Introduction
It is the policy of Eastern Washington University (EWU) to ensure the security, availability, privacy, and integrity of its information technology systems, networks, and data and to ensure full compliance with all applicable federal and state statutes and regulations. All providers and users of EWU information technology resources and data are required to comply with all established policies, guidelines, standards, and procedures, including applicable federal and state statutes and regulations.

Purpose
The purpose of this policy is to help ensure the security and availability of information technology systems and networks and the confidentiality and integrity of institutional data. Institutional data is defined as all data created, collected, maintained, recorded or managed by EWU, its staff, and agents working on its behalf. It includes data used for planning, managing, operating, controlling, or auditing university functions.

This policy provides direction for compliance with State and Federal statutes and regulations (Appendix B), specifies appropriate practices, and defines custodial responsibilities for records associated with University operations. This policy should be used as the foundation document for all standards, procedures, and guidelines that are developed and implemented by EWU related to information systems and data security.

Scope and Applicability
This policy applies to institutional information technology systems, networks, operational and institutional data, and all users (staff, faculty, students, agents working on the university’s behalf, and others). Successful compliance and protection of information technology systems and networks require that all users learn, understand, and abide by this policy. It is the responsibility of all users to evaluate their specific compliance requirements on a regular basis as directed by this policy.
This policy applies regardless of the environment, media, or device where the data resides or is used, and regardless of how data may be transmitted. It also applies regardless of the form the data may take or presentation format.

This policy applies to all extracts of institutional data, feeds of these data from enterprise systems, and data maintained within so-called shadow or secondary database systems whether derived from enterprise systems or collected or assembled directly by university units. Data in these systems must be protected in the same manner as prescribed by the Data Custodian.

Roles and Responsibilities

**Data Custodian**

Data Custodians have been officially designated by the President as the position accountable for the oversight and general operation of institutional data systems that serve a broad section of the university community. It is the responsibility of the Data Custodians to provide direct authority and control over the management and use of institutional data regardless of which system in which the data resides.

These positions play a critical role in protecting Eastern Washington University’s systems and data, following all appropriate and related security guidelines to ensure the protection of data. Data Custodians’ responsibilities include (but are not limited to):

- Ensure compliance with all Eastern Washington University’s policies, as well as state and federal statutory and regulatory requirements.
- Provide institutional requirements for access to and protection of institutional data in all test, development, and production institutional data systems.
- Assign, monitor, and review privileges for access to institutional data.
- Ensure appropriate security measures for transmission of institutional data.
- Review and recommend changes for procedures surrounding the assignment of access to institutional data.
- Coordinate staff and faculty training and development for the proper use of institutional data.
- Audit and maintain institutional data.
- Delegating object custodianship (authority and responsibility for specific data fields) as necessary to effectively manage use of data systems.
- Ensure the accuracy of data reporting; collaborates, when necessary, with other departments in provision of data reports.

Eastern Washington University’s officially designated Data Custodians are as follows:

- **Student Data** – Registrar
- **Financial Aid Data** – Director, Financial Aid
- **Finance Data** – Chief Financial Officer
- **Staff and Faculty Employment Data** – Director, Human Resources, Rights, & Risk
- **Faculty Personnel and Workload Data** – Director, Academic Personnel
**Object Custodian**

An Object Custodian is a university official with delegated operational authority and responsibility for defining, managing, and maintaining the integrity, security, and accuracy of one or more specific data fields (objects) found within EWU’s data systems.

**Data User**

Any individual (staff, faculty, students, and agents working on the university’s behalf) using institutional information technology systems, networks, or data in the conduct of university business.

**Access To and Use Of Institutional Data**

Institutional data created, collected, maintained, and recorded are required to conduct university business. EWU regards the security and confidentiality of its business data and information to be of significant importance. Each user (staff, faculty, students, and agents working on the university’s behalf) granted access to institutional data and information, whether electronic, paper, or other format, holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Access to this data:

- Is restricted to individuals whose job duties require it
- Is granted only to fulfill the specific functions required to perform a specific job
- Must be approved by both the user’s department head and the Data Custodian or designee before requested access is provided

Data and Object Custodians are expected to use the principle of least privilege when authorizing access to data for which they are responsible. In some cases, Data and Object Custodians may require users to attend formal training before access is granted.

All institutional data are the property of Eastern Washington University and may only be used by individuals for university business which they are authorized to conduct. Use of this data as it relates to the role or responsibilities of one’s position are considered to be routine, and therefore considered an acceptable use.

