Information Security Incident Management and Breach Notification

OVERVIEW
WSU is responsible for ensuring the confidentiality, integrity, and availability of WSU information systems, services, devices, and data under its care, as required by institutional policies and all applicable laws and regulations. As such, it is critical to promptly and effectively respond to information security incidents that may adversely affect the confidentiality, integrity, and availability of institutionally managed and maintained information assets.

Establishing a consistent and coordinated approach to handling security incidents helps to minimize the unauthorized access, misuse, loss, destruction, theft of information and disruption of services that can be caused by information security incidents. Information gained and lessons learned during the incident response process may improve future responses to incidents, improve training, and help to build institutional resilience. Proper handling of information security incidents may mitigate potentially adverse impacts to WSU system:

- Strategic plan and business objectives;
- Financial operations, brand, and reputation; and
- Compliance with applicable policies, standards, regulations, and legal requirements.

Purpose
This section (BPPM 87.55) addresses information security incidents, i.e., those incidents affecting the confidentiality, integrity, and availability of WSU managed and maintained information systems, services, devices, and data. It is intended to provide a WSU system-wide policy and framework to help facilitate development and implementation of consistent and coordinated processes for reporting and responding to information security incidents across the WSU system.

Scope
This policy applies to all WSU system business units, workforce members, systems, services, and devices that collect, store, process, transmit, or share WSU information.

See BPPM 87.01 for definitions and examples of University confidential and regulated information.

POLICY
Information owners are accountable for appropriately responding to information security incidents that may adversely affect the confidentiality, integrity, and/or availability of institutional
Information Security Incident Management and Breach Notification

POLICY (cont.)

All WSU system business units are to:

- Distribute this policy to their workforce members;
- Provide annual security incident response training that is appropriate for workforce member roles and responsibilities;
- Test their incident response processes annually for information systems, services, and data under their purview, to determine the effectiveness of the incident response processes;
- Document the test results;
- Develop and maintain a process to track and document security incidents for institutional systems, services, and data under their care.

INCIDENT MANAGEMENT AUTHORITY AND OVERSIGHT

On behalf of the WSU system, the following individuals have been delegated authority for the oversight and coordination of information security incident and breach response efforts, to include:

- Complying with applicable breach notification laws and regulations;
- Coordinating with WSU system compliance offices, subject matter experts, and resources as appropriate; and
- Coordinating with third parties (e.g., insurance carriers, vendors, law enforcement agencies, or other subject matter experts who may be providing breach response services).

Delegated Authority for Information Security Incident and Breach Response

<table>
<thead>
<tr>
<th>Delegated Authority</th>
<th>Area of Responsibility</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSU Chief Information Security Officer (CISO)</td>
<td>All WSU system confidential and regulated information systems, services, devices, and data</td>
<td>CISO: Telephone: 509-335-1642 E-mail: <a href="mailto:ciso@wsu.edu">ciso@wsu.edu</a></td>
</tr>
<tr>
<td>WSU Chief Compliance and Risk Officer (CCRO)</td>
<td></td>
<td>CCRO: Telephone: 509-335-5524 E-mail: <a href="mailto:compliance.risk@wsu.edu">compliance.risk@wsu.edu</a></td>
</tr>
</tbody>
</table>
Information Security Incident Management and Breach Notification

Delegated Authority for Information Security Incident and Breach Response

<table>
<thead>
<tr>
<th>Delegated Authority</th>
<th>Area of Responsibility</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSU HIPAA Privacy and Security Officer</td>
<td>Protected health information (PHI) for WSU designated health care components</td>
<td>CISO: Telephone: 509-335-1642 E-mail: <a href="mailto:ciso@wsu.edu">ciso@wsu.edu</a></td>
</tr>
<tr>
<td>Assistant Director, Office of Research Assurances (ORA)</td>
<td>Human research subject information</td>
<td>Assistant Director, ORA: Telephone: 509-335-7195 E-mail: <a href="mailto:irb@wsu.edu">irb@wsu.edu</a></td>
</tr>
<tr>
<td>Manager, Office of Research Support and Operations (ORSO)</td>
<td>Controlled unclassified information (CUI); National Security Information</td>
<td>Manager, ORSO: Telephone: 509-335-9661 E-mail: <a href="mailto:orso@wsu.edu">orso@wsu.edu</a></td>
</tr>
<tr>
<td>Export Control Officer, Office of Research Assurances (ORA)</td>
<td>International Traffic in Arms Regulation (ITAR) Information; Export Administration Regulation (EAR) Information</td>
<td>Export Control Officer: Telephone: 509-335-0039 E-mail: <a href="mailto:or.ora.export@wsu.edu">or.ora.export@wsu.edu</a></td>
</tr>
<tr>
<td>Hazardous Material Shipping Specialist, Office of Research Assurances (ORA)</td>
<td>Hazardous materials</td>
<td>Hazardous Materials Shipping Specialist: Telephone: 509-335-0039 Email: <a href="mailto:ora.hazmatshipping@wsu.edu">ora.hazmatshipping@wsu.edu</a></td>
</tr>
</tbody>
</table>

