Information Security

University Operations – Information Security

EWU Policy 203-01 | **Authority: EWU Board of Trustees**

Effective: February 24, 2023 | **Proponent: Vice President for Business & Finance**

Summary: This policy contains information related to the protection of institutional data and IT systems at Eastern Washington University.

History: This policy revises the previous version of this policy adopted by the EWU Board of Trustees on February 26, 2021. It was approved by the Board of Trustees on February 24, 2023.

Applicability: This policy applies to all users of institutional data and IT systems as described herein.

CONTENTS

CHAPTER 1 – INTRODUCTION

1-1. Purpose

It is the goal of Eastern Washington University (EWU) to ensure the security, availability, privacy, and integrity of its information technology systems and institutional data and to comply with applicable federal and state statutes and regulations.

The purpose of this policy is to support that goal by providing standards for protecting institutional data and defining user and custodial responsibilities for that data. This policy should be used as the basis for any related EWU standards, procedures, and guidelines.

1-2. Scope and Applicability

This policy pertains to all institutional data and IT systems and networks.. It applies regardless of the environment, media, or device where the data resides or is used, the form or format the data may take, or how the data may be transmitted. This policy applies to all users of institutional IT systems, networks, and/or data including staff, faculty, students, agents working on the university's behalf, and others.

1-3. Definitions

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

Availability –Assurance that a computer system is accessible by authorized users whenever needed.

Chief Information Officer (CIO) – the most senior university administrator responsible for the management and implementation of information and computer technologies**.**

Chief Information Security Officer (CISO) – the senior level university administrator responsible for developing and implementing the university's information security program.

Confidential Information – sensitive or private information, or information whose unauthorized disclosure could be harmful or prejudicial.

Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

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

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

Institutional Data – Data created, collected, maintained, recorded or managed by EWU, its staff, and agents working on its behalf. It includes 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.

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

Personally Identifiable Information (PII)- any data that can be used to identify a specific individual, including, but not limited to, social security numbers, driver's license numbers, date of birth, or student identification numbers.

Portable Computing Device – Any device used for computing and/or storage of electronic information. This includes portable computers (i.e. laptops and notebooks), smartphones, etc., as well as storage devices and media such as flash drives, removable hard drives, CDs, etc.

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.

Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

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.

Sensitive Data – Sensitive Data includes information that is protected from disclosure under the law. Sensitive information is often personal in nature but many other types of information such as legal or financial data are also protected. Detailed descriptions of these types of data can be found in RCW 42.56.210 et seq.

User – An individual who has been granted privileges and access to institutional computing, network, and data systems, services, applications, resources, and information.

CHAPTER 2 – Roles and Responsibilities

2-1. Controller

The designated data controller for purposes of compliance with the European Union's (EU) General Data Protection Regulation (GDPR) is the university's Chief Information Officer.

2-2. Data Custodian

Data Custodians play a critical role in protecting the University's institutional data and IT systems. Data Custodians are accountable for the oversight and general operation of institutional data systems. They provide direct authority and control over the management and use of institutional data regardless of where the data resides.

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, Personnel and Workload Data – Associated Vice President, Human Resources

2.3. 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.

2.4. Data User

A Data User is any individual (staff, faculty, students, and agents working on the university's behalf) using institutional data or IT systems in the conduct of university business.

As a condition of access, institutional data users agree to adhere to the Data User Responsibilities described in appendix A, when they access or are in possession of institutional data of any kind. 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.

2-5. Processor

For purposes of GDPR compliance, all data custodians, object custodians and data users are considered processors.

CHAPTER 3 – INFORMATION SECURITY STANDARDS

3-1. General

EWU regards the security and confidentiality of its business data and information to be of significant importance. Each user granted access to institutional data holds a position of trust and must preserve the security and confidentiality of that information.

