT System shall prohibit password reuse for 12 generations.

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

3.5.9.1 The IT System shall allow the use of a temporary password for system logons with an immediate change to a permanent password.

3.5.10 Store and transmit only cryptographically-protected passwords.

3.5.10.1 The IT System shall store and transmit only cryptographically-protected passwords.

3.5.11 Obscure feedback of authentication information.

3.5.11.1 The IT Systems shall obscure feedback of authentication information during the authentication process where feasible and appropriate. (e.g. by Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.)

3.5.11.2 The College shall require individuals and devices to implement specific security safeguards to protect authenticators, as appropriate.

3.5.11.3 The feedback from systems does not provide any information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly.

8.0 Incident Response

8.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

8.1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

1. Incident handling shall be addressed during the definition, design, and development of the College's business processes and systems.
2. An incident handling capability shall be implemented for the detection and analysis, containment, eradication, and recovery from systems security incidents.
3. Incident response resource(s) shall be identified and made available to support users by providing security incident handling and reporting advice and assistance.
4. Incident-related information from available sources shall be analyzed and leveraged for detection of incidents, such as: audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events.
5. Incident handling activities shall be coordinated among business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.
6. College personnel shall receive training that includes content and level of incident response detail consistent with the user's assigned role and responsibility.
7. Incident response training should include the following, as appropriate to the user's role:
8. Knowing who to call and how to recognize an incident on the system;
9. How to handle or remediate incidents; and
10. Specific training on forensics, reporting, system recovery, and restoration.
11. Incident response training shall include the following:
12. Identification and reporting of suspicious activities from external and internal sources;
13. Available incident response assistance such as help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

1. Documentation of security incidents from all relevant sources shall be collected, tracked, and maintained. Sources may include, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.
    - 1.1. Incident reports shall include:
    - 1.1. the status of the incident and information necessary for forensics,
    - 1.2. evaluating incident details, trends, and handling; and
    - 1.3. Other content required by applicable laws, Executive Orders, directives, regulations, and policies.
    - 1.4. Personnel shall report the following types of security incidents to EWX CIO within one business day for critical and high risk events.
    - 1.5. Incident examples are included in operational procedures.

2. Suspected security incidents may also be reported (e.g. the receipt of suspicious email communications that can potentially contain malicious code).

The College and its Stakeholders shall comply with the following Derived Security Requirements:

3.6.3 Test the organizational incident response capability.

1. Incident response capability shall be tested bi-annually to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies.
2. Incident response testing may include:
    a. The use of checklists, walk-through or tabletop exercises;
    b. Simulations (both parallel and full interrupt);
    c. Comprehensive exercises; and
    d. A determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Refer to Section 25.0 for the Incident Response Plan and procedures.

9.0 Maintenance Policy

9.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

3.7.1 Perform maintenance on organizational systems.

1. The College shall schedule and perform all types of maintenance and repairs necessary to help ensure the availability and confidentiality of CUI. This requirement applies to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity, including those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

1. All maintenance activities shall be approved and monitored by College Personnel, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
2. System owners shall first approve the removal of the information system or system components from facilities for off-site maintenance or repairs.
3. System owners and IT shall approve, control, and monitor the use of maintenance tools, techniques, mechanisms, and personnel used for diagnostic and repair actions on IT systems that process, store, or transmit CUI.
4. Hardware, software, firmware, and other maintenance and testing tools shall be monitored for malicious code before being approved for use.

The College and its Stakeholders shall comply with the following Derived Security Requirements:

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

1. Any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement) shall be sanitized to remove all information prior to removal for off-site maintenance or repairs.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

1. Media containing diagnostic or test programs must be inspected to determine whether the media contains malicious code before being used in a system or system component.

2. If, upon inspection of media containing maintenance diagnostic and test programs, it is determined that the media contains malicious code, the incident shall be handled consistent with incident handling policies and procedures.

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

1. Individuals without access authorization who are performing hardware or software maintenance on organizational systems shall be supervised. Such individuals may be provided temporary credentials for one-time use or for limited time periods.

3.7.7 Testing for data integrity will be performed at regularly scheduled intervals by the backup hardware but may also be performed manually at random times to verify the validity, accuracy, and authenticity of the backup. These random tests should total no less than six per year and it is recommended that these tests fall approximately two months apart, less if more than the minimum number of tests are used. We encourage that backup tests be taken within one week of the completion of the yearly and mid- yearly backups with the remaining backups spaced throughout the remaining months of the year. If six are used, it should follow this testing schedule:

- Test 1 – January 1-7
- Test 2 – March 1-7
- Test 3 – May 1-7
- Test 4 – July 1-7
- Test 5 – September 1-7
- Test 6 – November 1-7

If more than six tests are used, then the schedule may be set at the discretion of the EWC IT Department, however, two of the tests must occur no later than one week after the yearly and mid-yearly backups are completed.

3.7.8 Methods of Testing Testing shall consist of one or more of the following methods of data validation and verification of accuracy and authenticity:

- Random Dummy File Restoration: Six to twelve dummy files are inserted on the file server at random locations. Afterwards, we will intentionally delete these dummy files. Then, recovery will be tested to verify data is being restored properly. If this verifies the data is being restored properly, the test is completed and the dummy file may be removed.
- Random Actual File Restoration: Recovery of a six to twelve actual random files located on the server. Comparisons will then be made with current versions of the same files to verify content and accuracy of restoration process. If the comparisons verify that the recovery was successful, then the test is completed.
- Random File Location Verification: Movement of a single dummy file to various locations on the file server. Initially the file is inserted onto the file server and backups are tested to verify the file exists in backups at the initial location. If this is confirmed, then the file is moved on the file server to a second location and backups are tested yet again to verify that the file is in the second location. Once this is confirmed, the file is moved for a third time and backups are once again tested to verify the file exists in the new location. If this is confirmed then the test is

completed and the dummy file may be removed. Backups are working correctly and file contents and locations are being updated appropriately.

- Miscellaneous: Other tests may be used at the discretion of the EWC IT Department with only one restriction: they may not interfere with access or otherwise cause any data loss on the file server.

Restoration Processes

All restoration processes will follow, at minimum, one of the following methods:

- Re-routing primary traffic from backup and storage device in Douglas to accompanying device in Torrington or vice-versa
- Physically transporting one device to another location
- Copying all files or a subset of files from the backup equipment to the file server
- Via the testing process described in this document Utilizing the EWC IT Department's Disaster Recovery Plan
- Utilizing the EWC IT Department's Backup Priority List
- Other methods, approved by the EWC IT Department, that do not interfere with access or otherwise cause any data loss on the file server If it is found that a scheduled backup process is incomplete or missing due to a hardware or software malfunction, then the backup will be completed as soon as possible and a hardware test will be needed to verify no long-term problems exist that may affect backups in the future.
- Should a hardware test yield results that indicate serious issues, then a replacement for the faulty hardware should be found as soon as possible in order to prevent such issues from occurring in the future.
- If these issues prevent backups from occurring, then the off-site backup device in Torrington will be transferred to primary backup duties and a secondary device should be purchased and then placed at Douglas to regain primary functionality. The following is the maximum number of backups and replications that the EWC IT Department will retain at any one time. Once these backups or replications reach the maximum count, the oldest will be recycled so that the newest may be retained.
- Hourly Backup Copies on file: 16 per day, 112 total or 7 days worth of data at hourly intervals Weekly Backup o Copies on file: 12 total or 12 weeks (approx. 3 months) worth of data at weekly intervals
- Monthly Backup or Copies on file: 3 per month, 36 total or 36 months (approx. 3 years) worth of data at monthly intervals
- Mid-Yearly Backup Copies on file: 3 total or 3 years worth of data at yearly (mid-year) intervals
- Yearly Backup o Copies on file: 3 total or 3 years worth of data at yearly (end-of-year) intervals Daily Replication o Copies on file: 32 total or 32 days worth of exact copies of existing data and backups replicated off-site in daily intervals Online log files are retained consisting of information for each backup or replication process, hardware/software errors, access issues, or other critical errors involving the backup hardware. These entries are also emailed to the EWC Backup email account for verification and notification.

10.0 Media Protection Policy

10.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

9.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

3.8.1.1 Access to digital media containing design specifications shall be limited to the project leader and individuals on the development team.

3.8.1.2 System media containing CUI shall be protected by conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library.

3.8.1.3 Media containing CUI shall be physically controlled and securely stored through a controlled media library, locked drawers, desks, or cabinets, as appropriate.

3.8.1.4 Access to CUI on system media shall be limited by physically controlling such media, including conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media.

3.8.2 Limit access to CUI on system media to authorized users.

3.8.2.1 Access to system media containing CUI shall be limited by physically controlling system media and secure storage areas such as controlled media libraries, locked drawers, desks, or cabinets, as appropriate.

3.8.2.2 Physical control of system media shall be maintained by conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media.

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

3.8.3.1 All digital and non-digital system media containing CUI shall be sanitized before disposal or release for reuse.

3.8.3.2 Sanitization techniques and processes shall remove all CUI from the media such that the information cannot be retrieved or reconstructed.

3.8.3.3 When system media cannot be sanitized such that CUI may be able to be retrieved or reconstructed from the media, the media shall be destroyed.

3.8.3.4 Discretion on the employment of sanitization techniques and procedures shall be used for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal.

3.8.3.5 Sanitization of non-digital media may include destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document.

The College and its stakeholders shall comply with the following Derived Security Requirements:

3.8.4 Mark media with necessary CUI markings.

3.8.4.1 All digital and non-digital system media shall bear security markings containing security attributes.

3.8.5 Control access to media containing CUI.

3.8.5.1 Media containing CUI shall be in controlled areas or spaces with physical and/or procedural controls sufficient to meet requirements established for protecting systems and information.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

3.8.6.1 Cryptographic mechanisms shall be used to protect the confidentiality of CUI stored on portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives) during transport unless such devices are protected by appropriate physical safeguards.

3.8.7 Control the use of removable media on system components.

3.8.7.1 Removable media types shall be restricted or prohibited for use on College-owned systems:

3.8.7.2 The following technical and nontechnical controls shall be used to control the use of restricted or prohibited media on College-owned systems:

2.1. policies, procedures, and rules of behavior;

2.2. Control the use of portable storage devices by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices;

2.3. Limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned;

2.4. Control the use of portable storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices.]

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

3.8.8.1 All portable storage devices shall have the device's owner readily identifiable on the device (e.g., individuals, organizations, or projects).

3.8.8.2 In the event of a security incident due in part to use of a portable device (e.g., insertion of malicious code), responsibility and accountability for addressing known vulnerabilities shall lay with the device's owner.

3.8.9 Protect the confidentiality of backup CUI at storage locations.

3.8.9.1 Backed-up information containing system-level or user-level CUI shall be protected by cryptographic mechanisms or alternative physical controls.

3.8.9.2 data and associated backups from the primary backup device in Douglas to the secondary backup device in Torrington. During a replication, all data and backups are replicated so that a mirror copy is retained at the Torrington location for off-site, backup capability should a disaster or other issues occur.

3.8.9.3 Regularly scheduled backups and replications shall be performed by the EWC IT Department using the following schedule:

- **Hourly Backups,** 7:00 a.m. – 10:00 p.m., every day, every hour as noted herein, on the hour
- **Daily.** All data is replicated from the Douglas Campus to the Torrington Campus. At the beginning of each day, beginning at 7:00 a.m., backups will begin and continue each hour, on the hour, until 10:00 p.m. each evening.
- **Weekly Backups** 10:30 p.m. Every Friday at 10:30 p.m., after the last hourly backup for that day, a weekly backup will be completed. At the end of each month, on the last day of the month, a monthly backup will be completed at 11:59 p.m. On July 1 of each year, at 12:30 a.m., a mid-yearly backup will be completed.
- **Monthly Backups:**11:59 p.m, Last day of each calendar month
- **Mid-Yearly backups,** 12:30 a.m, July
- **Yearly backups,** 12:30 a.m January 1, yearly backup will be completed. At 12:01 a.m. every morning, all backups and data will be replicated from Torrington to Douglas for off- site storage and secondary backup. All backups are clearly labeled so as to distinguish one from another easily. At minimum, the following information is provided for each backup file:
    - Time (MST) – e.g. 12:00:00 AM or 12:34:59 PM
    - Date – e.g. 12/31/10 or 2/29/12
    - Backup Type – e.g. Hourly or End of Year

11.0 Personnel Security

11.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

10.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

- 3.9.1.1 All personnel shall be screened prior to providing access to College systems containing CUI.
- 3.9.1.2 Screening shall include vetting activities designed to evaluate and assess the individual's trustworthiness, conduct, integrity, judgment, loyalty, reliability, and stability.
- 3.9.1.3 Screening activities shall reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for the individual's assigned roles & responsibilities.