**Sharing and Release of Institutional Data**

- Within the institution, employees may share or disseminate institutional data to other employees who have a legitimate need to access or use the data
- Employees may release appropriate data, if such activity is defined to be a part of their role and at the direction of their supervisor, to honor requests from appropriate state or federal agencies, legislative bodies, and other applicable agencies
- Due to the complex nature of laws governing the use of certain types of data, as well as the sometimes complex nature of the data themselves, it is in the best interest of the institution and its employees that institutional data be formally released outside of the institution only by authorized individuals such as those who are designated as Data Custodians and the Director of the Office of Institutional Research, Demography, and Assessment.
It is the data user’s responsibility to access and use institutional data in accordance with Eastern Washington University’s policy and procedures and State and Federal Laws. If in doubt, contact your supervisor or the appropriate Data Custodian. Specifically, for each type of data:

- **Restricted/Internal/Confidential Data**: Requests for these data should be referred to the office of the appropriate Data Custodian and the Director of the Office of Institutional Research, Demography, and Assessment and are to be released only by authorized personnel in accordance with University policy. The use of much of the institution’s data is covered by State and Federal statutes and regulations (Appendix B) and may be defined as personal, private, or confidential.

Employee personnel information, payroll data, etc. are considered high risk data because it could cause damage to this University and the employees if disclosed, misused, or modified.

Student data likewise are considered high risk and covered by the Family Educational rights and Privacy Act (FERPA) as amended. Faculty and others who have access to student educational records may not release any information contained in a student’s educational record to a third party without written consent from the student. There are some exceptions to this rule, but requests for student information from outside the institution are to be referred to Records and Registration Office.

- **Public Data**: To present and interpret institutional data correctly, disclosure of even public data should be done by an appropriate University Official. Public data may be disseminated freely by such an official.

Specific non-university business use of institutional data may be authorized under other official university policy or with written permission of the Data Custodian responsible for housing and maintaining the data. The use of institutional data for personal gain, curiosity, academic research, or for another’s personal gain, or curiosity is prohibited.

**Data User Responsibilities**

As a condition of access, institutional data users agree to adhere to the following terms and conditions, as applicable, when they access or are in possession of institutional data of any kind. These requirements reflect best practices used in the industry today and may be amended in the future as needs change. Institutional data users are required to acknowledge they will adhere to these requirements to the best of their ability for the system(s) to which they require access. An individual given access to EWU institutional data in any format acknowledges an understanding of and agrees to adhere to the following:

- Users are expected to maintain the security of the systems they use. Users are responsible for all activity that occurs under their information system accounts. Users will not share their assigned security access (username and password) to any institutional information technology systems with anyone (this includes supervisors, co-
workers, or colleagues). Further, users may only share institutional data, in any format, with other users who are authorized to use that data.

- Student access to institutional data is generally discouraged. Offices that need student employee access must request individual access for each student and must ensure that the student has received the appropriate training and oversight. Shared usernames for use by multiple student employees in an office will not be granted in any system or application.
- Departments must inform the Office of Information Technology immediately when an individual student or employee no longer needs access.
- The username and password combination is considered equivalent to a signature and individual account owners are responsible for activities that occur under that account.
- Proper password security to all systems is to be maintained by all users and should never be revealed to anyone.
- Workstations that connect to EWU information technology systems are to be properly maintained and managed to prevent problems that could affect the any part of the EWU computing environment.
- The user is expected to maintain physical workstation security by not leaving a workstation unattended while logged into EWU information technology systems. Storing institutional and other sensitive data on a local or portable storage medium significantly increases the potential for the data to be fraudulently accessed and misused. Users are expected to take precautions to protect the security and integrity of data to which they have access regardless of format. Institutional data should be handle by users according to the following best practices:
  - Data should be stored on hardened, protected, and managed network file systems using security settings which prevent anyone other than approved users from accessing the data.
  - Data should not be stored on the local hard drive of an office workstation of any type nor be moved to any external media unless approved by the appropriate authority and the file and file system is encrypted.
  - Users will be held professionally accountable in the event of loss or disclosure of EWU data due to loss of workstation or external media.
- Users are expected to comply with institutional requirements, shared in this document, for sharing and release of institutional data. All requests to provide data should be provided to the appropriate office.
- When finished working with institutional data not subject to records retention guidelines, regardless of format, electronic files should be appropriately deleted and purged, and printed documents should be shredded or disposed of in a confidential shredding bin.

Sanctions and Violations

The privacy and confidentiality of all accessible data shall be maintained at all times. Individuals who violate this policy may be denied access to institutional information technology systems,
networks, and data and may be subject to disciplinary, civil, and/or criminal actions. The university may temporarily suspend, block, or restrict access to institutional information technology systems, networks, and/or data at any time when it reasonably appears necessary to do so in order to protect the integrity, security, or availability of these resources or to protect the university from liability. Eastern Washington University will take any and all actions it deems necessary to resolve violations of this policy.

Suspected security violations are to be reported to the appropriate Data Custodian and the Chief Information Officer immediately when an event involving breach, loss, or unauthorized exposure of institutional data is thought to have occurred. Users are expected to work with the appropriate university personnel in investigating and addressing suspected violation of this policy.
Appendix A
Definitions

The following terms are found within this policy and its associated procedures and guidelines.

