WASHINGTON STATE UNIVERSITY

# ITS Process: Information Security & Incident Response

## 1. Purpose & Scope

Information Security and Privacy Incidents must be handled promptly and in a controlled and coordinated manner. The purpose of this Incident Response Process to assist the Information Technology Services (ITS) management and staff in mitigating the risks from security incidents by providing practical steps to appropriately report, identify, and respond to information system security incidents.

This document is not intended to replace Continuity or Disaster Recovery Planning. It is not intended to be used as a detailed list to accomplish every task associated with information security incident handling and response. Rather, the document is intended to provide a framework and processes by which consistent approaches can be developed and resource allocations can be made for a given scenario to facilitate the detection, identification, containment, eradication, and recovery from specific information security incidents.

This document addresses incidents that are information security related, i.e., those systems and devices affecting the privacy, confidentiality, integrity, or availability of ITS managed and maintained information assets. All ITS Departments are covered by this document. This document is intended to provide guidance to address information security incidents that can potentially impact the University's strategic, operational, financial, or reputational standing and the ability to comply with University policies, federal and state standards, regulations, and legal requirements.

## 2. Background

A security incident is defined by the Department of Homeland Security as an occurrence that (a) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or (b) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.1 An incident could be either intentional or accidental in nature.

Examples of security incidents can be found in the ITS Incident Response Plan.

Establishing security incident response capabilities at Washington State University ensures systematic (i.e., following a consistent information security and privacy incident handling

methodology) and coordinated actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by information security and privacy incidents. Incident response capabilities and procedures also build institutional resilience. Information gained, and lessons learned during incident handling can help better prepare for dealing with future incidents.

## 3. Reporting a Security Incident

Security incidents should be reported immediately to Information Security Services or as soon as possible after discovery.

Security incidents can be reported in several ways including by email, phone, or in-person. Information Security Services Contact information: abuse@wsu.edu or 509-335-0404 - for a list of Information Security Services staff contact information, see Appendix XX.

The Incident Response Manager (see Incident Response Members and Roles Table below) should be notified directly of any critical security events (e.g., system security alerts, unauthorized activity, system intrusions, security events involving University Confidential or Regulated data).

If the incident involves University Confidential or Regulated data, the Incident Response Manager will promptly inform the CISO of the incident. The CISO will inform the proper Delegated Authority according to the Incident Response BPPM. (Provide link to policy here when available)

Further guidance on reporting information security incidents can be found in Appendix I of the ITS Incident Response Plan.

## 4. Incident Response Team

The ITS Incident Response Team is comprised of appropriate management and staff from Information Security Services, other business units within ITS, and business units who have a current SLA with ITS. Incident response team members should have the required skills to identify and control system compromises or other intrusions.

The ITS Security Operations Manager (or designee) will act as the Incident Response Manager (IRM) for all reported computer security incidents. The Incident Response Manager, with the assistance of the reporting entity will work together to coordinate all aspects of the

incident response process. The reporting entities shall coordinate with the Incident Response Manager (or designee) prior to initiating any actions during the investigation or in response to information security incidents. All communications regarding computer security incidents are to be conducted through channels that are known to be unaffected by the computer security incident under investigation.

ITS Incident Response members and roles are listed in the table below. IRT members shall be trained on the incident response process and on methods for handling security incidents. Members of the ITS incident response team should ensure their availability at all times to be able to respond to system intrusion and alerts from threat detection, response, and prevention systems.