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

- 3.9.2.1 This requirement applies to any personnel action involving a permanent or of such extended duration as to require protection of CUI, including terminations, transfers, and/or reassignments of individuals.
- 3.9.2.2 During and after the personnel actions, the following actions shall be timely executed.
  - 2.1. Terminate and/or revoke all authenticators and/or credentials associated with the individual for all systems containing CUI.
  - 2.2. Change system access authorizations (i.e., privileges);
  - 2.3. Close system accounts and establish new accounts;
  - 2.4. Retrieve all system-related property from the individual such as: hardware authentication tokens; identification card, keys, and building passes; and system administration technical manuals.
  - 2.5. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
- 3.9.2.3 For terminations, system accounts and/or access may be disabled prior to the individual being notified.
- 3.9.2.4 Where feasible, terminated employees should take part in an exit interview with their supervisor to ensure that:
  - 4.1. The individual is reminded of and understands the security constraints imposed by being a former employee, such as nondisclosure agreements and potential limitations on future employment.
  - 4.2. Appropriate accountability is achieved for system-related property.

12.0 Physical Access Policy

12.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

11..1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

3.10.1.1 Physical access to equipment (e.g. computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices) containing CUI shall be limited. Such equipment may be placed in locked rooms or other secured areas with only authorized individuals allowed access; or placing equipment in locations that can be monitored by College personnel.

3.10.1.2 A list of employees, individuals with permanent physical access authorization credentials, and visitors authorized to have access to non-publicly accessible physical or operating environments shall be maintained.

3.10.1.3 Individuals with authorized access to physical and operating environments shall possess credentials such as badges, identification cards, smart cards, and/or other physical access devices.

3.10.1.4 The EWC IT Department shall determine the strength of authorization credentials needed to physically access non-publicly accessible College facilities, operating environments, and organizational systems consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines.

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

3.10.2.1 Physical access to all facilities (including publicly accessible areas within organizational facilities), operating environments, and support infrastructure (e.g. system distribution, transmission, and power lines) of College systems shall be protected and monitored.

3.10.2.2 Physical access to facilities and operating environments may be protected and monitored by employing security guards, the use of sensor devices, or the use of video surveillance equipment such as cameras, or other methods, as appropriate.

3.10.2.3 Support infrastructure shall be protected to prevent accidental damage, disruption, physical tampering, eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

The College and its stakeholders shall comply with the following Derived Security Requirements:

3.10.3 Escort visitors and monitor visitor activity.

3.10.3.1 Visitors (i.e. individuals without permanent physical access authorization credentials) shall be escorted in the restricted areas defined in operational policies.

3.10.3.2 Procedural and/or automated audit logs may be used to monitor visitor activity.

3.10.5 Control and manage physical access devices.

3.10.5.1 Physical access devices (eg. keys, locks, combinations, and card readers) shall be controlled and managed to prevent unauthorized individuals from obtaining the output.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites.

3.10.6.1 Safeguarding measures shall be employed at alternate work sites where organizational systems and/or equipment may be located, such as government facilities, or the private residences of employees.

13.0 Risk Assessment Policy

13.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

- 3.11.1.1 System boundaries resulting from the operation of the College's systems and the associated processing, storage, or transmission of CUI shall be clearly defined for the purpose of conducting periodic risk assessments.
- 3.11.1.2 Formal and/or informal assessments of risk shall include:
  - 2.1. Assessment of threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems; and
  - 2.2. Assessment of risk posed by external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities).
- 3.11.1.3 Risk assessments may be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle, as appropriate.

The College and its stakeholders shall comply with the following Derived Security Requirements:
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

- 3.11.2.1 The IT Department shall determine the required vulnerability scanning for all system components (including potential sources of vulnerabilities such as networked printers, scanners, and copiers), and hosted applications.
- 3.11.2.2 Vulnerabilities to be scanned shall be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed.
- 3.11.2.3 Vulnerability scanning processes shall ensure that potential vulnerabilities are identified and addressed as quickly as possible.
- 3.11.2.4 Vulnerability scanning shall include:
  - 4.1. scanning for patch levels;
  - 4.2. scanning for functions, ports, protocols, and services that should not be accessible to users or devices;
  - 4.3. scanning for improperly configured or incorrectly operating information flow control mechanisms; and
  - 4.4. scanning of custom software applications using source code reviews and/or static analysis tools, web-based application scanners, binary analyzers, and/or other other analysis approaches, as appropriate.

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

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

3.11.3.1 Remediations of discovered vulnerabilities shall be prioritized with consideration of the related assessment of risk and the level of effort to be expended in the remediation for specific vulnerabilities.

14.0 Security Assessment Policy

14.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

3.12.4.1 System security plan(s) shall be developed and periodically updated that documents security-related information in established management and/or operational areas related to:

1.1. System boundaries;
1.2. Enterprise architecture and relationships with or connections to other systems;
1.3. System environments of operation;
1.4. System development life cycle;
1.5. Systems engineering and acquisition; and
1.6. How security requirements are implemented.

3.12.4.2 System security plan(s) shall contain:

2.1. Sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended;
2.2. Extensive references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained;
2.3. A high level description of how security plans relate to a set of security controls, and how security controls meet requirements set out in the system security plan(s); and
2.4. Information relevant for the purpose of making an overall risk management decision of whether third parties may choose to process, store, or transmit CUI on systems hosted by the College.

14.4 User Statements

- Separate user functionality from information system management functionality either logically or physically. Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.
- Prevent unauthorized and unintended information transfer via shared system resources. This control prevents information, including encrypted representations of information, produced by

the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

- Ensure that the information system protects against or limit the effects of the following types of denial of service attacks: [entity defined types of denial of service attacks] by employing [entity defined security safeguards].

- The information system restricts the ability of individuals to launch [entity defined denial of service attacks] against other information systems.

- Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

- Implement sub-networks for publicly accessible system components that are [physically; logically] separated from internal organizational networks, and connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

- Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.

- Deploy information systems that protect the [confidentiality; integrity] of transmitted information. This applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

- Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after [entity defined time period] of inactivity; this control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

- Establish and manage cryptographic keys for required cryptography employed within the information system in accordance with [entity defined requirements for key generation, distribution, storage, access, and destruction].

- Implement [entity defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal and state laws, directives, policies, regulations, and standards. Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

- Prohibit remote activation of collaborative computing devices.

- Provide an explicit indication of use to users physically present at the devices. Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

- Issue public key certificates under a [defined certificate policy] or obtain public key certificates from an approved service provider.

- Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.

- Define acceptable and unacceptable mobile code and mobile code technologies.

- Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

- Authorize, monitor, and control the use of mobile code within the information system. Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.

- Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

- Authorize, monitor, and control the use of VoIP within the information system.

- Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

- Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

- Ensure information systems that requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

- Ensure the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

- Employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server, to eliminate single points of failure and to enhance redundancy. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.

- Ensure the information system protects the authenticity of communications sessions. This control addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

- Ensure the information system protects the [confidentiality; integrity] of [entity defined information at rest]. This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

- Ensure the information system maintains a separate execution domain for each executing process. Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

The College and its stakeholders shall comply with the following Basic Security Requirements:

3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

3.13.1.1 Communications at external and key internal boundaries shall be monitored, controlled, and protected. Such boundary components include: gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, and encrypted tunnels implemented within the College's system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

3.13.1.2 External web communications traffic shall be restricted to designated web servers within managed interfaces.

3.13.1.3 External traffic that appears to be spoofing internal addresses shall be prohibited.

3.13.1.4 Unauthorized and/or unintended information transfer via shared system resources shall be controlled and prevented.

3.13.1.5 Commercial transmission services, third party-provided access lines, and other service elements shall be monitored for vulnerabilities and increased risk. Communications utilizing such services shall be monitored, controlled, and protected.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

3.13.2.1 Systems security engineering concepts and principles shall be applied to the development of new systems and systems undergoing major upgrades for the purpose of making systems and system components more trustworthy, secure, and resilient, while reducing risk to acceptable levels and allowing for more informed risk-management decisions.

3.13.2.2 For legacy systems, security engineering principles shall be applied to system upgrades and modifications to the extent feasible, given the system's current state of hardware, software, and firmware components.

3.13.2.3 Development of new systems and upgrades to existing system components shall include, where appropriate:

3.1. Developing layered protections;

3.2. Establishing security policies, architecture, and controls as the foundation for design;

3.3. Incorporating security requirements into the system development life cycle;

3.4. Delineating physical and logical security boundaries;

3.5. Ensuring that developers are trained on how to build secure software; and

3.6. Performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

The College and its stakeholders shall comply with the following Derived Security Requirements:

3.13.3 Separate user functionality from system management functionality.

3.13.3.1 User functionality shall be physically and/or logically separated from system management functionality (e.g. functions necessary to administer databases, network components, workstations, or servers).

3.13.3.2 Methods for separating user and system management functionality may include one or more of the following techniques, as appropriate:

2.1. Using different computers, different central processing units, different instances of operating systems, or different network addresses;

2.2. Virtualization techniques;

2.3. Web administrative interfaces that use separate authentication methods for users of any other system resources; or

2.4. Isolating administrative interfaces on different domains and with additional access controls.

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

3.13.4.1 Unauthorized and unintended information transfer via shared system resources (including encrypted representations of information) shall be prevented.

3.13.4.2 Information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) shall not be available to other current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system.

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

3.13.5.1 Sub-networks shall be implemented for publicly accessible system components that are [physically; logically] separated from internal networks.

3.13.5.2 Such networks (referred to as demilitarized zones or DMZs) shall be connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the College's security architecture.

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

3.13.6.1 A deny-all, permit-by-exception network communications traffic policy shall be applied to all inbound and outbound network traffic at the system boundary and at identified points within the system.

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

3.13.7.1 The system shall detect split tunneling and/or configuration settings that allow split tunneling in remote devices (e.g., notebook computers, smart phones, and tablets). If split tunnelling is detected, the organizational system shall prevent the remote device from connecting.

3.13.7.2 Remote devices shall be configured to disable split tunneling.

3.13.7.3 Remote devices' configuration settings shall be set so that the end user cannot change the device's configuration settings.

3.13.8 Encryption Algorithm Requirements (Non-NIST Reference)

1. Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
2. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
3. Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Consider RFC6090 to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

4. Requirements
    a. Critical systems shall adhere to the NIST Policy on Hash Functions.

b. Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
c. End points must be authenticated prior to the exchange or derivation of session keys.
d. Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
e. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
f. All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

5. Key Generation
    a. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
    b. Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

6. Compliance Measurement
    a. The IT Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.
    b. Any exceptions to the policy must be approved by the IT Team in advance.
    c. An employee found to have violated this policy may be subject to disciplinary action, up to an including termination of employment.

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.9.1 Information systems shall be configured to terminate internal and external network connections associated with a communications session at the end of the session or after of inactivity as defined in operational policies.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

3.13.11.1 FIPS- validated cryptography and/or NSA-approved cryptography shall be to support the protection of CUI.

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

3.13.12.1 Remote activation of collaborative computing devices shall be prohibited, except for the following:

1.1. Dedicated video conferencing systems that rely on one of the participants calling or connecting to the other party to activate the video conference.