**WSU Information Security Incident Management Team**

The following offices and administrators comprise the membership of the WSU Information Security Incident Management Team:

- Chief Information Officer (CIO)
- Chief Compliance and Risk Officer (CCRO)
- Office of the Attorney General—WSU Division (AGO)
- Chief Information Security Officer (CISO)
- WSU Office of the President/Chief of Staff
- Office of Marketing and Communications
- Office of the Provost and/or College (as required)
Information Security Incident Management and Breach Notification

Incident Mgmt. Team (cont.)

- Office of External Affairs and Governmental Relations (as required)
- Office of Finance and Administration (as required)
- WSU Police Department (as required)
- Office of Research (as required)
- Office of Student Affairs (as required)
- Office of International Programs (as required)
- Office of Human Resources (as required)
- WSU Foundation (as required)
- Director of Intercollegiate Athletics (as required)
- Health Sciences (as required)
- Academic Outreach and Innovation (as required)
- Chief Audit Executive (as required)
- Office of the Chancellor (for non-Pullman campuses (as required)
- Other (faculty, staff, or 3rd party subject matter experts (as required))

INFORMATION SECURITY INCIDENT REPORTING

All information security incidents involving institutional systems, services, devices, and data are to be reported by e-mail or telephone as soon as it is practicable after discovery to the WSU Pullman Information Technology Services (ITS)—Security Operations Center; e-mail abuse@wsu.edu; telephone 509-335-0404.

Security incident reporting is to be provided by telephone or by secure electronic means (e.g., internal WSU Office365 e-mail services). Non-WSU information systems such as commercial e-mail services (e.g., gmail) are not to be used to report security or privacy incidents.
Information Security Incident Management and Breach Notification

INCIDENT REPORTING  
Various state and federal laws and regulations may contain specific incident and/or breach reporting requirements (e.g., FERPA, HIPAA, GDPR, GLBA, PCI, RCW 42.56.590, and RCW 19.255.010). Security incident and data breach reporting processes are to be compliant with all applicable policies, laws, regulations, and standards.

All information security incidents involving an unauthorized or potential disclosure, loss, theft, or misuse of WSU confidential and/or regulated information (see BPPM 87.01) are to be escalated immediately after discovery to the CISO, the CCRO, and the applicable delegated authority. (See the Delegated Authority for Information Security Incident and Breach Response table.) This includes WSU system confidential or regulated information wherever it is stored, processed, or transmitted, including but not limited to:

- Information technology systems;
- Servers;
- Endpoints;
- Wireless and mobile devices;
- Other electronic media,
- Vendor hosted and cloud services, and
- Printed hard copies.

The purpose of the Incident Response Process is to:

- Guide management and staff in responding to, and mitigating the risks resulting from information security incidents; and
- Provide the necessary expertise and resources to respond to security-related incidents appropriately and consistently.

Business units are responsible for internally executing the WSU Information Security Incident Management Process to mitigate the impact of potential security incidents, and to coordinate their incident management processes with the Pullman ITS—Security Operations Center, appropriate information owner(s), central
Information Security Incident Management and Breach Notification

INCIDENT RESPONSE campus ITS unit(s), and/or the delegated authority for information security incident and breach response.

The delegated authority for information security incident and breach response is responsible for the coordination of WSU breach response efforts. However, the business unit experiencing the suspected or actual breach is accountable and responsible for assisting in providing resources to resolve the incident and/or breach in a timely fashion.

The major phases of the incident response process are described below:

- Preparation;
- Identification and assessment;
- Communication and notification;
- Containment;
- Eradication;
- Recovery; and
- Incident closure.

A more detailed process and checklist of the steps necessary for business units to perform during the management of an incident can be found in the WSU Information Security Incident Management Process document.

Preparation

Preparation is fundamental to the success of incident response programs. Preparation activities generally include the proactive and continuous use processes, tools, and training necessary for preventing, detecting, and responding to security incidents affecting networks systems, applications, and devices.

Identification and Assessment

Once an incident has been detected and verified, steps may be taken to correctly identify the incident, assess the scope and impact of the incident, and assign the right amount of resources for the required response.

The initial assessment should provide enough information for the business unit in collaboration with ITS, Information Security Services, and if necessary, the applicable delegated authority for information security incident and breach response, to prioritize subsequent activities. Subsequent activities may include a deeper analysis of the effects of the incident, subsequent containment of the incident, and eradication of the threat.
Information Security Incident Management and Breach Notification

Identification and Assessment (cont.)