**Availability** – The assurance that a computer system is accessible by authorized users whenever needed

**Confidentiality** – An attribute of information; confidential information is sensitive or private information, or information whose unauthorized disclosure could be harmful or prejudicial

**Data Custodian** – Individuals officially designated by the President whose position is accountable for the oversight and general operation of institutional data systems that serve a broad section of the university community

**Encrypt** – The process of turning readable text into unreadable cipher text

**Integrity** – Data or a system remains intact, unaltered, reliable, and available

**Principle of Least Privilege** – Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more

**Privacy** – An individual’s right to be left alone; to be secluded and not intruded on; to be protected against the misuse or abuse of something legally owned by the individual or normally considered by society to be his or her property

**Security** – An attribute of information systems that includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals

**System** – A network, computer, software package, or other entity for which there can be security concerns

**User** – An individual who has been granted privileges and access to institutional computing, network, and data systems, services, applications, resources, and information
Appendix B  
State and Federal Statutes and Regulations

Below are State and Federal Statutes and Regulations that directly or indirectly affect this policy and operational guidelines referenced within this document. These statutes and regulations are listed here for reference and to demonstrate the volume and complexity of the rules that relate to the use of computers, networks, applications, and data at EWU. This list is an attempt to provide a comprehensive review of appropriate statutes and regulations that are applicable. There are continual changes and additions, so this list may not be an exhaustive review.

**United States Code (USC)**

Applicable United States Codes include the following:
- 5 USC Sec. 552 - Freedom of Information Act (FOIA)
- 5 USC Sec. 552a - Privacy Act
- 15 USC Sec. 6501 - Children’s Online Privacy Protection Act of 1998
- 15 USC Sec. 6801 - Protection of nonpublic personal information
- 18 USC Sec. 1029 - Fraud and Related Activity in Connection with Access Devices
- 18 USC Sec. 1030 - Fraud and Related Activity in Connection with Computers
- 18 USC Sec. 1362 - Communications Lines, Stations, or Systems
- 18 USC Sec. 2701 - Electronic Communications Privacy Act
- 18 USC Sec. 2703 - Requirements for Government Access
- 20 USC Sec. 1232g - Family Educational Rights and Privacy Act (FERPA)
- 29 USC Sec. 102 - Employee Retirement Income Security Act
- 39 USC Sec. 3623 - Mail Privacy Statute
- 42 USC Sec. 1029 - Equal Employment Opportunity Act
- 42 USC Sec. 1001 - Communications Assistance for Law Enforcement
- Pub. L. 107-056 - USA Patriot Act

**Revised Code of Washington (RCW)**

Applicable Revised Codes of Washington include the following:
- RCW 5.60.060 - Who Are Disqualified – Privileged Communications
- Chapter 9.73 RCW - Violating Right of Privacy (Privacy Act)
- RCW 9A.48.100 - Malicious Mischief – “Physical Damage” Defined
- RCW 9A.52.110, 9A.52.120, and 9A.52.130 - Computer Trespass
- RCW 19.190.020 - Unpermitted or Misleading Electronic Mail – Prohibition
- Chapter 40.14 RCW - Preservation and Destruction of Public Records
- RCW 42.17 - Washington State Public Records Act
RCW 42.17.020 - Definitions (public records “writing” inclusive of graphics or computer records)
RCW 42.17.260 - Documents and indexes to Be Made Public
RCW 42.17.310 - Certain Personal and Other Records Exempt
RCW 42.52 - Ethics in Public Service
RCW 42.52.050 - Confidential Information – Improperly Concealed Records
RCW 43.105.041 - Powers and Duties of Information Services Board (ISB)
RCW 43.105.200 - Application to Institutions of Higher Education
RCW 70.02 - Laws on Health Information Disclosure

Washington Administrative Code (WAC)
Applicable Washington Administrative Codes include the following:
- Chapter 172-190 WAC - Family Educational Rights and Privacy Act of 1974
- Chapter 292-130 WAC - Agency Organization – Public Records
- Chapter 478-276 WAC - Governing Access to Public Records

Washington Information Services Board (ISB)
The Washington Information Services Board is the state of Washington’s policy-making body for information technology. Applicable Washington Information Services Board publications include the following:
- Information Technology Security Policy
- Information Technology Security Standards
- Information Technology Security Guidelines

Code of Federal Register (CFR)
Applicable Code of Federal Register includes the following:
- 16CFR Part 312 - Children’s Online Privacy Protection Rule
- 16CFR Part 313 - Privacy of Consumer Financial Information
- 16CFR Part 314 - Standards for Safeguarding Customer Information
- 28CFR Part 35 - Americans with Disabilities Act
- 29CFR Part 825 - Family Medical Leave Act
- 45CFR Parts 160 & 164 - Health Insurance Portability and Accountability Act

Additional Information Resources
- Eastern Washington University Strategic Goals: http://www.ewu.edu/x9798.xml