3.13.12.2 Collaborative computing devices shall provide an explicit indication of use to users physically present at the device.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.14.1 VoIP within the College systems shall be authorized, and controlled

3.13.14.2 The IT Department shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

3.13.15 Protect the authenticity of communications sessions.

3.13.15.1 Authenticity of system-supported communication sessions, including validity of information transmitted and identities of parties, shall be protected.

15.0 System and Information Integrity Policy

15.1 Policy Statements

The College and its stakeholders shall comply with the following Basic Security Requirements:

3.14.2 Provide protection from malicious code at designated locations within organizational systems.

- 3.14.2.1 The system shall be protected from malicious code at designated system entry and exit points such as firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices.
- 3.14.2.2 Malicious code includes viruses, worms, Trojan horses, and spyware, regardless of the code's format, or method or medium used to gain access to the system (e.g. web accesses, electronic mail, electronic mail attachments, portable storage devices; and logic bombs, back doors, or other unauthorized code present in commercial off-the-shelf or custom-built software.
- 3.14.2.3 In addition to employing traditional malicious code protection mechanisms used to detect malicious code, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices shall be utilized to help ensure that software does not perform functions other than the functions intended.

3.14.3 Monitor system security alerts and advisories and take action in response.

- 3.14.3.1. Publicly available sources of system security alerts and advisories shall be monitored.
- 3.14.3.2. System security alerts and advisories from publicly available sources, software vendors, subscription services, and industry information sharing and analysis centers (ISACs) shall be monitored.
- 3.14.3.3. The College shall notify relevant internal authorities and external organizations in response to security alerts and advisories.

The College and its stakeholders shall comply with the following Derived Security Requirements:

3.14.4 Update malicious code protection mechanisms when new releases are available

- 3.14.4.1 Malicious code protection mechanisms shall be updated as new releases are available in accordance with configuration management policies and procedures.

3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

- 3.14.5.1 Systems shall be periodically scanned for malicious code.
- 3.14.5.2 Files from sources external to the College's systems shall be scanned for malicious code in real time as files are downloaded, opened or executed.

3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

- 3.14.6.1 Inbound and outbound communications traffic shall be continually monitored to detect attacks and indicators of potential attacks.
- 3.14.6.2 The system shall be externally monitored, to include the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection); and internally monitored, to include the observation of events occurring within the system (i.e. traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems).

3.14.6.3 Monitoring requirements (including the need for specific types of system monitoring and the granularity of monitoring information) shall be established based on the College's monitoring requirements and incident response program, organizational monitoring objectives, and the capability of systems to support such objectives.

3.14.6.4 Output from system monitoring shall serve as input to continuous monitoring and incident response programs.

3.14.6.5 Evidence of malicious code shall be used to identify potentially compromised systems or system components.

3.14.7 Identify unauthorized use of organizational systems.

3.14.7.1 Unauthorized use of organizational systems shall be identified as part of the College's continuous monitoring and incident response programs, and other security requirements.

16.0 Acceptable Use Policy and Guidance

16.1 Policy Statements

This policy establishes the acceptable usage guidelines for all EWC-owned technology resources. These resources can include, but are not limited to, the following equipment:

- Computers that include desktop computers, mobile devices, servers, etc.
- Network Equipment that include switches, routers, network and communications cabling, wall plates, wireless antennas, wireless bridge devices, fiber optic lines, fiber optic equipment, VoIP phones, etc.
- Audio/Video Equipment that include video codecs, HDTVs, document cameras, projectors, security cameras, miscellaneous cabling, digital cameras and camcorders, printers, copiers, fax machines, etc.
- Software that includes operating systems, application software, etc.
- Resources that include group drive file storage, website file storage, email accounts, social networking accounts, etc.

This policy applies to all employees, contractors, consultants, temporaries, and other workers at EWC, including any and all personnel affiliated with third parties, including vendors. This policy applies to all equipment that is owned or leased by EWC.

A trusted and effective information technology environment (“IT environment”) is vital to the mission of Eastern Wyoming College. To that end, the college provides an IT environment which includes an array of institutional electronic business systems, computing services, networks, databases, and other resources (collectively, “EWC IT resources” or “resources”). These resources are intended to support the scholarship and work activities of members of the college’s academic community and their external collaborators, to support the operations of the college, and to provide access to services of the college and other publicly available information.

This policy applies to all equipment that is owned or leased by EWC. While EWC's IT Department desires to provide a reasonable level of freedom and privacy, users should be aware that all EWC-owned equipment, network infrastructure, and software applications are the property of EWC and therefore are to be used for official use only.

Also, all data residing on EWC-owned equipment is also the property of EWCC and therefore, should be treated as such, and protected from unauthorized access. The following activities provide a general guideline to use EWC’s technology resources in an acceptable manner:

- All passwords used to access EWC systems must be kept secure and protected from unauthorized use.
- No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Do not transfer personally identifiable information on portable equipment and storage devices.
- Public postings by employees from a EWC email address should contain the following disclaimer stating that the opinions expressed are strictly their own and not necessarily those of EWC, unless

the posting is in the course of business duties with any views or opinions presented in this message are solely those of the author and do not necessarily represent those of Eastern Wyoming College. Employees of Eastern Wyoming College are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by electronic communications. Any such communication is contrary to EWC policy and outside the scope of the employment of the individual concerned. EWC will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising.

- All computers residing on the internal EWC network, whether owned by the employee or EWC, shall be continually executing approved virus-scanning software with a current, up-to- date virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders.
- Personally identifiable information cannot be sent via electronic means and should be transferred within the internal network or through secure VPN connections.
- Off-campus work should be completed via a secure VPN connection so that no data is transferred off-network.
- All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorized users from accessing secure files. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of CSC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CSC-owned resources.

Access to and usage of EWC IT resources entails certain expectations and responsibilities for both users and managers of the IT environment. These are stated below.

16.2 Purposes & Appropriate Uses

EWC IT resources are provided for college-related purposes, including support for the college's teaching, research, and public service missions, its administrative functions, and student and campus life activities.

Users are granted access to EWC IT resources for the purposes described in this Policy. Use should be limited to those purposes, subject to Section 2.3.

16.3 Password Guidance

All systems shall have strong passwords as described in the Access Control policy. Additional policy guidance for users is listed below:

- Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- NOTE: Please do not use either of these examples as passwords!

- Do not use the same password for EWC accounts as for other non-EWC access (e.g., personal ISP account, option trading, benefits, etc.). Do not share EWC passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential EWC information

List of Don’ts

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to a supervisor.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers.
- Don’t reveal a password to vendors.
- In short, don’t reveal a password to ANYONE.
- Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger, Internet Explorer, Firefox, Thunderbird).
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without proper encryption.
- Change passwords at least once every three months.
- If someone demands a password, refer them to this document or have them call the EWC IT Department to determine the validity of their request.
- If an account or password is suspected to have been compromised, report the incident to the EWC IT Department immediately and change all passwords as soon as possible.
- Password cracking or guessing may be performed on a periodic or random basis by the EWC IT Department or its delegates.
- If a password is guessed or cracked during one of these scans, the user will be required to change it.
- Never give your password out to anyone. This may or may not include your supervisor, a friend or relative, a student or part-time worker, or even a co-worker.
    - Administrative Rule 7.4.5 Application Development
- Application developers must ensure that their programs contain the following security precautions:
- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

16.4 Incidental Personal Use

Users may make incidental personal use of EWC IT resources, provided that such use is subject to and consistent with this Policy, including Article 3 of this Policy. In addition, incidental personal use of EWC IT resources by an EWC employee may not interfere with the fulfillment of that employee's job responsibilities or disrupt the work environment. Incidental personal use that inaccurately creates the appearance that the college is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

Users who make incidental personal use of EWC IT resources do so at their own risk. The college cannot guarantee the security or continued operation of any EWC IT resource.

16.5 User Responsibilities

Users are responsible for informing themselves of any college policies, regulations, or other documents that govern the use of EWC IT resources prior to initiating the use of EWC IT resources.

16.6 Use of Resources Accessed through EWC IT Resources

When using EWC IT resources or resources owned by third parties that are accessed using EWC IT resources, all Users must comply with all applicable federal and state laws, all applicable college rules, ordinances, and policies, and the terms of any contract or license which governs the use of the third-party resource and by which the User or the college is bound.

In amplification and not in limitation of the foregoing, Users must not utilize EWC IT resources to violate copyright, patent, trademark, or other intellectual property rights.

Users may not engage in unauthorized use of EWC IT resources, regardless of whether the resource used is securely protected against unauthorized use.

16.7 Privacy of Other Users

Users are expected to respect the privacy of other Users, even if the devices and systems by which other Users access EWC's IT resources, the content other Users place on EWC IT resources, or the identities and privileges (rights to access and use certain systems and/or data), of other Users are not securely protected.

Unauthorized use by a User of another User's personal identity or access (login) credentials is prohibited.

EWC IT resources have a finite capacity. Users should limit their use of EWC IT resources accordingly and must abide by any limits EWC places on the use of its IT resources or on the use of any specific IT resource. In particular, no User may use any IT resource in a manner which interferes unreasonably with the activities of the college or of other Users.

EWC IT resources may not be used to fundraise, advertise, or solicit unless that use is approved in advance by the college.

16.8 Partisan Political Activities

EWC IT resources may not be used to engage in partisan political activities on behalf of, or in opposition to, a candidate for public office.

EWC IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that does not affect the college's interests. EWC IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that affects the college's interests unless that use is approved in advance by the President.
These prohibitions do not apply to private devices that are attached to the college's network, provided that EWC IT resources are not used in a way that suggests the college endorses or supports the activity originating on the private device.

EWC IT resources may not be used to operate a business or for commercial purposes unless that use is approved in advance by the college.

EWC IT resources may not be used to support the operations or activities of organizations that are not affiliated with the College unless that use is approved in advance by the college.

16.9 Pornography and Sexually Explicit Content

Unless such use is for a scholarly or medical purpose or pursuant to a formal college investigation, Users may not utilize EWC IT resources to store, display, or disseminate pornographic or other sexually explicit content. This prohibition does not apply to private devices that are attached to the college's network. Child pornography is illegal. The use of EWC IT resources to store, display, or disseminate child pornography is absolutely prohibited. Any such use must be reported immediately to the Torrington or Douglas Police Department.

In operating its IT environment, the college expects Users to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-to-date and patched, and employing security measures on their personal devices.

16.10 Enforcement

Use of EWC IT resources is a privilege and not a right. A User's access to EWC IT resources may be limited, suspended, or terminated if that User violates this Policy. Alleged violations of this Policy will be addressed by the Chief Information Security Officer of IT or his/her designee.

Users who violate this Policy, other college policies, or external laws may also be subject to disciplinary action and/or other penalties. Disciplinary action for violation of this Policy is handled through the college's normal student and employee disciplinary procedures.

In addition to its own administrative review of possible violations of this Policy and other college policies, the college may be obligated to report certain uses of EWC IT resources to law enforcement agencies.

If the Chief Information Officer determines that a User has violated this Policy and limits, suspends, or terminates the User's access to any EWC IT resource as a result, the User may appeal that decision to

the Chief Information Officer (CIO). If the User believes that his/her appeal has not been appropriately addressed by the CIO, he/she may seek further redress as follows:

- if a student, through the Vice President for Student Affairs, or his/her designee;
- if a member of the faculty or academic staff, through the Vice President of Academics, or his/her designee;

Alleged violations of local rules will be handled by the local systems administrator, network administrator, or employee supervisor/unit manager, depending on the seriousness of the alleged violation. These individuals will inform and consult with the Chief Information Officer or his/her designee regarding each alleged violation of a local rule and the appropriate consequences for any violation of a local rule. Users who object to the limitation, suspension, or termination of their access to any EWC IT resource as a consequence of their violation of a local rule may appeal to the CIO.