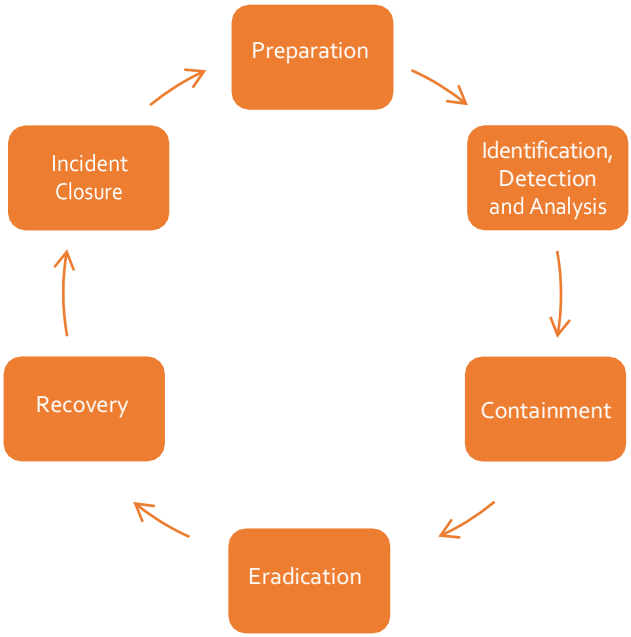
## Incident Response Team Members and Roles

| Members | Role |
|---|---|
| ITS Senior Management | Provide authority to operate and has authority to make business -related decisions based on information garnered from the other team members. |
| ISS Security Operations Manager | Acts as Incident Response Manager for all reported security incidents. Coordinates all aspects of the incident response process. |
| Information Security Services | Assess security incidents, perform containment, eradication and basic forensics. Assist information technology in recovery role. |
| Information Technology Management and Staff (or WSU Business Unit Personnel if current SLA exists) | Minimize the impact to systems end users. Assist the Information Security team with technical issues and with incident assessment, containment, eradication, and recovery processes recovery roles. |
| Physical Security | Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence. |
| Human Resources/Internal Audit Office/Attorney General's Office | Provide advice to ITS senior management on employee, ethical, and legal issues related to the incident. |

# 5. The Incident Response Process

This section describes the major phases of the incident response process—preparation, detection, identification and analysis, containment, eradication and recovery, and post-incident activity.

Appendix D of the ITS Incident Response Plan provides a checklist of the major steps to be performed during different phases of handling an Information Security and Privacy Incident. The checklist does not dictate the exact sequence of steps that should always be followed and should be used to guide for those involved. Appendix D also provides basic Unix/Linux and Windows Operating Systems Checklists for responding to system compromises.




## Preparation

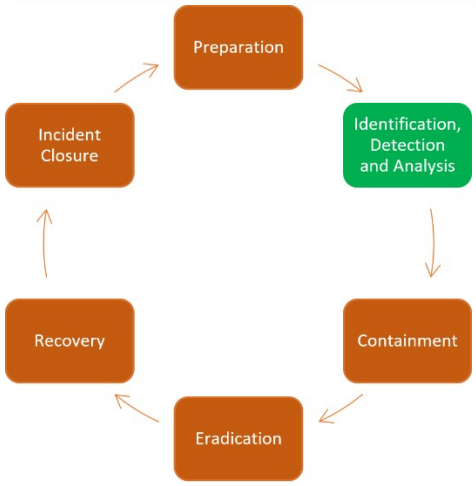
Preparation is fundamental to the success of incident response programs.
Incident response methodologies typically emphasize the proactive and ongoing use of tools, training, and processes necessary for preventing and/or mitigating incidents by ensuring that systems, networks, and applications are sufficiently secure. Incident response team members should be properly trained on incident response processes to include identifying and controlling system compromises and other intrusions.

One of the recommended preparation practices is for University colleges and departments to conduct an annual IT Risk assessment. The benefits of conducting an IT Risk Assessment include identifying applicable threats, including organization-specific threats. Each risk is categorized and prioritized to determine if risk can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.

**Conducting an IT Risk Assessment enables departments to correlate IT resources with mission critical business processes and services. Using that information, it then becomes possible to characterize interdependencies and the consequences of potential disruptions, as well as to generate plans to eliminate or ameliorate risks.**

## Identification, Detection, and Analysis

Early steps taken to detect, identify, investigate, and analyze an incident are important to developing an effective containment and eradication strategy. Once an Information Security and Privacy Incident has been confirmed, resources can be assigned to investigate the scope, impact, and response needed. The detection and analysis phases determine the source of the incident and preserve evidence.




