EASTERN
WASHINGTON UNIVERSITY
start something big

Title:	Incident Response Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:			
Related Policies or Procedures:	EWU 203-01: Information Security Policy		

History

Revision Number:	**Change:**	**Date:**
1.0	Initial version	4/2/2019

A. Purpose

This policy defines the steps that employees must follow to ensure that Information Security Incidents are identified, contained, investigated, and remedied. It also provides a process for appropriate reporting internally and externally.

B. Definitions

Chief Information Security Officer (CISO) - The CISO is responsible for the University's information security program and ensuring that policies, procedures, and standards are developed, implemented and maintained

Incident Response Team – The Incident Response Team may be convened to provide a quick, effective and orderly response to serious information security related incidents.

Information Security Incident: A security incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy

Information Security Breach: A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personally identifiable information (PII) maintained by Eastern Washington University. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure. Personally identifiable information means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

Social security number
Driver's license number or Washington identification card number
Full account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account.
Family Educational Rights and Privacy Act (FERPA) protected information
Health Insurance Portability and Accountability Act (HIPAA) protected information

C. Procedure

Initial Reporting of an Incident

An information security incident begins when a security-related event is reported to the CISO. This could originate from automated detection systems, a trouble ticket submitted by a user, IT staff, or other sources. Anyone suspecting that a security breach or unauthorized release of personally identifiable information has occurred must report it as soon as possible to the CISO. Individuals should not take any containment steps before reporting the incident.

If you suspect a security breach has occured:

1. **Preserve Evidence**: Avoid making any updates or other modifications to software, data, or equipment suspected to be involved
2. **Report the Incident**:
    - Email infosecurity@ewu.edu or call the IT Help Desk extension 2247, or 509-359-2247 from off campus
    - Call the University's CISO extension 4985, or 509-359-4985 from off campus
    - Contact an IT Senior Leadership member or IT representative

Incident Assessment

The CISO or designee will immediately contact the individual that has reported the incident to obtain an initial understanding of the nature and scope of the incident. As needed, the CISO will call an emergency Incident Response Team meeting to determine appropriate next steps. The CISO or designee will prepare an interim report, which will include a description of the incident , the types of data involved, the number of individuals affected, and status of evidence preservation and containment activities.

Incident Response Team

The University Chief Information Officer designates the membership of the Incident Response Team. Membership will include appropriate individuals from Information Technology, Enterprise Risk Management, and, as needed, the appropriate Data Management Custodian. The Incident Response Team, led by the University CISO, will develop and execute communication and Incident Response action plans to ensure:

A. Appropriate action is taken in a timely manner, including reporting, notification and other communication of the Information Security Incident, as required by law or otherwise deemed appropriate.

B. Appropriate progress reports are made on the Information Security Incident and execution of the Plan

Incident Response Team Actions:
Once it is suspected that an information security breach has occurred, the Incident Response Team will begin assessing the potential breach, the severity, remedial steps necessary to prevent ongoing unauthorized access, and consult with other university personnel regarding notification requirements and actions.

The Incident Response Team is responsible for documenting all details of an incident and facilitating communication to other university staff as needed. Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the response must record his or her own actions. The team will:

1. Work with the appropriate parties to determine the extent of the potential breach. Identify systems affected and data stored and compromised on all systems (including non-production systems) and the number of individuals at risk.
2. Identify and contact the appropriate Data Owner (Records Custodian) affected by the breach.
3. Contact all appropriate database and system administrators to assist in the investigation effort
4. Determine the type of personal information that is at risk
5. Have the Data Owner (Records Custodian) determine what records might be affected.
6. Determine if an intruder has exported or deleted any personal information data.
7. Determine where and how the breach occurred. Identify the source of compromise, and the time frame involved. Review the network to identify all compromised or affected systems.
8. Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information, including:
    a. shutting down particular applications or third party connections
    b. altering firewall rules
    c. changing computer access codes
    d. modifying physical access controls
    e. Do not access or alter the compromised system
    f. Do not turn off the compromised machine
    g. Isolate the system from the network (i.e., unplug cable)
    h. Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users.
9. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.
10. Monitor systems and the network for signs of continued intruder access.
11. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date.
12. Compile an Incident Report that provides a summary of confirmed findings and of the steps taken to mitigate the situation.

Communication & Notification

All communications to the general public about an incident or incident response are the responsibility of Marketing and Communications. Private communications with other affected parties should be limited to the minimum information necessary. The minimum information necessary to share for a particular incident is determined by the CIO and the CISO in consultation with other EWU administrative authorities.

Federal and state law and university policy requires notification to individuals affected by unauthorized access or release of personally identifiable information. The Chief Information Officer, Chief Information Security Officer will coordinate with the Vice President of Finance and Administration, the Data Owner (Records Custodian), Associate Vice President for Civil Rights, Compliance and Enterprise Risk Management, Attorney General's Office, and, if necessary, Marketing and Communications to determine notification requirements.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.