The CIO may temporarily suspend or deny a User's access to EWC IT resources when he/she determines that such action is necessary to protect such resources, the college, or other Users from harm. In such cases, the CIO will promptly inform other college administrative offices, as appropriate, of that action. Local EWC IT resource administrators may suspend or deny a User's access to the local resources they administer for the same reasons without the prior review and approval of the CIO, provided that they immediately notify the Chief Information Officer of that action.

16.11 Security & Operations

The college may, without further notice to Users, take any action it deems necessary to protect the interests of the college and to maintain the stability, security, and operational effectiveness of its IT resources. Such actions may be taken at the institutional or local level, and may include, but are not limited to, scanning, sanitizing, or monitoring of stored data, network traffic, usage patterns, and other uses of its information technology, and blockade of unauthorized access to, and unauthorized uses of, its networks, systems, and data. Local and central institutional IT resource administrators may take such actions in regard to the resources they manage without the prior review and approval of the CIO as long as the actions involve automated tools and not direct human inspection.

16.12 Privacy General Provisions

Responsible authorities at all levels of the EWC IT environment will perform management tasks in a manner that is respectful of individual privacy and promotes User trust.

15.13 Monitoring and Routine System Maintenance

While the college does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of those resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities. The college may access IT resources as necessary for system maintenance, including security measures.

The college's routine operation of its IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic, and perform other

essential administrative tasks. The creation and analysis of this information may occur at central institutional and local levels.

The college may, without further notice, use security tools and network and systems monitoring hardware and software.

The college may be compelled to disclose Users' electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation, and requests for public records under the Wyoming Freedom of Information Act ("WYFOIA").

The college reserves the right to monitor and inspect Users' records, accounts, and devices as needed to fulfill its legal obligations and to operate and administer any EWC IT resource. The college may disclose the results of any general or individual monitoring or inspection of any User's record, account, or device to appropriate college authorities and law enforcement agencies. The college may also use these results in its disciplinary proceedings.

15.14 General Provisions Regarding Inspections and Disclosure of Personal Information

In order to protect User privacy, the CIO or his/her designee must review and approve *any* request for access by a person to an individual User's personal communications or electronically stored information within EWC IT resources.

Incidental access to the contents of an individual User's personal communications or electronically stored information resulting from system operational requirements described elsewhere in this Policy does not require the prior review and approval of the CIO.

The college, acting through the CIO, may access or permit access to the contents of communications or electronically stored information:

When so required by law. If necessary to comply with the applicable legal requirement, such disclosures may occur without notice to the User and/or without the User's consent.

In connection with an investigation by the college or an external legal authority into any violation of law or of any college policy, rule, or ordinance. When the investigational process requires the preservation of the contents of a User's electronic records to prevent their destruction, the CIO may authorize such an action.

If it determines that access to information in an employee's electronic account or file is essential to the operational effectiveness of a college unit or program and the employee is unavailable or refuses to provide access to the information.

If it receives an appropriately prepared and presented written request for access to information from an immediate family member or the lawful representative of a deceased or incapacitated User.
If it must use or disclose personally identifiable information about Users without their consent to protect the health and well-being of students, employees, or other persons in emergency situations, or

to preserve property from imminent loss or damage, or to prosecute or defend its legal actions and rights.

16.15 Transporting Confidential Data

- Members of the Community are strongly discouraged from removing records containing Confidential data off campus. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any unsecure location.

- When there is a legitimate need to provide records containing Confidential data to a third party outside Eastern Wyoming College, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

16.16 Destruction of Confidential Data

- Records containing Confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.

- Paper and electronic records containing Confidential data must be destroyed in a manner that prevents recovery of the data. Massachusetts General Law 93I specifies the manner in which records containing PI must be destroyed.

16.17 Traveling Abroad with Students' Personal Information

- In the event that transmission of student passport information is required by the hotel or program abroad in advance of the travel, only the relevant information requested (e.g., Name, Passport Number, Date of Expiry, and Date of Birth) will be provided, not complete copies of the passport images. This information should first be transmitted via fax *or through eFax Secure website (SSL)*, provided that the Eastern Wyoming College department arranging the travel confirms the accuracy of the fax number by sending an initial confirmation message before the actual data. If faxing is unavailable, the data may be sent via Eastern Wyoming email, provided that the same confirmation of transmission takes place.

- Faculty/staff who need to retain these passport numbers for arranging travel will store this data in spreadsheets that are saved on the College's secure Vault server. Any spreadsheets containing student passport information should be routinely deleted by the spreadsheet owner when no longer needed.

- Faculty/staff who are traveling with the students abroad that need student passport and visa information for hotel check-in will keep a paper record on their person that contains relevant information (such as the passport and visa numbers and their expiry dates) and the last names of the students only. Faculty/staff must not retain or travel with copies of student passports.

- In extreme circumstances involving travel to a remote location where access to technology would be limited and would prohibit retrieval of a lost passport, a program director may request an exemption to this policy allowing for him or her to retain copies of the students passports during travel. This request will be made to the Chief Information Officer for approval. If the request is approved, the program director will sign the "Faculty/Staff Agreement for Traveling with Secure Data" to acknowledge their understanding of the WISP and their responsibilities in protecting the passports. The program director also agrees to alert LTS immediately if the copies of passport are lost.

16.16 Wireless Communications

Wireless implementations are a benefit to EWC as well as its' faculty, staff, and students. Maintaining this equipment can be a tedious process but is a necessity. At present, this policy allows access to the EWC wireless network via any data communication device containing the hardware required to connect. Connecting to the WC wireless network does not grant a user access to the internal networking infrastructure or any internal information of EWC, only external access to the internet. Utilizing EWC's wireless network for access to the internal network and/or information requires additional software that must be obtained through the EWC IT Department. This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of EWC's wireless networking access points. This includes any form of wireless data communication device capable of transmitting packet data.

All wireless data communication devices connected with EWC's wireless network will be required to have current virus-scanning software installed with the most recent updates and perform a full system scan a minimum of once per week. All wireless data communication devices connected with EWC's wireless network that require access to EWC's internal network and/or information will be required to utilize specific software and/or access credentials obtained through the EWC IT Department to do so. At no time shall any device connected to the EWC wireless network operate outside the parameters defined in the Acceptable Use Policy provided by EWC. All wirelessly connected devices may be monitored and their information such as IP address, MAC address, general hardware profile, etc. be archived for future use. Random scans may also be performed to ensure the security of the wireless networks and connected devices and to obtain a general device survey to further enhance the accessibility and usability of EWC's wireless networks.

17.0 Accessibility Policy

This policy establishes the accessibility guidelines for all EWC-owned technology resources. The purpose of this policy is to ensure that every EWC student is presented with an equal opportunity to learn and that all employees can adequately use the required technology equipment for the purpose of their required occupation.

17.1 Requirements

These requirements must be met where any learning impairment exists for any EWC student or work limitation exists for any EWC employee. These types of accessibility requirements may include, but are not limited to, the following applications or devices:

- Screen reading software
- Screen magnification software
- Stereo headsets or other sound devices

This rule applies to all EWC-owned technology resources in labs and other learning areas for student use and in departmental or teaching areas for employee use. A reasonable attempt shall be made at all times to address the needs of our students and employees, particularly when those needs are due to an accessibility issue presented by a physical impairment or learning disability of some kind.

The EWC IT Department shall make every effort to ensure that each and every student is presented with an equal or comparable learning environment regardless of the hurdle they may face. The EWC IT Department will always strive to offer technology solutions that help improve the learning environments for all students but will be particularly diligent in ensuring that no student will be unable to learn within a classroom due to a physical impairment or learning disability of some kind. The same will be provided for any employee requiring accommodation due to a physical impairment or learning disability of any kind. Please note that advance notice of these needs is required and may change due to the request. For instance, additional software needs will take some time to produce an order and install the software so it will be unreasonable to expect a request such as this to have an immediate turnaround time. Casting aside the general expectations above, the EWC IT Department cannot be held liable for issues surrounding software application issues, hardware failures, or the inability of employees or students to convey their respective needs in a reasonable amount of time to allow such software or hardware to be properly installed. With that said, the EWC IT Department will continually strive to ensure that all learning environments have the necessary technology and are adequately structured in a way to provide the most conducive learning environment possible, regardless if a learning disability or physical impairment may be present for any student. The EWC IT Department will also ensure that all employee areas are adequately designed to facilitate a productive working environment as well.

17.2 Other Data Storage

Every effort shall be made by the individual departments and employees at EWC to store sensitive, important, and confidential data on their respective group drive. As mentioned above, the EWC IT Department cannot be held liable for issues with data stored elsewhere. Regular backup schedules are in place within the group drive storage device to ensure that backups occur at regular intervals and over

a time span to provide ample opportunity for the EWC IT Department to recover a file, folder, or group of such.

17.3 Notification of Corruption

It should be noted that the EWC IT Department does require immediate notification in the event a file, folder, or collection of either is found to be missing, corrupt, or otherwise damaged. Waiting to inform the EWC IT Department decreases the probability of successful recovery. Specific information regarding backup restoration on an institution scale can be found in the EWC IT Department's Disaster Recovery Plan or the associated Backup Priority List (in progress). These deal with catastrophic recovery needs that affect multiple departments or the institution as a whole. T One device is placed in the server area of the ITS Department on the Douglas Campus to serve as a primary storage and backup device while the other is placed in the server area of the ITS Department on the Torrington Campus to serve as an off-site backup and replication device. The primary device in Torrington holds all data and backups and serves as the primary device for file access and immediate backup. The secondary, off-site device in Douglas replicates all data from the Torrington device to create a stable off-site copy of the data and backups present on the Torrington device. For this document, considering the type of hardware described above, normal backups do not necessarily retain the same meaning as when used in conjunction with other hardware devices. Because of this, the following descriptions are provided, based on the current hardware being used, so as to better understand the overall backup process.

17.4 Remote Access

All users needing access to EWC or other applications requiring network connectivity to the campus can facilitate this by connecting from home via a VPN connection. This type of connection establishes a secure, encrypted connection, to the campus network to allow the user to manipulate and access the data at a distance. At no time should any PII be transferred off- campus on any type of device.
If a given user wishes to work while off-campus, he/she should use the enclosed Remote Access Procedure to obtain a secure connection to the network and work from a distance. This type of connection allows the user to remotely manipulate and access the data without actually transferring any data off-site thus ensuring all PII and other data is kept safe and secure from unauthorized access.

18.0 Electronic Communications

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:

- Email
- VoIP
- Videoconferencing
- 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:

- is always understood to represent an official statement from the institution
- 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
- shall not be used for personal gain
- shall not be used extensively for personal use
- shall not be used to distribute malicious or harmful software or information

18.1 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.

18.2 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.

18.3 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.

18.4 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.

19.0 Emergency Notification Policy

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.

19.1 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
- Torrington Campus Administrators
- Vice President for Student Services
- Vice President of Academic Services
- Other designee deemed necessary by the President

20.0 Clean Desk Policy

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information. The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our students and our vendors is secure in locked areas and out of site. A Clean Desk policy is part of standard basic privacy controls that apply to all Eastern Wyoming College employees and affiliates.

20.1 Requirements

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

19.2 Compliance

The IT Team and College Supervisors will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the CIO.

21.0 Enforcement Policy

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.

21.1 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

22.0 Equipment Configuration and Equipment Ordering

This policy has been established to create a standard configuration for all technology resources at EWC. Because of the variances between the types, makes, models, configurations, builds, versions, and brands of technology resources available, it is necessary to standardize all technology resources to make service and maintenance easier.

22.1 Equipment Recommendations

All employees shall order and utilize equipment that is serviceable and recommended by the EWC IT Department. Since equipment availability changes over time, especially when referring to technology, a comprehensive list indicating appropriate hardware would be virtually impossible to create. Because of this, any individual or department wishing to purchase technology equipment should first consult a EWC IT Department personnel member for current specifications for any given piece of equipment. This applies to any and all technology equipment including, but not limited to:

- Computers (Servers, Desktop, Laptop, Tablets and Mobile Devices, etc.)
- HDTVs Printers, scanners, copiers, fax machines, or all-in-one devices
- Projectors, screens, and SmartBoards
- VoIP phones
- Digital cameras and camcorders
- Software (Application, Operating System, Network-Based, etc.)
- Other technology equipment not specifically mentioned here For more details on procedures required to place an order for technology equipment, please see the Equipment Ordering Procedures included in this document for detailed instructions.