The general steps required for incident identification, detection, and analysis are to:

- Review Internal Audit guidelines for department personnel actions regarding unacceptable computer use and other computer security incidents - See Appendix G.
- Observation of the anomalous event.
- Determine whether an incident has occurred and its scope.
- Determine the severity of the incident.

Coordination between ISS and the affected department is important to make sure that steps taken to verify the incident and not to alter data that will be needed for further investigation.
ISS will work with the affected department to quickly analyze and validate each incident and perform an initial assessment to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g.,

what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.
A coordinated investigation may be required once an incident has been confirmed. The Incident Response Manager will lead the incident response effort, is the point of contact for all matters relating to the incident and is responsible for coordinating the data required for documenting the investigation and gathering evidence. In some cases, Federal, State, or local law enforcement may be involved in an incident investigation. See Appendix I in the ITS Incident Response Plan for contact information for the Federal Bureau of Investigations (FBI), Department of Homeland Security (DHS), state, campus, and local police.

**Inter-departmental Cooperation Guidelines**

Once University personnel is alerted to a threat from an internal or external source, it is important to notify ISS once a threat has been detected.
• The local systems administrator is responsible for fixing the problem on the machine(s)
• All incidents should be handled by departmental IT staff with the support of ISS and, if necessary, the ITS IRT.

For further guidance on gathering security incident data and incident reporting, see:
*See Appendix E in the ITS Incident Response Plan: Compromise Questionnaire and Information Gathering*

*See Appendix I in the ITS Incident Response Plan: Guidance on Reporting a Security Incident*

Incident Categorization, Classification, and IRT Activation
The incident type and impact will determine the level of response needed by the University. ISS will work with departments to determine the appropriate response for each confirmed incident. The general steps required for incident categorization and classification are:
1. Categorize the incident based on type of incident, security objective, and impact.
2. Classify the incident as a local or enterprise incident.
3. Prioritize handling of the incident based on the WSU CSIRT Incident Response Classification Matrix
4. Activate IRT if necessary
5. Report the incident to the appropriate internal personnel and external organizations.

### Common Categories of Computer Security Incidents

| Incident Type | Description |
|---|---|
| Unauthorized Access | When an individual or entity gains logical or physical access without permission to a university network, system, application, data, or other resource. |
| Denial of Service (DoS) | An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS. |
| Malicious Code | Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software. |
| Improper or Inappropriate Usage | When a person violates acceptable computing policies. |
| Suspected PII Breach | If an incident involves personally identifiable information (PII) a breach is reportable by being merely **Suspected**. (Suspected PII incidents can be resolved by confirmation of a non-PII determination.) |
| Suspected loss of Sensitive Information | An incident that involves a suspected loss of sensitive information (not PII) that occurred as a result of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) Use, where the cause or extent is not known. |

**Source**: Incident Response and Management: NASA Information Security Incident Management

## Impact Definitions

| | Potential Impact | | |
|---|---|---|---|
| **Security Objective** | **Low** | **Medium** | **High** |
| **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals |
| **Integrity:** Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

| | | | |
|---|---|---|---|
| **Availability:** Ensuring timely and reliable access to and use of information | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

**Source**: FIPS Publication 199

Once an incident is classified, it is important to categorize the incident as a local or enterprise event.

**Local events** represent a risk to Washington State University systems, networks, and data but are confined to a single or small number of departmental systems. An example of a local issue would be malware discovered on a departmental desktop or server. Local issues may even lead to data breaches if unencrypted sensitive data is stored on the compromised systems. Most computer security threats are identified, contained, and eradicated through coordinated efforts between ISS and affected departments. Local events are the most common type of attack observed at Washington State University.