3-2. Access

a. Access Requirements. Access to institutional data:

(1) Is restricted to individuals whose job duties require it

(2) Is granted only to fulfill the specific functions required to perform a specific job

(3) 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 institutional data for which they are responsible. In some cases, Data and Object Custodians may require users to attend formal training before access is granted.

b. Use of Institutional Data

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 institutional data as it relates to the role or responsibilities of one's position are considered to be routine, and therefore considered an acceptable use.

Under specific conditions, institutional data may also be used for purposes other than official university business. In such cases, use of institutional data may be authorized under other official university policy or related state and federal laws, or with written permission of the Data Custodian responsible for housing and maintaining the data.

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, data users should contact their supervisor or the appropriate Data Custodian.

c. Release of Institutional Data

The authority to release institutional data varies depending on the type of data involved and the person or agency to whom the data is released. In most cases, institutional data should only be released according to the guidelines contained in appendix B. Any release of data which does not conform to these guidelines must be authorized by the appropriate Data Custodian. Any data sharing agreements with persons or entities outside of EWU must be reviewed and approved in accordance with EWU Policy 204-07 (Purchasing, Contracts & Agreements).

3-3. Protection of IT Systems and Institutional Data

Safeguarding institutional data and IT systems requires a combination of personnel security, physical security, and technological security.

a. Personnel security includes restricting access, training users, and administering and complying with this policy.

b. Physical security means taking appropriate measures to secure IT equipment and storage media from unauthorized physical access, vandalism, and theft.

c. Technological security includes all IT equipment, applications, and technologies designed to protect systems and data from compromise.

d. User authentication systems and firewalls are used to restrict access

e. Virus protection applications help protect systems from malicious software

f. Data encryption helps protect information from being compromised even when it has been accessed by unauthorized persons

Inadequate physical security and lack of data encryption pose a significant threat to the security of institutional data. Storing institutional and other sensitive data on laptop computers or portable storage devices/media significantly increases the potential for data to be fraudulently accessed or misused. Similarly, unattended / unsecured workstations create opportunities for IT equipment to be lost or misused and for the data they contain to be compromised. To protect against the compromise of institutional data, precautions must be taken to physically secure IT equipment and storage media containing institutional data and to encrypt such data when adequate physical security is impractical. Related security requirements are described in appendix A.

3.4. 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 data and IT systems and may be subject to disciplinary, civil, and/or criminal actions. The university may temporarily suspend, block, or restrict access to institutional data or IT systems 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.

CHAPTER 4 – UNAUTHORIZED DISCLOSURES AND BREACH NOTIFICATIONS

4-1. Reporting

All EWU employees shall immediately report any suspected unauthorized disclosures of institutional data or any potential security breach of sensitive or confidential information. This includes the disclosure of personal information as defined in RCW 42.56.590 and any student education records as defined in WAC 172-191. A breach includes instances where sensitive or confidential data that was not encrypted may have been acquired or accessed by an unauthorized person or entity.

Reports must be made to the appropriate Data Custodian, Chief Information Officer and the Associate Vice President for Enterprise Risk Management.

Users and departments are expected to work with appropriate university personnel in investigating and addressing reports of suspected unauthorized access or disclosure of institutional data.

4-2. Investigation

EWU will review all relevant facts to determine if a breach of sensitive or confidential information has occurred, including a risk assessment to determine whether or not the security of such information has been compromised.

EWU will also consider the type of data in question, any relevant legal or contractual obligations, and whether or not the breach was reasonably likely to subject consumers to a risk of harm.

The department in which the potential breach occurred shall cooperate with the investigation, assist in remediating identified issues, and may be responsible for funding the response and notification of affected persons.

4-3. Notifications

EWU will provide notifications to affected individuals in accordance with state and federal requirements. Unless another process is required by state or federal law, EWU's notification procedures include sending a notice to affected individuals that meets the following requirements:

a. Written in plain language;
b. Includes contact information for a department at EWU that can answer questions;
c. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
d. A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and,
e. Toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

Unless otherwise required by law, for current and former students and current employees, EWU will send this notification to their official university email. For all other persons and entities, EWU will send notice to the last known email, if available, and if an email is not available, to the last known physical mailing address.