22.2 Equipment Ordering Procedure

This procedure serves as guidance for all EWC Faculty and Staff who choose to order computing equipment. The following steps shall be taken:

1. Contact the EWC IT Department to obtain a quote and or information regarding the equipment you wish to purchase.
2. For Dell computers and some other specific technology equipment, the IT Department has the existing costs.
3. Submit your order and preferences to EWC IT Department.
4. Your order will be routed through the appropriate approving channels, including the ITS Department, since it is a technology equipment purchase.
5. Once your order has been approved, EWC IT will order it.
6. When your equipment arrives, the EWC IT Department will notify you that your equipment is in and will configure it, if necessary, prior to delivering it to you.

NOTE: All technology orders must be received by the EWC IT Department before it can be released to the purchaser. This is to ensure that the proper software is installed and all equipment is properly tagged and placed in inventory.

23.0 Guest/Visitor Access and Technology Use

EWC maintains an atmosphere that is open and allows guests and visitors access to 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 the internal network.

Policy Guest and visitor access shall be classified into two types as described below:

- Standard – Access granted to internet resources and institutional resources located online.
- Special – Access granted above plus any internal access as requested by an individual with the authority to do so from the Vice President for Administrative Services, Vice President for Academic Services, President, Chief Information Officer or other designee deemed necessary by the President.

Internal Access may include:

- Wireless VLANs (i.e. ewcwireless, ewcguest)
- Wired VLANs (i.e. housing, guest)
- Singular or multiple file access
- System access such as Canvas, ID Card System, etc. Under no circumstances should visitors be given special access unless permission has been obtained from the appropriate administrative personnel (i.e. a signature from one of the personnel above) along with detailed description of access. To obtain guest/visitor access users should contact the EWC IT Department with their requested system access requirements using the attached Authorization of User Access form. For vendor access, please see the appropriate vendor access policy included herein.

24.0 Information Sharing

24.1 Illegal File Sharing

Legal compliance is a primary focus at EWC. Because of this, we have set forth this policy which addresses illegal file sharing legislation, legal alternatives to illegal file sharing, and penalties for violating state and federal copyright laws. This policy applies to all EWC employees, students, vendors, or visitors utilizing EWC-owned computers, equipment, or the EWC network. Policy File sharing (peer-to-peer) software programs have led to significant increases in anti-piracy efforts and legislation.

24.2 Copyright Ownership

Peer-to-peer software allows the sharing of files often consisting of copyrighted content such as music, movies, and software which usually occurs without the consent of the owner. It is the policy of EWC to respect copyright ownership and protections given to authors, owners, publishers, and creators of copyrighted work. It is against EWC policy for any employee, student, affiliate, or visitor to copy, reproduce, or distribute any copyrighted materials on EWC-owned equipment or the EWC-managed network unless expressly permitted by the owner of such work. EWC also discourages the use of any file-sharing program as these types of programs may allow copyrighted material to be downloaded to a EWC-owned computer or device.

Many of these programs automatically place downloaded files in a shared folder on your computer, which means you could be sharing files without your knowledge. This also means that you may be held responsible for illegal file sharing, whether you are aware that copyrighted files are being shared or not. EWC also employs the use of network appliances, equipment, and rules to limit the amount of file-sharing traffic on the EWC network. Active blocking of peer-to-peer traffic is used to protect the EWC network from unwanted traffic and the presence of potentially malicious files introduced through file-sharing programs.

EWC encourages employees, students, affiliates, and visitors to utilize legal alternatives to illegal file sharing. There are a variety of free and pay-per-use options available that can be used instead of illegal file sharing programs. EWC leaves it to the discretion of the employee, student, affiliate, or visitor to decide which alternative to utilize.

24.3 Information Sensitivity

Information sensitivity is a primary focus at EWC. Since we are an educational entity, we deal with many different types of information, some for public use, some not. To make these distinctions, this document will address both types of information. This policy is intended to help employees determine what information can be disclosed to non- employees, as well as the relative sensitivity of information that should not be disclosed outside of EWC without proper authorization.

24.4 Sharing of Information

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and

information shared orally or visually (such as via phone and videoconferencing). All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect confidential information (e.g. confidential information should not be left unattended in conference rooms.). NOTE: The impact of these guidelines on daily activity should be minimal. Questions about the proper classification of a specific piece of information should be addressed to your supervisor or the EWC IT Department. Questions about these guidelines should be addressed to the EWC IT Department.

24.5 Public Information

By grouping information into two different categories, we can adequately address the needs of each type of information. The first type, public Information, is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the institution.

24.6 Confidential Information

The second type, confidential information contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as specific personnel information, student data, billing information, etc. Also included in confidential information is information that is less critical, such as telephone directories, personnel information, etc., which does not require as stringent a degree of protection.

24.6 Third-Party Confidential Information

A subset of the latter is third-party confidential information. This is confidential information belonging or pertaining to another corporation which has been entrusted to EWC by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into EWC's network to support our operations. EWC personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor and/or the EWC IT Department for more information and instructions on how this information should be handled.

24.7 Sensitivity Guidelines

The sensitivity guidelines below provide details on how to protect information at various sensitivity levels. Use these guidelines as a reference only, as EWC Confidential Information at each level may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the EWC Confidential Information in question.

Minimal Sensitivity Description: General information, some personnel, and technical information.

- Access: EWC employees, associates, or third-parties with a business need to know.
- Distribution internal to EWC: Approved electronic mail and approved electronic file transmission methods.
- Distribution external to EWC: Approved electronic mail and approved electronic file transmission methods.
- Storage: When viewing data, do not allow viewing by unauthorized individuals. Do not leave data open and/or unattended in any format. Protect data from loss, theft, or misplacement. Electronic information should have individual access controls where possible and appropriate.
- Disposal/Destruction: Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

Medium Sensitive Description: Business, financial, technical, and most personnel information.

- Access: EWC employees, associates, or third-parties with signed non-disclosure agreements with a business need to know.
- Distribution internal to EWC: Approved electronic file transmission methods.
- Distribution external to EWC: Approved electronic file transmission methods via a private link to approved recipients external to EWC locations.
- Storage: Individual access controls are highly recommended for more sensitive electronic information.
- Disposal/Destruction: Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

Critical Sensitive Description: Operational, personnel, financial, source code, & technical information integral to the security of the institution.

- Access: Only those individuals (EWC employees and associates) designated with approved access and signed non-disclosure agreements.
- Distribution internal to EWC: Approved electronic file transmission methods.
- Distribution external to EWC: Approved electronic file transmission methods to recipients within EWC. Strong encryption is highly recommended.
- Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored on a physically secured computer.

- Disposal/Destruction: A necessity. Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

25. Physical Security Guidelines

This policy will establish physical security guidelines that apply to all computing and networking equipment locations. It is important to note that incremental degrees of security will be needed for each area depending on the actual equipment configuration and critical need to the institution.

25.1 Classification

All areas will be classified into two categories:

- Office Areas
- Restricted Office areas are simply that, office locations for EWC IT Department employees. The areas contain computing equipment and other data that should be protected at all times. Restricted areas are those areas that belong to the EWC IT Department and contain equipment owned and/or operated by the EWC IT Department or a third-party vendor such as:
    - Switch closets
    - Server rooms
    - Telecommunications rooms
    - EWC IT Department storage areas
    - At the time of this policy, our current physical security offerings are somewhat limited so more advanced options cannot currently be used. As upgrades occur, recommended options will be changed to required options to increase and enhance security.
    - At minimum, all office and restricted locations require the following security mechanisms:
    - Solid wood or steel door
    - Either keyed handle or deadbolt lock
    - All EWC IT Department restricted and office locations should contain the following recommended security mechanisms:
    - Reinforced steel doors and frames
    - Keyed deadbolt locks
    - ID card access
    - Steel bars over windows

26.0 Incident Response Management

26.1 Background

The Eastern Wyoming College Data Information Security and Privacy Incident Response Plan outlines the College's actions following a data breach or other type of data related incident in order to ensure timeliness of response, compliance with applicable laws and regulations and ensure consistency in all aspects of the College's response. Information security and privacy is everyone's responsibility. All EWC Personnel and Persons of Interest (POIs) are covered by this administrative regulation.

The number of data breaches worldwide increases every year as a result of hackers attempting to capture confidential and/or protected information. Academic institutions are at risk because of the kinds of sensitive information they maintain. Data breaches can occur anywhere that information resides, including computer systems, portable media, paper records, automated HVAC systems, etc.

Eastern Wyoming College is committed to protecting the privacy of its community, which includes safeguarding the sensitive and protected data that is owned and maintained by the college. Eastern Wyoming College has taken many steps to reduce the risk of breach of such data, many of which are outlines in the College's Written Information Security Program (WISP). However, no protection is foolproof, and many data breaches occur as a result of human error. Therefore, Eastern Wyoming College must be prepared to respond to a breach in the event that one should occur.

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

25.2 Purpose

In accordance with federal and state laws and regulations, Eastern Wyoming College is required to provide notice about security breaches of protected information at the college to affected individuals and appropriate state agencies. Eastern Wyoming College is also committed to protect other kinds of sensitive institutional information that is maintained at the College. In the event that sensitive and/or protected information at Eastern Wyoming College is exposed as a result of a breach, the College must take steps to:

- Prevent further exposure

- Investigate the incident and support law enforcement if criminal activity is suspected
- Determine any legal obligations
- Notify the departments and individuals affected
- Respond to media inquiries
- Document any responsive actions taken
- Conduct a post-incident review of these actions

Accomplishing the above tasks will necessarily involve individuals from diverse areas of the College and will require that a plan be in place to address a breach before it occurs. The purpose of this plan is to outline the College's response to a data breach, including procedures for reporting a breach and individual team member's responsibilities following a breach.

26.3 Scope

The Incident Response Plan addresses four types of information compromises:

1. Computing devices compromised by Malware
2. Computing devices compromised by Unauthorized Access (includes any devices accessed without permission, either by stolen or compromised credentials, or other attempts to access a device without authorization)
3. Lost or Stolen Computing devices
4. Lost or Stolen Paper Records containing Confidential Data, as defined below.

The scope includes all computing devices (both College-owned and personal), including computers, servers, portable media, external hard drives or other mobile devices and all paper records, which contain Confidential data. **All Eastern Wyoming College employees that maintain or access Confidential data, both paper and electronic, at the college must comply with the plan.**

26.4 Definitions

Breach of security: The unauthorized acquisition or use of sensitive or protected data that creates a substantial risk of identity theft, fraud or harm to the reputation or business interests of an individual or institution.

Compromised computer: Some ways a compromised computer can be identified include: the computer user suspects that his/her system is exhibiting suspicious behavior or has suspicious files stored on the device; network or system logs indicate unusual network behavior coming from or going to the device; or individuals at Eastern Wyoming College or outside the College report cyber-attacks or unusual network behavior emanating from the device.

Confidential data: Refers to any information, both paper and electronic, that is protected by Federal, state, or local laws and regulations, or other sensitive personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operation or reputation of Eastern Wyoming College. Protected data includes Personal Identifiable Information (defined below), student education records, Protected Health Information (PHI). For a more complete description of these terms and the types of data

identified as Confidential, see the College's Written Information Security Program (WISP) and the related policies cross-referenced at the end of this document.

Personal Identifiable Information: Personal Identifiable Information (PII) is the first and last name, or first initial and last name of a person in combination with any one or more the following: 1) Social Security number; 2) Driver's license number or state-issued identification card number; 3) Account number, credit or debit card number, in combination with a linked security or access code or password of an individual's financial account; 4) Tribal identification card; 5) Federal or state government-issued identification card; 6) Username or email address, in combination with a password or security question and answer that would permit access to an online account; 7) Birth or marriage certificate; 8) Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; 9) Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person, or information related to a person's application and claims history; 10) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; 11) Individual taxpayer identification number; 12) A Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.