**Enterprise events** are rare but have a large impact. A Distributed Denial of Service attack (DDoS) that degrades network performance in a manner that disrupts University operations is an example. This would be an enterprise-wide issue that would affect the entire University. Enterprise issues may require the activation of the Computer Security Incident Response Team (CSIRT). CSIRT team members may be drawn from many departments across the university and have knowledge of critical systems that can be leveraged to protect Washington State University IT assets during an enterprise incident.

When multiple incidents occur simultaneously, the most serious or highest potential impact incidents should be handled first.

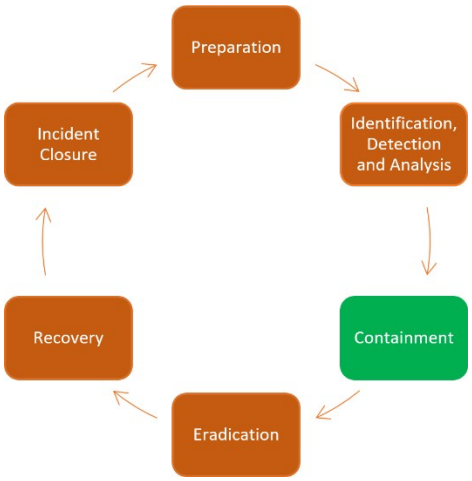
The incident classification is performed by the Incident Response Manager (IRM) using the WSU IRT Incident Response Classification Matrix.

**IRT Incident Severity Classification Matrix**

| Classification Level (3=Most Severe) | Typical Characteristics | Impact | Response | Activate IRT |
|---|---|---|---|---|
| 3 | DDoS attack against University Servers. Attacks against network infrastructure. Network disruption for a large segment of the WSU population | An enterprise-wide attack involving multiple departments requiring local and enterprise administrator support from the affected departments. | CSIRT directs, response coordinated by ISS. WSU senior management, local sysadmin involved. Possible Legal Counsel, Law Enforcement involvement | Yes |
| 2 | Affects data or services for a group of individuals and threatens sensitive data, or involves accounts with elevated privileges with potential threat to sensitive data | Compromised Banner, Exchange, Active Directory, domain controller system administrator account, or Learning Management System (LMS) administrator account compromise | Response coordinated by ISS. Local Sysadmin. CSIRT advised, Legal Counsel notified if PII breach. | Advised |
| | Affects data or services of a single individual, but involves significant amounts of sensitive data | Faculty desktop with University defined sensitive data compromised, physical theft of computer/computer equipment | | No |

| | | | | |
|---|---|---|---|---|
| 1 | Affects data or services of a group of individuals with no sensitive data involved | Compromise of an account with shared folder access | Local sysadmin, ISS notified, event logged, progress monitoring, Standard forensics performed if local admin is unable. | No |
| | Affects data or services of a single individual with no sensitive data beyond their own involved; focus is on correction and/or recovery and education/future prevention | Compromised faculty machine w/no University defined sensitive data etc. | | No |
| **0** | Occurrences of very minor or undetermined focus, origin and/or effect for which there is no practical follow-up | Network scans, firewall logs | ISS monitors periodically, periodic summaries, vulnerability database maintenance sends reports to central logging facility for trending weekly/monthly reports. | No |

# Containment




Containment procedures attempt to actively limit the scope and magnitude of the attack. A vulnerability in a particular IT architecture can be exploited quickly. Containment involves acquiring, preserving, securing, and documenting all evidence.

Containment has two goals:

• System isolation to prevent data from leaving the network via the affected
machines.
• Prevent attacker from causing further damage to Washington State University information assets.

