BOARD POLICY 7.0 INFORMATION TECHNOLOGY

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.

Scope and Change Management

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:

1. Computers that include desktop computers, mobile devices, servers, etc.
2. 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.

3. Audio/Video Equipment that include video codecs, HDTVs, document cameras, projectors, security cameras, miscellaneous cabling, digital cameras and camcorders, printers, copiers, fax machines, etc.
4. Software that includes operating systems, application software, etc.
5. Resources that include group drive file storage, website file storage, email accounts, social networking accounts, etc.

Applicable Standards and Regulations

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

1. Federal Education Rights and Privacy Act (FERPA), §20 U.S.C. § 1232g; 34 CFR Part 99
2. National Institute of Standards and Technology (NIST), Special Publication 800-171, Rev. 2
3. National Cyber Security Review NCSR as a measurement of cyber maturity
4. Gramm-Leach-Bliley Act (GLBA)

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.

Data and Information Classification - 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:

1. Name
2. SSN
3. Address(es)
4. Phone Number(s)
5. SSN
6. Birth date
7. Birthplace
8. Mother's maiden name
9. Family names
10. Other family data such as addresses, contact information, etc.
11. Financial information such as bank account information, account balances, etc.
12. 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
13. 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.

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.

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:

1. No loss of mission capability, but inconveniences may be experienced by some individuals
2. No damage to College assets
3. 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, Gramm-Leach-Bliley Act (GLBA), Wyo. Stat. § 40-12-502(d)(iii) & (iv), 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.

BOARD POLICY 7.1 ACCESS CONTROL
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.2 TRAINING AND AWARENESS
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.3 AUDIT AND ACCOUNTABILITY
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.4 CONFIGURATION MANAGEMENT
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.5 IDENTIFICATION AND AUTHENTICATION
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.6 INCIDENT RESPONSE
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.7 MAINTENANCE
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.8 MEDIA PROTECTION
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.9 PERSONNEL SECURITY
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.10 PHYSICAL ACCESS
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.11 RISK ASSESSMENT
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.12 SECURITY ASSESSMENT
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.13 SYSTEM AND INFORMATION INTEGRITY
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.14 **ACCEPTABLE USE AND GUIDANCE**

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:

1. Computers that include desktop computers, mobile devices, servers, etc.
2. 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.
3. Audio/Video Equipment that include video codecs, HDTVs, document cameras, projectors, security cameras, miscellaneous cabling, digital cameras and camcorders, printers, copiers, fax machines, etc.
4. Software that includes operating systems, application software, etc.
5. 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 EWC 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:

1. All passwords used to access EWC systems must be kept secure and protected from unauthorized use.

2. No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.

3. Do not transfer personally identifiable information on portable equipment and storage devices.

4. 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.

5. 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.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders.

7. Personally identifiable information can be sent via electronic means only through encrypted methods and should be transferred within the internal network or through secure VPN connections.

8. 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 EWC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing EWC-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.

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.

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

1. 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.

2. NOTE: Please do not use either of these examples as passwords!

3. 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

4. List of Don’ts

5. Don't reveal a password over the phone to ANYONE.

6. Don't reveal a password in an email message.

7. Don't reveal a password to a supervisor.

8. Don't talk about a password in front of others.

9. Don't hint at the format of a password (e.g., "my family name").

10. Don't reveal a password on questionnaires or security forms.
11. Don't share a password with family members.

12. Don't reveal a password to co-workers.

13. Don’t reveal a password to vendors.

14. In short, don’t reveal a password to ANYONE.

15. Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, Internet Explorer, Firefox, and Thunderbird).

16. Do not write passwords down and store them anywhere in your office.

17. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without proper encryption.

18. Change passwords at least once every three months.

19. 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.

20. 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.

21. Password cracking or guessing may be performed on a periodic or random basis by the EWC IT Department or its delegates.

22. If a password is guessed or cracked during one of these scans, the user will be required to change it.

23. 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.

24. Application developers must ensure that their programs contain the following security precautions:

25. Applications must support authentication of individual users, not groups.

26. Applications must not store passwords in clear text or in any easily reversible form.

27. Applications must not transmit passwords in clear text over the network.

28. 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.

29. Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

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.

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.

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.

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.

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.

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.

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:

1. If a student, through the Vice President for Student Affairs, or his/her designee;

2. 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.

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.

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.

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.

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.

Transporting Confidential Data

1. 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.

2. 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.

Destruction of Confidential Data

1. 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.

2. Paper and electronic records containing confidential data must be destroyed in a manner that prevents recovery of the data.

Traveling Abroad with Students' Personal Information

1. 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.

2. 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 server. Any spreadsheets containing student passport information should be routinely deleted by the spreadsheet owner when no longer needed.

3. 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.

4. 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 VPSS immediately if the copies of a passport are lost.

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 EWC 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.

BOARD POLICY 7.15 ACCESSIBILITY

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.

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:

1. Screen reading software
2. Screen magnification software
3. 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.

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.

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.

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.

BOARD POLICY 7.16 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:

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

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

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

1. is always understood to represent an official statement from the institution

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

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

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

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

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

BOARD POLICY 7.17 EMERGENCY NOTIFICAITON

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

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

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

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

1. Director of College Relations
2. Director of Housing
3. Vice President of the Douglas Campus
4. Vice President for Student Services
5. Vice President of Academic Services
6. Other designee deemed necessary by the President

BOARD POLICY 7.18 CLEAN DESK
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.19 ENFORCEMENT

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

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

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

BOARD POLICY 7.20 EQUIPMENT CONFIGURATION AND EQUIPMENT ORDERING
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.21 **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:

1. Standard – Access granted to internet resources and institutional resources located online.
2. 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:

1. Wireless VLANs (i.e. campus, employees and Lancers)
2. Singular or multiple file access
3. System access such as Canvas, Colleague, 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.

BOARD POLICY 7.22 **INFORMATION SHARING**
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.23 **PHYSICAL SECURITY GUIDELINES**
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.24 **INCIDENT RESPONSE MANGEMENT**
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.25 **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.

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:

1. 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.
2. No on-site work. All equipment must be brought to the EWC IT Systems Department for a preliminary diagnosis and troubleshooting.
3. No parts purchases. All parts to be installed must be purchased by the user
4. No illegal software. Only legally licensed software may be installed.
5. 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.

BOARD POLICY 7.26 VENDOR ACCESS
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.27 SECURITY PROGRAM
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.28 DISASTER RECOVERY PLAN
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.29 EMERGENCY OPERATING PROCEDURES
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.30 GRAMM LEACH BLILEY ACT (GLBA) INFORMATION SECURITY PLAN
(Under Review - Contact Sally Watson for a copy)

BOARD POLICY 7.31 **INCIDENCE RESPONSE PLAN FOR COMPROMISED NETWORKS**
(Under Review - Contact Sally Watson for a copy)