Eastern Wyoming College employees: Includes all Eastern Wyoming College employees, whether full-time or part-time, including faculty, administrative staff, contract or temporary workers, hired consultants, interns and student employees.

26.5 Responsibilities

The College's Chief Information Officer is charged with the identification of all data security incidents involved in electronic data or paper records where the loss, theft, unauthorized access, or other exposure of Confidential data is suspected. When the CIO confirms an incident involving Confidential electronic data, the CIO will contact the Chair of the Data Incident Team- the President who will convene the Data Incident Team. In the event the President is unavailable, the Vice President for Finance and Administration will assume the role of the Chair in his or her absence. The Chair of the Team is responsible for coordinating the Data Incident Team and determining appropriate actions in their response to the breach.

This applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information (PII) or Protected Health Information (PHI) of Eastern Wyoming College members. Any agreements with vendors will contain language.

The Data Incident Team includes members from:

- Chief Information Officer
- IT Department
- VP of Finance and Administration
- Legal Consultants (both for EWC and Insurance Company)
- College Relations

- And other members or the affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional individuals as deemed necessary by the CIO
- Confirmed theft, breach or exposure of Eastern Wyoming College data

General responsibilities of the DIT:

- Take charge of the incident response.
- Inform General Counsel and the EWC Board of Trustees if an actual or suspected Security Incident has been reported and provide them with an overview of the situation.
- Lead the investigation and the remediation and mitigation efforts.
- Triage each actual or suspected Security Incident.
- Contact the individual who reported the actual or suspected Security Incident.
- Determine the nature and scope of the actual or suspected Security Incident.
- Take steps to ensure that communications among DIT members and with the President and any other EWC executives are confidential and, where appropriate, subject to the attorney-client privilege.
- Determine and engage other members of the DIT in the investigation of and response to an actual or suspected Security Incident as needs dictate.
- Determine whether or when it is appropriate to notify EWC's network security and privacy coverage insurance carrier.
- Be solely responsible for communicating and coordinating with EWC's network security and privacy coverage insurance carrier.
- Determine whether there are possible criminal aspects to the actual or suspected Security Incident and, if so, contact local police department.
- Coordinate responsibilities among themselves and other DIT.
- Develop a communication plan appropriate for the circumstances including formulating as needed public or internal messages about an actual or suspected Security Incident with the approval of the President and College Relations.
- Make operational, security, and other related business decisions relating to the actual or suspected Security Incident after receiving input from members of the DIT, if appropriate.

The President will oversee the investigation of the incident and involve legal counsel, insurance companies, local, state and federal law enforcement as necessary. The severity of the breach will determine the nature of the investigation, including what authorities are involved and how evidence is collected.

The CIO will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the CIO's office.

All Eastern Wyoming College employees are responsible for identifying and reporting potential security breaches. For help with security issues, including descriptions of the various types of breaches and how to report them, please talk with someone in IT.

26.6 Response Plan

This administrative rule mandates that any individual who suspects that a theft, event, incident, including a breach or exposure, must immediately provide a description of what occurred via e-mail to tvasko@ewc.wy.edu or by calling 532-8235. The IT Team will investigate all reported theft, events, incidents, breaches, or exposure, and the Chief Information Officer will follow the appropriate procedure in place.

For suspected breaches, the CIO will:

1. Conduct a preliminary investigation: Gather details about the incident, including when the breach was first discovered and how the employee responded. In cases involving electronic data, the CIO will also inquire about symptoms of the compromised computing device.
2. **Determine if Confidential data was involved:** Inquire about the nature of records or data involved in the breach and what kinds of information it contained. For electronic data breaches, the CIO will use a variety of technologies to determine if Confidential data was present on the compromised device. If the computing device was stolen, the CIO will do the analysis on backups. If backups are not available, the severity of the incident will be classified based on access to various sensitive data.

If an incident involving Confidential data is confirmed, the CIO will contact the President. The President will:

1. **Notify Senior Staff:** Provide details about the incident and provide status updates.
2. **Convene the Data Incident Team (DIT):** If PII, PHI or student education records were determined to be involved in the data breach, or if the presence of sensitive data could not be ruled out, the incident team will be convened.
3. **Consult Legal Counsel**: The President will consult the College's legal counsel to review the incident to determine the College's legal obligations for reporting under applicable federal and state laws.
4. **Notify affected individuals**: The College is required to notify any individuals whose personal information or protected health information (respectively) may have been compromised as a result of this incident (regardless of confirmation of identity theft). Depending on the breach, the College may be obligated to notify other individuals and agencies as prescribed as law. The nature of the breach will also determine the method(s) of notification.
5. **Notify College Insurance Company**: The College carries cyber security insurance and the insurance company will provide additional assistance with resources needed for the College.

26.7 Incident Response Steps

The EWC DIT will generally follow the steps identified below in responding to incidents. Notably, after the initial assessment commences, some components will proceed simultaneously.

Additionally, these steps in practice may change if EWC network security and privacy insurance carrier is involved in the matter. For instance, EWC insurance carrier may direct that EWC hire outside legal counsel to assist with the legal issues surrounding the actual or suspected Security

Incident in which case EWC General Counsel and the President will jointly supervise the work of that counsel.

The steps below are intended to be guidelines, and not set standards, for how EWC's response to an actual or suspected Security Incident is conducted.

1. Report and Assess Situation
2. Investigate and Conduct Fact Finding
3. Strategize to Formulate Response
4. Contain and Limit Exposure.
5. Remediate and Resolve Vulnerabilities
6. Document Investigation and Communicate
7. Conduct an Annual Review and Simulation

[1] A Security Incident is the unauthorized access to and/or misappropriation of Confidential Information, or threats to the security and privacy of EWC's information technology systems, such as malware or ransomware. Confidential Information is information that is so deemed under applicable law. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Confidential Information covered under Wyoming Statutes, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.

26.8 Enforcement

Any employee who neglects to report a known security breach, or who fails to comply with this plan in any other respect, will be subject to disciplinary action.

Failure to Comply: Failure to comply with this administrative regulation may result in disciplinary actions up to and including dismissal from employment and termination of service at EWC. Legal actions, including, but not limited to the application of civil and criminal penalties, may also be taken for violations of applicable regulations and/or laws.

Policies Cross-Referenced

FERPA
HIPAA Privacy Notice
Written Information Security Plan (WISP)

25.9 Effective Date-

This plan is effective immediately (July 4, 2021).

This process defines to whom it applies and under what circumstances, and it will include the definition of an event or incident, , staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. This process shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Eastern Wyoming College Information Technology intentions of this process are to focus significant attention on data security and data security breaches and how Eastern Wyoming College ’s established culture of openness, trust and integrity should respond to such activity. Eastern Wyoming College Information Technology is committed to protecting Eastern Wyoming College 's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Potential Incident

25.2 Critical Steps

As soon as an event or incident containing Eastern Wyoming College Protected data or information is identified, the process of removing all access to that resource will initiate. The CIO will chair an incident response team to handle any event or incident.

The President will immediately be notified of the event or incident. The Data Incident Team (DIT) along with a designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators. As provided by Eastern Wyoming College cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan. The CIO and President will work with EWC College Relations and legal consultants to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

25.3 Confirm and communicate roles/responsibilities

- Sponsors - Sponsors are those members of the Eastern Wyoming College community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Eastern Wyoming College Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Chief Information Officer is that member of the Eastern Wyoming College community, designated by the President. The CIO provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the Eastern Wyoming College community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

- The Data Incident Team shall be chaired by CIO and shall include, but will not be limited to, the following departments or their representatives: IT Team, College Relations; Legal; VP of Financial and Administrative Services.

25.4 Enforcement

Any Eastern Wyoming College personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any student or third party partner company found in violation may have their network connection terminated.

27.0 Personal Technology Use

This policy will set forth the rules and regulations which will determine how the EWC IT Department personnel are to perform work on personally-owned employee or student technology products. The EWC IT Department does not service technology equipment for individuals who are not EWC employees or students.

27.1 Personally Owned Technology Equipment

The EWC IT Systems Department always strives to ensure that EWC employees, students, affiliates, and visitors receive the best possible technology assistance available for us to provide. However, this can leave something to be desired for non-EWC, personally-owned technology equipment owned by employees, students, affiliates, and visitors.

NOTE: All technology requests for configuration or connectivity to the EWC network from personal technology devices will be handled at no cost. This policy applies only to technology issues related to the personal needs of the user. All requests for personal technology assistance will begin with a preliminary diagnosis and troubleshooting process which is provided for FREE.

If additional work is authorized by the user then the accompanying Personal Technology Service Policy Consent Form must be read and signed before any work may begin. The EWC IT Department offers no implied warranty or guarantee on any work performed on personal technology equipment. All work is performed as-is as a service to our students and as a cost-saving alternative for their benefit. However, it is beneficial to note that all work is performed on the same level as comparable service on EWC owned equipment.

All personal technology work will be performed within the following restrictions:

- Personal technology work may be performed during regular business hours, only if such work does not directly interfere or delay the normal operations or job duties of the EWC IT Department employee.
- No on-site work. All equipment must be brought to the EWC IT Systems Department for a preliminary diagnosis and troubleshooting.
- No parts purchases. All parts to be installed must be purchased by the user
- No illegal software. Only legally licensed software may be installed.
- No work without proper authorization signature on consent form. All issues should be expected to take approximately 24-48 hours to complete; however, they may take longer depending upon the severity of the problem at hand.

Please expect to leave any equipment for a minimum of 48 hours for proper problem resolution. Eastern Wyoming College cannot be held responsible for any work done after hours by CSC ITS Department personnel on any personal technology equipment. All work provided is not warranted or guaranteed. By signing the Personal Technology Service Policy Consent Form, you agree to these terms and conditions and waive any damages which may occur due to any work on your personal

technology equipment. All work is done and once completed is left as is and no standing warranty or guarantee is implied.

28.0 Vendor Access

This policy will set forth parameters for vendors to abide by when access to our internal or external network, workstations, or servers is required. All vendors, regardless of status, frequency of visitation, work being performed, or size of entity shall abide by this policy at all times unless such work does not require access to the EWC network or computing resources.

All vendors shall notify their contact on campus of any work that will require access to any of the following EWC resources:

- Internal network
- External network
- On-campus workstation(s)
- On-campus server(s)
- Network infrastructure
- Any other computing device on campus Upon notification of the need for access, the EWC IT Department shall create login credentials and access requirements necessary to facilitate the access required for the vendor to complete their job function. Access shall always be restrictive meaning un-warranted or un-needed access will not be available until deemed necessary by the requirements of the project. All requests for access shall be evaluated on a case-by-case basis to ensure that proper access is granted and no un-warranted or un- needed access is given without cause.
- At all times, the vendor shall
- Fulfill their primary job responsibility only
- Not seek to undermine or circumnavigate the access which has been provide
- Not tamper or adjust security settings on existing network infrastructure or devices
- Ensure that access credentials are not shared with anyone other than those individual approved for access
- Work to ensure that EWC's information is kept safe and secure from loss or theft
- Never disclose any information he or she may come to know from working with or on any EWC technology resource with a separate third-part entity
- Notify the EWC IT Department IMMEDIATELY upon any inclination that loss or theft has occurred, access has been lost or tampered with, or there is a concern that any other type of access violation has occurred
- Never seek to use any of EWC's information for personal or other monetary gain
- Not use any access or technology resource in a manner that has been prohibited for employees, students, or visitors in any of the other, enclosed policies herein

29.0 Security Program

The Eastern Wyoming College Written Information Security Program ("WISP") is intended as a set of comprehensive guidelines and policies designed to safeguard all confidential and restricted data maintained at the College, and to comply with applicable laws and regulations on the protection of Personal Information and Nonpublic Financial Information, as those terms are defined below, found in records and in systems owned by the College.