ISS assigns a high priority to determining who the attackers are and what vector (port, software vulnerability, etc.) they are using to attack Washington State University hosts. Once this information is obtained, ISS may request a router block or physical disconnection to temporarily prevent an IP address, port or both from connecting to the WSU network. This may disrupt other normal traffic, but this disruption will be kept to a minimum. Containing a security incident generally has a higher priority than maintaining normal business traffic.
The following actions are taken during the containment phase:

**Coordinate all activities with local system administrator. Possible actions include:**

• Upon direction by the IRM, the local system administrator can proceed to repair the system as needed to return to normal business operations.
• Consulting provided by ISS to the local system administrator. ISS will remain available to provide consulting support during the repair process.
• The deployment of a small team from ISS with the appropriate expertise to the site.
• Securing the physical area on site if necessary.
• Gathering further information if required. *See Appendix E: Compromise Questionnaire and Information Gathering to guide documentation.*
• A review of the information provided by the system administrators.
• Not allowing the system to be altered in any way. Maintaining a low profile in order to avoid tipping off the attacker.
• Using a trusted system binary kit (Unix/Linux, Windows) to verify the system binaries have not been compromised.

• Making a forensic copy of the system for further analysis. Ensuring that any backup tapes are in a secure location.

***Determine risk of continued operation.***

Possible actions include:

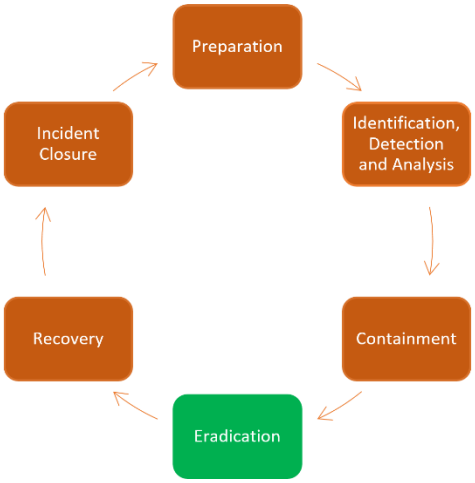
• Disabling network access but leaving the system up. Disabling the port if the attack is ongoing or if the compromised system is attacking another site. The Network Team should utilize available tools to identify and disable the port.
• Making a recommendation to the local management (faculty member, department head, dean, supervisor, etc.) regarding whether the affected system(s) should remain online. Attempting to restore operations as quickly as possible. However, if the compromised system threatens the integrity of the network, systems, or data, it should be disconnected from the network as soon as possible.
• Changing all user and system credentials on the affected machine(s).

**Back up the system**

• In some cases, a forensic image disk will be requested by law enforcement or by the WSU Attorney General. Contact ISS to initiate the forensics process.
• Use network backup systems to determine what files were changed during the event.

## Eradication

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. We strongly recommend a complete re-installation of the OS and applications.
The general steps involved in the eradication phase of incident response are to:



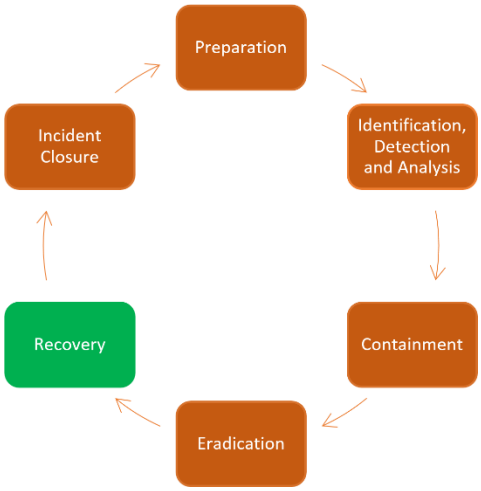
• Define eradication benchmarks
• Consult various checklists for compromises. See Appendices D & E of the Incident Response Plan for additional information
• Identify and mitigate all vulnerabilities that were exploited
• Remove malware, inappropriate materials, and other components
• Remove unnecessary system services
• Reinstall OS, apply patches, reinstall applications, apply known patches, and required security software
• If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps to identify all other affected hosts, then contain and eradicate the incident for them

## Recovery

Once the incident has been contained and eradicated, recovery can start. This phase allows business processes affected by the incident to recover and resume normal operations.