The notification must be sent in a timely manner in accordance with state and federal laws. In most cases, such notification must be sent in the most expedient time possible, without unreasonable delay, and no more than 30 calendar days after the breach was discovered, unless the delay is at the request of law enforcement, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

4-4. GDPR Breach Notification Process

This section is intended to comply with the European Union's (EU) General Data Protection Regulations (GDPR). In addition to the notification requirements specified above, the following additional notifications must be made when a breach involves the data of a person(s) who is physically located in an EU member state.

A. Notification to the Supervisory Authority

1. In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the appropriate EWU supervisory authority of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. "Supervisory authority" means the authority identified for a particular country under GDPR. Where the notification to the supervisory authority is not made within 72 hours, the notification shall be accompanied by reasons for the delay. The supervisory authority for the country(ies) of the individual(s) impacted by the breach may be identified on the European Data Protection Board website. This notification must include:

(a) Description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and the categories and approximate number of personal data records involved;

(b) The name and contact details of a contact at EWU where more information can be obtained;

(c) A description of the likely consequences of the personal data breach;

(d) A description of the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

3. The processor shall notify the Controller without undue delay after becoming aware of a personal data breach.

4. The Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken sufficient to enable verification of compliance with GDPR Article 33.

B. Notification to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall ensure that a notification is provided to such person(s) without undue delay. Such notification must:

(a) Describe in clear and plain language the nature of the personal data breach and contain information about the extent and type of breach, contact information for more information, the likely consequences of the breach, and a description of the measures taken by EWU to address the breach.

2. Notification to the data subject is not required if:

(a) EWU has implemented appropriate technical and organizational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those measures that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

(b) The Controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize; or,

(c) Such notification would involve disproportionate effort. In this case, EWU must issue a public communication or similar measure whereby the data

subjects are informed in an equally effective manner.

3. Even if EWU determines that notification is not required, it will do so if required by the supervisory authority identified in section 4-4(a).

Appendix A – Data User Responsibilities

An individual given access to EWU institutional data in any format acknowledges an understanding of and agrees to adhere to the following:

a. Users shall comply with established policies, guidelines, standards, and procedures, including applicable federal and state statutes and regulations. This includes participating in annual state required security awareness training that covers the risks of data compromise, their role in prevention, and how to respond in the event of an incident.

b. Users shall routinely evaluate their IT security practices based on the requirements of this policy and related guidance.

c. Users shall maintain the security of the systems they use. Users are responsible for all activity that occurs under their information system accounts. Further, users may only share institutional data, in any format, with other users who are authorized to use that data.

d. Users will not share their assigned security access credentials (username and password) for any institutional information technology systems with anyone (this includes supervisors, co-workers, or colleagues). If access to a user's system is required to support the operational needs of the University and the user is unavailable, unwilling, or unable to provide needed information or data, the Office of Information Technology will access the system. A supervisor or manager needing such access shall contact OIT for assistance. To meet the requirements for accessing a system under this section, the following provisions apply.

(1) there must be a need to access specific information or data in support of university operations;

(2) the information or data needed must be reasonably expected to be stored on or accessible through the system in question;

(3) the primary user of the computer or device in question is unavailable, unable, or unwilling to provide the information or data needed;

(4) the vice president or designated representative for the unit involved must approve the access in writing prior to OIT taking action (memo or email approval will suffice);

(5) the provisions of this section shall not be used as a subterfuge to access a system for any other reason; and,

(6) whenever possible, at least two persons shall be present when accessing a system under these circumstances.

e. 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.

f. Departments must inform the Office of Information Technology immediately when an individual student or employee no longer needs access.

g. Users and departments will ensure that workstations connected to EWU IT systems are properly maintained and managed to prevent problems that could affect the EWU computing environment.

h. Users will not leave a workstation unattended while logged into EWU IT systems.

i. Users will take precautions to protect the security and integrity of data to which they have access.

j. Users will take precautions to ensure the physical security of IT equipment and media, including:

- Lock offices and rooms containing IT equipment when unoccupied.
- Secure laptops, media, and other IT equipment when not in use.
- Maintain physical control of portable equipment and media.
- Do not leave equipment/media unattended in a vehicle.

k. Users will take precautions to protect institutional data from being compromised even when IT equipment has been lost or stolen. This includes, but is not limited to:

- Users will store institutional data only on approved network file systems using security settings which prevent anyone other than approved users from accessing the data.
- Users will not store sensitive institutional data on the local hard drive of an office workstation of any type nor move such data to any external media unless approved by the appropriate authority and the file and file system are encrypted.
- Users will not store sensitive institutional data on portable computing devices. In the event there is no alternative to portable storage, data must be encrypted using approved encryption mechanisms provided by the Office of Information Technology. Such local storage on a portable computing device must also be approved by the appropriate Data Custodian.

l. Users will be held professionally accountable in the event of loss or disclosure of EWU data due to negligence in providing reasonable protection for the data.

m. Users will comply with institutional requirements, as described in this policy, for sharing and release of institutional data.

n. When finished working with institutional data that is not subject to records retention guidelines, users should delete and purge electronic files, regardless of format. Similarly, printed documents should be shredded or disposed of in a confidential shredding bin.

Appendix B – Release of Institutional Data

The authority to release institutional data varies depending on the type of data involved and the person or agency to whom the data is released. In most cases, institutional data should only be released according to the guidelines which follow. Any release of data which does not conform to these guidelines must be authorized by the appropriate Data Custodian.

a. To EWU employees: Within the institution, employees may share or disseminate institutional data to other employees who have a legitimate need to access or use the data

b. To external agencies: 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

c. Other: 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, release of institutional data to persons or agencies other than those described in paragraphs a and b above must be approved by an authorized individual and accomplished in accordance with applicable university policies and State and Federal laws. Authorized individuals, in these cases, may include designated Data Custodians, the Director of Institutional Research and the Public Records Officer.

Specific requirements based on the type of data include:

(1) Restricted/ Internal/ Confidential Data: Requests for these data must be referred to the appropriate Data Custodian. If necessary, the Data Custodian will work with the Public Records Officer and/or the Director of Institutional Research to facilitate the release of data. Such data 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 C) and may be defined as personal, private, or confidential.

i. Employee personnel information, payroll data, etc. are considered high risk data due to the potential damage that could be caused through unauthorized disclosure, misuse, or modification.

ii. Student data are also considered high risk and are protected under 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 except as authorized by law. All requests for student information from outside the institution must be referred to Records and Registration Office or the Public Records Officer.

(2) Public Data: To present and interpret institutional data correctly, disclosure of even public data should be done by an appropriate University Official. Although public data may be disseminated freely by such an official, officials should contact the appropriate Data Custodian, the Public Records Officer, or other appropriate official if they have any doubts or concerns about the release of information.

(3) Electronic Data: Preservation and release of electronic data for anticipated or pending legal actions are governed by EWU Policy 201-02 (Records Retention, Preservation & Management). All such activities should be coordinated through the Director of Risk Management.

Appendix C – References

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)

- 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. 200e - 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)

- 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 42.56 - Washington State Public Records Act
- RCW 42.52 - Ethics in Public Service
- RCW 43.105 – Consolidated Technology Services
- RCW 70.02 - Laws on Health Information Disclosure

Washington Administrative Code (WAC)

- Chapter 172-190 WAC - Family Educational Rights and Privacy Act of 1974

Washington Technology Solutions

Sets policy for information technology for the State of Washington: watech.wa.gov

Code of Federal Register (CFR)

- 16 CFR Part 312 - Children's Online Privacy Protection Rule
- 16 CFR Part 313 - Privacy of Consumer Financial Information
- 16 CFR Part 314 - Standards for Safeguarding Customer Information
- 28 CFR Part 35 - Americans with Disabilities Act
- 29 CFR Part 825 - Family Medical Leave Act
- 45 CFR Parts 160 & 164 - Health Insurance Portability and Accountability Act