29.1 Overview & Purpose

The WISP was implemented to comply with regulations issued by the State of Wyoming entitled "Wyoming Data Breach Law" (Wyo. Stat. § 40-12-502(d)(iii) & (iv) and by the Federal Trade Commission [16 CFR Part 314], and with our obligations under the financial customer information security provisions of the federal Gramm-Leach-Bliley Act ("GLB") [15 USC 6801(b) and 6805(b)(2)].

Under Wyoming law, "[a]n individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Wyoming resident. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system."

"Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state. Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure.

In accordance with these federal and state laws and regulations, Eastern Wyoming College is required to take measures to safeguard personally identifiable information, including financial information, and to provide notice about security breaches of protected information at the college to affected individuals and appropriate state agencies.

The purposes of the plan is to:

- Establish a comprehensive information security program for Eastern Wyoming College with policies designed to safeguard sensitive data that is maintained by the College, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

29.2 Employee Training

All administrative employees are required to complete the online or in-person security training on an annual basis. Any faculty, student or contract employee that has access to PII is also required to complete this yearly training. The training is also strongly recommended for all employees.

Additionally, users who are the victims of a phishing attack will be required to complete this course within 2 weeks after Computer Services identifies the issue, regardless of whether or not they have already completed the training. If a user fails to complete the training within 2 weeks, his or her remote access to College resources will be disabled. The IT Security Team maintains records of all such training.

29.3 Definitions

Data
For the purposes of this document, data refers to information stored, accessed or collected at the College about members of the College community.

Data Custodian
A data custodian is responsible for maintaining the technology infrastructure that supports access to the data, safe custody, transport and storage of the data and provide technical support for its use. A data custodian is also responsible for implementation of the business rules established by the data steward.

Data Steward
A data steward is responsible for the data content and development of associated business rules, including authorizing access to the data.

29.4 Personal Identifying Information

- Personal Information ("PII"), as defined by Wyoming law (Wyo. Stat. § 40-12-502(d)(iii) & (iv), is the first name and last name or first initial and last name of a person in combination with any one or more of the following:
- Social Security number;
- Driver's license number or state-issued identification card number;
- Account number, credit or debit card number, in combination with a linked security or access code or password of an individual's financial account;
- Tribal identification card;
- Federal or state government-issued identification card;
- Username or email address, in combination with a password or security question and answer that would permit access to an online account;
- Birth or marriage certificate;
- Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional;
- Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person, or information related to a person's application and claims history;
- Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes;

- Individual taxpayer identification number.
- In Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.
- For the purposes of this Program, PII also includes passport number, alien registration number or other government-issued identification number.

Nonpublic Financial Information
The GLB Act (FTC 16 CFR Part 313) requires the protection of "customer information", that applies to any record containing nonpublic financial information ("NFI") about a student or other third party who has a relationship with the College, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the College. For these purposes, NFI shall include any information: A student or other third party provides in order to obtain a financial product or service from the College;

About a student or other third party resulting from any transaction with the College involving a financial product or service; or

Otherwise obtained about a student or other third party in connection with providing a financial product or service to that person.

Examples of NFI include:

- Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;
- Account balance information, payment history, overdraft history, and credit or debit card purchase information;
- The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
- Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
- Any information you collect through an Internet "cookie" (an information collecting device from a web server); and
- Information from a consumer report.

29.5 Responsibilities

All data at the College is assigned a data steward according to the constituency it represents. Data stewards are responsible for approval of all requests for access to such data. The data steward for each constituency group are designated as follows:

Type of Data	**Data Steward***
Faculty	Vice President of Academics
Staff	Vice President for Finance and Administration

Student	Vice President of Student Services and Director of Financial Aid

*The data steward may appoint a designee to serve in their place.

Human Resources will inform EWC staff about an employee's change of status or termination as soon as is practicable but before an employee's departure date from the College. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to College data.

Department heads will alert EWC IT Staff at the conclusion of a contract for individuals that are not considered Eastern Wyoming College employees in order to terminate access to their Eastern Wyoming College accounts.

The EWC Security Team is in charge of maintaining, updating, and implementing this Program. The College's Chief Information Officer (CIO) has overall responsibility for this Program.

All members of the Community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the Community are required to access, store and maintain records containing sensitive data in compliance with this Program.

28.6 Identification and Assessment of Risks to College Information

Eastern Wyoming College recognizes that it has both internal and external risks to the privacy and integrity of College information. These risks include, but are not limited to:

- Unauthorized access of Confidential data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

Eastern Wyoming College recognizes that this may not be a complete list of the risks associated with the protection of Confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, IT Staff will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

Eastern Wyoming College believes the College's current safeguards are reasonable and, in light of current risk assessments made by IT Staff, are sufficient to provide security and confidentiality to

Confidential data maintained by the College. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

29.7 Safeguarding Confidential Data

To protect College data classified as Confidential, the following policies and procedures have been developed that relate to access, storage, transportation and destruction of records.
or an overview of storage guidelines. Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.

- To the extent possible, all electronic records containing Confidential data should only be stored on Vault (the College's on-campus secure network storage) and not on local machines or unsecured servers.
- PHI may be stored or accessed through the Google Apps core suite (including Mail, Drive, Groups, Sites, Chat) as these apps are certified HIPAA compliant, provided that access to the PHI is appropriately restricted. This does not apply to Google consumer apps such as Google+, Hangouts, etc.
- Wyoming PI and NFI must not be stored on any Google app.
- Confidential data must not be stored on cloud-based storage solutions that are unsupported by the College (including DropBox, Microsoft OneDrive, Apple iCloud, etc.).
- Members of the Community are strongly discouraged from storing Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport Confidential data electronically, the mobile device containing the data must be encrypted.
- Paper records containing Confidential data must be kept in locked files or other secured areas when not in use.
- Upon termination of employment or relationship with Eastern Wyoming College, electronic and physical access to documents, systems or other network resources containing Confidential data is immediately terminated. (See the Stewardship of Electronic Content Policy for more information.)

Digital Signature Acceptance

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in Eastern Wyoming College electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted. This policy applies to all Eastern Wyoming College employees, affiliates, contractors, and other agents conducting Eastern Wyoming College business with an Eastern Wyoming College-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-Eastern Wyoming College affiliated persons or organizations.

Use of Digital Signature

A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted on the site of the VP of Finance and Administration (CFO) on the organization's intranet:
https://ewc.wy.edu/about-eastern-wyoming-college/presidentscabinet/

The VP Administration's office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles are not considered valid.

Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

Signer Responsibilities

- Signers must obtain a signing key pair from the Eastern Wyoming College Business office. This key pair will be generated using Eastern Wyoming College's Public Key Infrastructure (PKI) and the public key will be signed by the Eastern Wyoming College's Certificate Authority (CA), Kwin Wilkes.
- Signers must sign documents and correspondence using software approved by Eastern Wyoming College the IT Team.
- Signers must protect their private key and keep it secret.
- If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact Eastern Wyoming College Business Office immediately to have the signer's digital key pair revoked.

Recipient Responsibilities

- Recipients must read documents and correspondence using software approved by Eastern Wyoming College IT department.

- Recipients must verify that the signer's public key was signed by the Eastern Wyoming College's Certificate Authority (CA), Kwin Wilkes, by viewing the details about the signed key using the software they are using to read the document or correspondence.
- If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.
- If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to Eastern Wyoming College Identity Management Group.

30.0 Disaster Recovery Plan

Since disasters happen so rarely, leadership often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event event of a disaster gives Eastern Wyoming College a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Crisis Management Plan. This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by Eastern Wyoming College that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes major outage. The scope of this policy is directed to the IT Team who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

30.1 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.
- After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed and updated on an annual basis.

30.2 Policy Compliance

The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the CIO. The IT Team will work with the Registrar, Financial Aid Director, Human Resources, the Business Office and other groups using IT Services and Programs. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

FORMS

EWC IT Policies and Procedures Compliance

The forms following this page are required for every employee upon successfully reading and agreeing to the policies and procedures set forth within this document. All other forms mentioned earlier within this document may be used as needed during daily activities and as required for performing job duties. A copy of these two forms shall be retained by the EWC Human Resources Department at all times to ensure all employees have signed and agreed to the policies and procedures included herein.

An employee's signature on a previous version of this policies and procedures manual does not exclude any user from being required to abide by any new or updated policies or procedures. Any signature, by any employee, upon first being hired is transferable to subsequent iterations of this document from henceforth so that all current employees shall not be required to re-sign these documents. Upon successful approval of changes, a copy shall be made available for all employees so that any current employee may view new policies and procedures and/or any changes to current policies and procedures.

If any employee disagrees with any policy, procedure, or change included herein, he/she may voice this complaint to Administration. However, it is important to note that since agreement with this document is stringent upon employment, any employee who does not agree to this document and sign these required forms, will effectively resign from his/her position effective immediately and all technology access will be revoked. Employees may obtain a current copy of this document from the Human Resources or EWC IT Department at any time.

Incident Report Form

User Causing/Experiencing Incident:_____

Name: _____ Incident Date: _____ Email Address: _____ Cell Phone: _____

Incident Details:

_____

_____

_____

_____

_____

_____

_____

_____

_____ Special Requirement/Notes: _____

_____

_____

EWC IT Department Personnel Use Only:

Receiving Employee: _____ Date Received: _____

Details:

_____ _____

_____Additional Steps Needed: _____

_____

Personal Technology Service Consent Form

By signing this form, I understand that the EWC IT Department is not liable for any loss of information that may occur during the service of my technology equipment. I also understand that I waive my right to file any complaints, either formally or informally should such issues arise.

The EWC IT Department will do everything we can to ensure your data is retained, however, issues may occur that cause data loss beyond the control of the ITS Department such as equipment failure, virus activity, data corruption, or pre-existing data loss prior to arrival on-site.

I understand that this service is provided free of charge and that I will be liable for any and all additional hardware costs, if needed. I also understand that no warranty or guarantee is provided once services are rendered and that my only recourse is to return the equipment for additional service, if needed.

By signing below, I understand the above statements and agree to the terms and conditions as described within this form and the associated Personal Technology Service Policy.

Please Print:

Name: _____WCID:_____

Email Address: _____ Home Phone: _____ Cell Phone: _____ Login credentials for equipment:

_____

_____Detailed Description of Problem: _____

_____

_____

Student Signature: _____

EWC IT Department Personnel Use Only:

Receiving Employee: _____ Record Added to Spreadsheet? Yes – No

Date Received by Employee: _____ Problem Resolved? Yes – No

Date Returned to Student: _____

Security Recommendations Checklist

Hardening of Systems

- Advanced Endpoint Monitoring Solution
- Logging and Security Information and Event Management
- Disable SMBv1
- Disable Windows PowerShell
- Restrict Remote Desktop Protocol (RDP)
- Disable Macros
- Regularly Update Software and Operating systems
- Password Management
- Conduct Periodic Vulnerability Scans

Data Protection

- Backups
- Darkweb Search and Monitoring
- Volume Shadow Copies

Perimeter Protection

- Virtual Private Network (VPN) Solution with 2-Factor Authentication
- Firewall and Intrusion Detection systems (IDS)
- Network Isolation/Segmentation
- Layered or Defense-in-depth Security
- Office 365
    - Check 0365 with Microsoft Secure Store at https://docs.microsoft.com/en-us/office365/securitycompliance/microsoft-secure-score

31.0 Emergency Operating Procedures

In the event of an emergency, normal operating procedures should be restored as quickly as possible. Due to the small size of our IT department, it is beneficial that all employees learn laterally to allow for greater ability to maintain operations should any individual employee be unavailable.

31.1 Steps to Take

The steps below will indicate how operations should continue in the event of an emergency directly affecting the EWC IT Department.