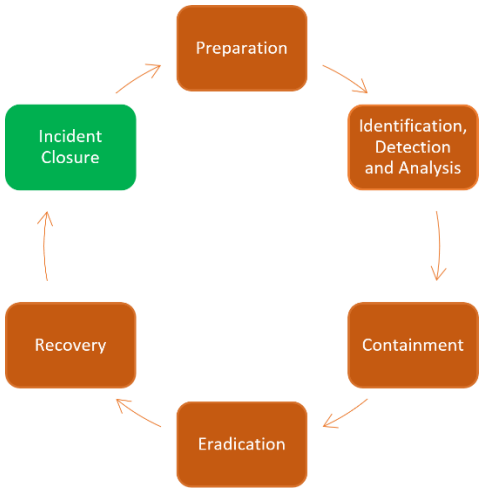
The general recovery steps are:

1. If there was sensitive data on the affected machine, go to step 2. If there was not, go to step 4.
2. Follow the flow chart steps in Appendix B.
3. Conduct the following, 1) Reinstall and patch the OS and applications, 2) Install required security software and perform OS and application hardening, 3) conduct an user/system access audit, and 4) change all user and system credentials.
4. Restore data to the system.
5. Return affected systems to an operationally ready state.
6. Confirm that the affected systems are functioning normally.
7. Continue system monitoring for future, incident-related Post-Incident Activity.



# Incident Closure

Documentation of a security incident and the steps taken to mitigate issues encountered are important. The documentation offers an opportunity to improve Incident Response processes and identify recurring issues. Most local issues can be properly documented using the University's Cougtech ticket system. Certain security incidents should be documented more thoroughly when their impact warrants. ISS will identify those local incidents that should be more thoroughly documented. A follow up report and documentation is required for all enterprise level incidents. Follow-up reports document the incident and include the lessons learned in order to preserve and expand knowledge.




Depending on the scope of the incident, an incident follow-up report may be produced by ISS and the IRT. A more comprehensive Root Cause Analysis may also be conducted by ISS in collaboration with the Office of Internal Audit. The purpose of this report is to understand any systemic issues that may have contributed to the incident, provide lessons learned, and risk mitigations to prevent or reduce the likelihood of a recurring incident.

Any follow-up reports should include the following:

- Information about the incident type
- A description of how the incident was discovered
- Information about the systems that were affected
- Information about who was responsible for the system and its data
- A description of what caused the incident
- A description of the response to the incident and whether it was effective
- Recommendations to prevent future incidents
- A discussion of lessons learned that will improve future responses
- A timeline of events, from detection to incident closure
- The follow-up report should be shared with the VP for Information Technology and CIO as well as other stakeholders deemed appropriate. A “Lessons Learned” meeting with all those involved in the handling and response of the incident should be held and is mandatory for enterprise level incidents.

# 4. Appendix A- Assignment of IRT Member Roles and Responsibilities

The following table contains the assignment of roles for the security incident response team.

| Name | Title | Email Address | Office Phone | Role | Availability |
|---|---|---|---|---|---|
| Michael Walters | Chief Information Security Officer | michael.walters@wsu.edu | 335-0690 | Incident Response Mgr | 24x7 |
| Jim Walsborn | Data Security Analyst | jim.walsborn@wsu.edu | 335-9776 | Senior Security Analyst | 24x7 |
| Rebecca Solen | Data Security Analyst | rebecca.solen@wsu.edu | 335-5051 | Security Analyst | 24x7 |
| Brian Hall | Data Security Analyst | brian.hall2@wsu.edu | 335-0849 | Security Analyst | 24x7 |
| Bill Bonner | | bbonner@wsu.edu | 335-9161 | Subject Matter Expert | 24x7 |
| Bill Rivers | | bill.rivers@wsu.edu | 335-0015 | Subject Matter Expert | 24x7 |
| Justin Hughes | | justin.hughes@wsu.edu | 335-0637 | Subject Matter Expert | 24x7 |
| Gary Saunders | | gary.saunders@wsu.edu | 335-1003 | Subject Matter Expert | 24x7 |
| Dave Whelchel | | whelchel@wsu.edu | 335-0497 | Subject Matter Expert | 24x7 |