Once an incident is detected and verified, steps to be taken during this phase include the following:

• Identify and record the incident;

• Report the incident to the ITS Security Operations Center;

• Preserve evidence;

• Document all decisions made during the incident response process;

• Identify the source, scope, and impact of the incident;

• Determine the severity of the incident and what information is potentially at risk;

• If required, notify the appropriate delegated authority for information security incident and breach response (see the Delegated Authority table);

• If required, the delegated authority assembles the required members of the WSU Incident Management Team (see Incident Management Team);

• Perform a risk assessment of using the RCW 42.56.590 Breach Assessment form (also referred to as the OCIO Data Breach Assessment form);

• If required, contact the cyber liability insurer; review the cyber liability policy and coverages;

• If required, assemble additional members of the WSU Incident Management Team;

• If required, inform University Purchasing Services and/or the Real Estate Business Office (REBO);

• If required, acquire incident response breach response services (e.g., legal services, law enforcement, investigation, forensics services);

• If required, inform the WSU system President, WSU Pullman Chancellor, the Board of Regents, or other appropriate WSU executive officers.
Information Security Incident Management and Breach Notification

Identification and Assessment (cont.)

The initial assessment should provide enough information for the business unit, in collaboration with the ITS Information Security Services team, to prioritize subsequent activities. Subsequent activities may include a deeper analysis of the effects of the incident, subsequent containment of the incident, and eradication of the threat.

Communication and Notification

Communication and notification steps include the following:

- Determine if communications and/or notifications are required to affected individuals, stakeholders, constituents, partners, customers, law enforcement, state and federal agencies, regulatory organizations, or other affected third parties;
- Determine what communication and notifications are to be provided, to whom, and when;
- Develop and execute a communications plan.

Containment

Containment is the process of attempting to actively limit the scope and magnitude of the incident. The primary objectives of the containment phase are to prevent an attacker from causing further damage to WSU information assets, to include the loss of confidentiality, integrity, and availability of WSU systems and data. The containment process is as follows:

- Take steps necessary to contain or isolate the affected networks, systems, and services to limit the scope and magnitude of attack;
- Make a forensic copy of the system for further analysis;
- Ensure that backup media are stored in a secure location;
- Determine risk of continued operation;
- Identify and communicate to all affected parties as required.

Eradication

Eradication is the removal of malicious code, accounts, and other inappropriate access. Eradication also includes repairing system misconfigurations and vulnerabilities that may have been the root cause of the compromise. The eradication process is as follows:

- Remove malicious code, compromised accounts, inappropriate access, and unnecessary system services;
Information Security Incident Management and Breach Notification

Eradication (cont.)

- Mitigate vulnerabilities or system weaknesses that have been found, have been exploited, or may have been the root cause to allow the incident to occur;
- Document any changes to systems, services, or processes;
- Perform a risk assessment to ensure the confidentiality, integrity, and availability of new or updated systems, services, and processes.

Recovery

Once the incident has been contained and the threat eradicated, recovery may start. During this phase, business systems, processes, and data affected by the incident are restored and may be returned to normal operations. The recovery phase is as follows:

- Reinstall systems, and services;
- Reinstall and patch systems and applications;
- Install required security software;
- Perform system and application hardening;
- Conduct system/user access audits;
- Change system and user credentials;
- Restore data to the system;
- Restore systems to normal operations;
- Confirm systems are operating normally;
- Perform system backups as necessary;
- Continue system monitoring for post-incident related activity;
- Communicate to all affected parties.

Incident Closure

Documenting the nature of the incident and the mitigation steps taken to resolve the incident are important. This documentation provides valuable insight into the effectiveness of the incident response plan, identifies issues, and provides an opportunity to improve WSU's incident response processes. Incident closure steps are as follows:
Information Security Incident Management and Breach Notification

Incident Closure (cont.)

- Provide incident summary to the CIO, CCRO, CISO, Internal Audit Office, Attorney General's Office, and other stakeholders as appropriate;
- Ensure proper retention of incident logs and evidence;
- Perform a root cause analysis (to be conducted by ITS, the Internal Audit Office, and appropriate business units);
- Provide recommendations for process and system improvements to the CIO, CISO, CCRO, Internal Audit Office, Attorney General's Office, and other stakeholders as appropriate;
- Follow-up to ensure required actions have been taken.

Enforcement

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable WSU system or state policies and handbooks (e.g., the WSU Faculty Manual, the Administrative Professional Handbook, WAC 357-40 (civil service employees), applicable collective bargaining agreements, and/or the WSU Standards of Conduct for Students, WAC 504-26).

Exceptions

The Office of the CIO manages and maintains exceptions to this policy, under the guidance of the Chief Information Security Officer (CISO).

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exception. Approval for policy exceptions are effective for a specific period of time and must be reviewed by the Office of the CIO on a periodic basis.

Maintenance

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, standards, or regulatory requirements.