1. Assess situation and determine if any personnel impact to the EWC IT Department exists. If so, go to step 2. If not, go to step 3.
2. Given any personnel impact below, the following options are available to ensure IT operations can continue in an emergency. If the IT Department suffers the loss of any of the following employees, the available options are:

a. Chief Information Officer of IT Systems

i. Responsibilities will defer to the President or designee until a suitable appointment can be made.

b. Network Systems Administrator

i. Responsibilities will defer to the CIO.

ii. Interim assistance can be performed by Instructional Technologist or another suitable vendor to facilitate network management.

iii. Network management is more specialized than workstation management so vendor assistance will most likely be a necessity.

c. Desktop Administrator

i. Responsibilities will be shared between remaining personnel.

ii. Emergency/Interim hiring may be required.

d. Instructional Technologist

i. Responsibilities will be shared between remaining personnel.

ii. Emergency/Interim hiring may be required.

g. Programmer

i. Responsibilities will defer to the CIO.

ii. Interim assistance can be performed by WCCC IT or another Wyoming ETS may be willing to assist.

iii. Emergency/Interim hiring may be required.

h. Departmental catastrophe (3+ users unavailable to perform duties)

i. Responsibilities will defer to the President or designee until emergency hiring can be finalized.

ii. If necessary, assistance may be obtained from other institutions and/or vendors:

1. EWC Operations: ETS or Wyoming Community College Commission Institutions
2. Networking: ETS and Action Communications

i. NOTE: Emergency approval for costs associated with assistance will need to be obtained under any scenario.

3. Determine if any equipment loss has occurred. If so, proceed to step 4. If not, proceed to step 5.
4. Determine what resources are affected and bring them back up as soon as possible:

a. Network and connectivity equipment

b. Mission critical services (group drives, ID card system, etc.)
c. Non-mission critical services (security cameras, wireless infrastructure, dorm connectivity, etc.)

5. Once all connectivity and resources have been restored, normal operations can now resume.

NOTE: Please see the EWC IT Department's detailed Disaster Recovery Plan for detailed information regarding disaster scenarios and specific planning information.

32.0 Gramm Leach Bliley Act (GLBA) Information Security Plan

This Information Security Plan ("Plan") describes Eastern Wyoming College safeguards to protect information and data in compliance ("Protected Information") with the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. Section 6801. These safeguards are provided to:

- Protect the security and confidentiality of Protected Information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of Protected Information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten Protected Information maintained by Eastern Wyoming College;
- Designate employees responsible for coordinating the program;
- Design and implement a safeguards program;
- Manage the selection of appropriate service providers;
- Adjust the plan to reflect changes in technology, the sensitivity of protected Information, and internal or external threats to information security; and
- Reference related policies, standards, and guidelines.

32.1 Identification and Assessment of Risks to Customer Information

Eastern Wyoming College that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of Protected Information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Eastern Wyoming College recognizes that this may not be a complete list of the risks associated with the security of Protected Information. Since technology growth is not static, new risks are created regularly.

Accordingly, the District Information Technology Services (ITS), the Office of Student Affairs, and other designated stakeholders will actively participate with and seek advice from district office, colleges, and community representatives for identification of new risks. Risk assessments include advisory review for mitigation, acceptance of risk, gap analysis, or other appropriate review based on outcomes of the risk assessment on an annual basis. Eastern Wyoming College believe current safeguards used by the District's Security and Technology Office are reasonable and, in light of current risk assessments, are sufficient to provide security and confidentiality to Protected Information maintained by the colleges and district.

32.2 Information Security Plan Coordinators

An advisory committee is responsible for the maintenance of information security and privacy. The advisory committee will include representatives from the departments primarily responsible for safeguarding Protected Information. Each department responsible for safeguarding Protected Information will provide an annual update report indicating the status of its safeguarding procedures. The advisory committee is responsible for assessing the risks associated with unauthorized transfers of Protected Information and implementing procedures to minimize those risks that are appropriate based upon severity, complexity, and the nature and scope of its activities.

32.3 Design and Implementation

32.4 Employee Management and Training

In accordance with Eastern Wyoming College policies, standards, and guidelines, reference checking and background reviews are conducted for all new hires. During employee orientation, each new employee in departments that handle Protected Information are required to participate in several training sessions on the importance of confidentiality of Protected Information. Each new employee will also be trained in the proper use of computer information and passwords. Further, each department responsible for maintaining Protected Information will provide ongoing updates to respective staff. These training efforts should help minimize risk and safeguard covered data and information security.

Physical Security

Eastern Wyoming College has addressed the physical security of Protected Information by limiting access to only those employees who have a business reason to know such information and requiring signed acknowledgement of the requirement to keep Protected Information private. Existing policies establish a procedure for the prompt reporting of the loss or theft of Protected Information. Offices and storage facilities that maintain Protected Information limit customer access and are appropriately secured. Paper documents that contain Protected Information are shredded at time of disposal.

Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. Eastern Wyoming College has policies, standards, and guidelines governing the use of electronic resources and firewall and wireless policies. Eastern Wyoming College will take reasonable and appropriate steps consistent with current technological developments to make sure that all Protected Information is secure and to safeguard the integrity of records in storage and transmission. Eastern Wyoming College will follow current policies for all electronic Protected Information by encrypting it for transit.

32.5 Management of System Failures

Eastern Wyoming College will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; imaging documents and shredding paper copies; backing up data regularly and storing back-up information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

32.6 Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that Eastern Wyoming College determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access Protected Information, the evaluation process shall include the ability of the service provider to safeguard Protected Information. Contracts with service providers may include the following provisions:

- A requirement that the Protected Information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- A requirement that the service provider have documented appropriate safeguards and controls (e.g. SOC2) to protect the Protected Information it receives, and that it must promptly report any security incidents that may affect Eastern Wyoming College protected information;
- Where appropriate, a requirement that the service provider maintain certain types of insurance to cover potential liability in the event of a security incident;
- Where appropriate, a requirement that the service provider submit to audits of its information security and privacy policies, procedures and controls.

32.7 Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment, especially when due to the constantly changing technology and evolving risks. The Coordinators, in consultation with the Office of General Counsel, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

Policies, Standards and Guidelines (GLBA Audit Requirements)

Eastern Wyoming College Written Information Security Plan

Information Security and Privacy Incident Response Plan

Policies

- Eastern Wyoming College District Office Information Security
- Student Data and Data Handling
- Privacy Rights of Students
- Release of Student Information
- Fraud Prevention and Suspected Identity Theft
- Data Governance
- Use of Computer Software

Guidelines

- Student Educational Records – FERPA
- Eastern Wyoming College Statement on Privacy
- Networking and Security
- Phishing
- Telecommuting and Best Practice
- Computer Software
- Security Terms

33.0 Incidence Response Plan for Compromised Networks

Steps to follow when dealing with a cyberattack:

1. **Contain**

The primary step is to immediately contain and isolate the critical systems. Temporarily suspend all the systems after discovering the attack. This will help stop the spread of the attack to all college-critical networks. Look for any strains of ransomware or malware on the affected systems and isolate them from the main network immediately. Also, changing the passwords of all critical accounts will help mitigate the risks. A well-organized approach of isolation and containment will certainly help regain control of the affected systems and eliminate the risks. ***At this point the CIO and the President should be involved.***

2. **Report**

Reporting the cyberattack to the staff, faculty and students, to law enforcement, Wyoming Community College Commission, immediately after it happens will create a sense of trust and transparency in the organization. Law enforcement includes:

- Local law enforcement (Torrington PD 532-7001) (Douglas PD 358-3311)
- Homeland Security (307-777-4663)
- FBI (307-632-6224 Cheyenne Office)
- Cyber-Insurance Company ( )
- Wyoming Community College Commission (307-777-7763)
- Wyoming Department of Enterprise Technology Services (307-777-5840)
- Wyoming Department of Enterprise Technology Services (307-777-5840)
- Federal Student Aid (support@cpssaid.ed.gov) (FSASchoolCyberSafety@ed.gov)

Most enterprises are often judged based on their incident handling capabilities during a ransomware or data breach attack. Organizations could encounter severe negative consequences for any delays or coverups in disclosing the incident. Besides, companies are liable under various data privacy regulations to report any security data breach incident and can attract a huge penalty from regulatory agencies if failed to report.

3. **Investigate and Recover**

It is necessary to have an effective disaster recovery plan for organizations to restart the affected business operations smoothly. Report and engage with law enforcement authorities to investigate the incident to find out the cybercriminals responsible for the attack. Organizations can even hire a digital forensic team to inspect the security incident to understand the actual cause of the attack, what data, and how many have been affected. We have used Arete Incident Response for forensics work (Arete911@AreteR.com) and legal issues were provided by FisherBroyles, LLP (www.fisherbroyles.com)

4. **Remediate**

Organizations must learn from their mistakes after sustaining a cyberattack. Analyze the attack to know if there are any unpatched vulnerabilities or security loopholes in the organization's cybersecurity

posture. Come up with a set of efficient remedial measures to boost security and deal with the potential cyberattacks in the future.

5. **Wrap Up**

No individual or company is 100% immune to cyberattacks. Organizations must bolster their security standards to defend against evolving cyberthreats. Cybersecurity precautions like encouraging employees to use strong passwords, training them to identify phishing, and other attacks ultimately improve organizational security.

STATEMENTS AND AMENDMENTS

Eastern Wyoming College Privacy Statement (on Canvas Webpage)

EWC expects that you will respect the rights of faculty and other students as you participate in the educational process. Participating in an Online/Hybrid courses means that you may have access to personal information and academic work produced by other students and faculty members, such as discussion board postings, drafts of papers and other work produced in the course. Academic norms and EWC policy require that you must not reveal any information about classmates, course work content, or its authors to anyone outside the course.

Students should be aware that their use of CANVAS materials and communication tools in a particular course may be observed and recorded by the instructor of that course. These observations and records may include a student's access to online library materials linked through the Canvas course website. Use of these observations and records must conform to the use and release of confidential student records as described in Eastern Wyoming College's Access to Student Information. Students may link to library resources directly, without linking through Canvas, using the Library website.

EWC Policies and Procedures Agreement Form

I certify, by signing below, that I have read and understand the policies and procedures contained in this document.

Also, by signing below, I agree to abide by the aforementioned policies and procedures having known and understood the consequences outlined within this document.

Please print.

Name: _____Date: _____ Title: _____ Signature: _____

SOLOMON AMENDMENT

The 1996 Solomon Amendment is the popular name of 10 U.S.C. §983, a United States federal law that allows the Secretary of Defense to deny federal grants (including research grants) to institutions of higher education if they prohibit or prevent ROTC or military recruitment on campus. In other words, it is a federal law that allows military recruiters to access some address, biographical and academic program information on students age 17 and older who have not filed any FERPA restrictions.
The Department of Education has determined the Solomon Amendment supersedes most elements of FERPA. An institution is therefore obligated to release data included in the list of "student recruiting information," which may or may not match our FERPA directory information list.

Procedure for releasing information to military recruiter:

1. Under the Solomon amendment, information will be released for military recruitment purposes only. The military recruiters may request student recruitment information once each term for each of the 12 eligible units within the five branches of the service:
    - Army: Army, Army Reserve, Army National Guard
    - Navy: Navy, Navy Reserve • Marine Corps: Marine Corps, Marine Corps Reserve
    - Air Force: Air Force, Air Force Reserve, Air Force National Guard
    - Coast Guard: Coast Guard, Coast Guard Reserve
2. The request should be submitted via our the Office of the Registrar at https://ewc.wy.edu/future-students/register-for-class/
3. The request should specify the details of what you are seeking, including whether the information is needed for the future, current, or previous semester.

What information are military recruiters entitled to under the Solomon Amendment?

- Name
- Address
- Telephone
- Age and date of birth
- Place of birth (EWC does not collect)
- Level of education
- Academic major
- Degrees received
- Educational institution in which the student was most recently enrolled.

Schools are not required to collect those elements.

Version Control

Version Date	Changes	Changed made by
11/8/2021	Formatting Sections	Security Subcontractor
11/7/2021	Integrated Incident Response Plan and Management Sections	Security Subcontractor