*<*WWU System*>*
Incident Response Plan

**System:** <APPLICATION / SYSTEM NAME>

**Last Update:** <DATE>

Contents

[Introduction 2](#_Toc83191460)

[System Overview 2](#_Toc83191461)

[Architecture Model 2](#_Toc83191462)

[System Hardware Inventory 2](#_Toc83191463)

[Audit Logging 2](#_Toc83191464)

[System Contacts 2](#_Toc83191465)

[Incident Response Workflow 3](#_Toc83191466)

[Incident Response Procedures 3](#_Toc83191467)

[Detection 3](#_Toc83191468)

[Incident Reporting 4](#_Toc83191469)

[Initial Investigation 4](#_Toc83191470)

[Containment 4](#_Toc83191471)

[Incident Characterization and Risk Classification 4](#_Toc83191472)

[Communications 4](#_Toc83191473)

[Detailed Investigation 4](#_Toc83191474)

[Remediation and Recovery 5](#_Toc83191475)

[Data Loss and Breach Reporting 5](#_Toc83191476)

[Post-Incident Lessons Learned 5](#_Toc83191477)

[References 5](#_Toc83191478)

# Introduction

This is the System Incident Response Plan (SIRP) for <APPLICATION/SYSTEM NAME> that documents the procedures for responding to a cybersecurity incident.

The goal of the SIRP is to provide tools to help technical staff who are responsible for supporting enterprise or mission-critical systems and systems containing confidential data. The plan assists in effectively responding to security incidents and minimizing any negative impact to institutional operations through a set of detection, analysis, and recovery activities.

# System Overview

<Provide a summary of the covered system’s business and technical functions. If the information is maintained in other documents, provide links to those documents.>

# Architecture Model

<Attach a high-level diagram of the application/system data flow and data storage, including all interconnected system names and networks>

# System Hardware Inventory

<Insert hardware inventory of covered devices. You may provide a link to the inventory file.>

# Audit Logging

<Insert details of the application system audit logging processes. Include details about where the log files are located, as well as a brief description of the events captured in each log file.>

# System Contacts

The University’s IRP requires identification of key contacts. See the University’s IRP for definitions if needed. The <Application/System Name> Incident Response Team (IRT) includes the following staff:

|  |  |  |  |
| --- | --- | --- | --- |
| **Role**  | **Work Phone** | **Home Phone** | **Email Address(es)** |
| **Incident Response Coordinator (IRC)\*** |  |  |  |
| **System Steward or Service Owner\*** |  |  |  |
| **Chief Information Officer (CIO)\*** |  |  |  |
| **Information Security Office Contact(s)\*** |  |  |  |
| **ATUS Contact(s)**\* |  |  |  |
| <Other relevant contacts>\*\* |  |  |  |

\* Required.

\*\* Add any other relevant contact including, but not limited to Campus Police, Enterprise Infrastructure Services, Enterprise Applications Services, HIPPA officer, FERPA officer, Human Resources, public relations, internal auditor, Attorney General Office, and technical staff.

Incidents should be reported as per the University’s IRP. Those that have a Major Risk classification should be handled according to this SIRP.

# Incident Response Workflow

Incidents follow a standardized workflow as shown below.



Fig 1. High-Level Incident Response Workflow

# Incident Response Procedures

## Detection

<Summarize any possible ways cybersecurity incidents may be identified on the system. For example, management interfaces, alerts, logs, etc.>

## Incident Reporting

All suspected incidents found by an end user should be reported to their supervisor. They should also [open a ticket](https://wwuhelp.atlassian.net/servicedesk/customer/portal/1/group/17) with the ATUS Help Desk.

Any suspected incidents found by a system administrator (sysadmin) via checking dashboards, reports, or receiving alerts may proceed to the initial investigation.

## Initial Investigation

An initial investigation should be done to determine if the suspected incident is real.

*<Summarize any easy steps that can be taken to investigate an incident in the system. Examples include interviewing end users, reviewing error messages, checking the MS Security Center.>*

If an incident has been found to be real, a ticket should be opened with the ATUS Help Desk if not yet done.

## Containment

If an incident was found to be real, steps should immediately be taken to contain the incident. Any containment steps should be logged.

<Summarize ways that incidents may be contained in the system. Examples are shutting applications or servers down, disconnecting servers from the network, disabling accounts.>

Any real incident should have an ATUS Help Desk ticket created if not yet done.

## Incident Characterization and Risk Classification

After containment, the incident should be characterized as per the University IRP. The Incident Response Coordinator (IRC) will work with the ISO and the CIO to determine if the incident risk classification is Major.

<Add a summary of indicators of a Major incident such as a loss of confidential data or unauthorized access to confidential data.>

The Cybersecurity Major Incident Documentation form in Appendix B of the University’s IRP should be started for Major incidents.

## Communications

*<List customer communication channels (DLs, ATUS, University communications office).>*

## Detailed Investigation

For Major incidents, the following procedures should be followed for an investigation:

<List possible ways to investigate and document the security issue such as:

* Reviewing actions by system users.
* Checking emails.
* Researching error messages.
* Taking screen shots.
* Reviewing access in system and application logs.
* Using MS Defender for Endpoint.
* Using Cloud App Security.
* Using Splunk (e.g., firewall, netflow, DNS, DCHP, Active Directory, Office 365 events.)
* Checking networking equipment logs.
* Checking audit trails in Azure Security.
* Listing Data impacted.
* Encryption status of data.
* Anything else that might be useful.>

Any observations and decisions made based upon discussion or evidence analysis should be documented.

## Remediation and Recovery

<Lists ways that potential security issues can be remediated and any procedures for recovery. You can reference a DR plan here if desired.>

## Data Loss and Breach Reporting

*<List any confidential data stored in the system and any compliance actions such as reporting to our FERPA officer.>*

Once a suspicious event is detected, the *Incident Handler* should start by determining whether suspicious system events constitute a *Security Incident*.

# Post-Incident Lessons Learned

Document any lessons learned from the incident and any actions that must be done to prevent the issue in the future.

# References

<Provide any references that would be helpful during a cybersecurity investigation.>