

DRAFT
Marshall University Incidence Response Plan (MU IRP)

What is an incident?

An incident is the act of violating an explicit or implied security policy. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

We encourage you to report any activities that you feel meet these incident criteria. It is our policy to keep any information specific to your systems confidential.

Benefits of an Incident Response Plan

- Respond to incidents systematically so that appropriate actions are taken.
- Help the University to recover quickly and efficiently and minimize loss and disruption of services.
- Use recommendations gathered from the post-mortem meeting to better prepare for future incidents and provide stronger protections for University data and assets.
- Deal properly with legal issue

Roles and Responsibilities

Level 1: MU Executive Response Team

- President of the University
- Vice President of IT/CIO or Assistant Vice President
- Information Security Officer (ISO) No One with Formal Title
- Chief of Staff/University Counsel
- Provost, Academic Affairs or designee
- Director of Human Resources
- Dean of Student Affairs
- Chief of Police
- Internal Audit
- Vice President of Communications

Level 2: IT Response Team

- Information Security Officer
- Systems Administration
- Networks and Telecommunications
- IT Customer Service
- DataBases and Shared Systems
- Affected Department Representative

Action Steps

Step 1 -Information Security office is notified that a potential or actual breach has occurred.

How are they informed?

Through the help desk?

Via a direct contact? i.e., Form www.marshall.edu/it/security ,

What is the process?

Step 2 – The IT Response Team designate meets with department to discuss and begin documenting the incident.

Every incident will be different. However, several basic questions will be asked during the initial interview:

- What happened?
- What systems, devices, etc., were compromised?
- What is the net damage and costs?
- Was information lost or stolen? If yes, what?
- Was the information sensitive or PI?
- How was the information acquired?
- How was the system or device configured?
- What are the maintenance procedures?
 - Do log files exist?
 - Who was affected by the breach?

Step 3 -If necessary, and with approval from the MU Executive Response Team, the IT Response Team seeks IT experts or other external information to mitigate the problem and complete initial evidence collection.

In addition to detailed documentation it is important to preserve evidence.

- The preservation of evidence is important if you intend to:
 - Continue to analyze the problem after the initial intervention, and cleanup process has ended.
 - File criminal charges.
 - Involve law enforcement.
- We will be developing standard methods to preserve evidence with time limitations.

Step 4 – IT Response Team submits preliminary report and Severity Level (see Appendix B) to IS0 and AVP IT within (48 hours?)

If the Severity Level is 3 the incident is handled by internal standard operating procedures.

If the Severity level is a 1 or 2 the ISO or AVP IT inform the VP IT/CIO and with concurrence of the President the MU Executive Response Team is activated and briefed on the incident.

Severity Level 2: Internal Remediation and Communication Procedures:

- Assemble the MU Executive Response Team to discuss the incident, confirm the Severity Level and, in conjunction with the IT Response Team, develop the remediation and communication plan and begin those processes.
- Notify general counsel, the President's office, and the director of WV Office of Security of the incident.
- Inform the department's management team that the incident is reportable.
- If necessary, contact the appropriate law enforcement agencies to file a report.

Severity Level 1: External Remediation and Communication Procedures:

- Assemble the MU Executive Response Team to discuss the incident, confirm the Severity Level and, in conjunction with the IT Response Team, develop the remediation and communication plan and begin those processes.
- Notify general counsel, the President's office, and the director of WV Office of Security of the incident.
- Inform the department's management team that the incident is reportable.
- If necessary, contact the appropriate law enforcement agencies to file a report.

The notification letter, press materials and other external communications are written by the ISO, AVP IT and the Institutional Communications Office in conjunction with the MU Executive Response team.

Contents of the Notification Letter

The notification letter contains the following pieces of information:

- Description of the breach.
- Contact information for the major credit reporting agencies:
 - Trans Union
 - Experian
 - Equifax
- Recommendations:
 - Place a fraud alert on the credit report
 - Monitor credit reports
- University contact information

Distributing the notice of a breach

Notifications are sent to individuals in one of two ways:

- If 50,000 or fewer individuals:
 - Send a letter to each individual on University letterhead via first class mail.
- If more than 50,000 individuals
 - Send notification to a last known email address
 - Conspicuously post a "Notice of Breach" on the campus web site
 - Notify statewide media including television, radio and print media

Training Staff to Respond to Inquiries

University Staff will be trained to answer several basic questions:

- What happened?
- Who attacked you?
- When did it happen?
- How did they breach your security?
- How widespread is the breach?
- What steps are you taking to determine what happened?
- What steps are you taking to prevent this from happening again?
- What is the estimated monetary cost of this incident?

During training, staff will be instructed to do the following:

- Do not offer unsolicited information or comments to inquirers.
- Advise the inquirer that the incident is under investigation (if this is the case).
- Direct the inquirer to a web site, www.marshall.edu/itlsecurity/ Include Best Practices, Tips, Form, etc
- Direct inquiries from law enforcement to the University Police department.
- Direct inquiries from the media to the Director of Public Affairs.
- Direct inquiries from vendors to the Information Security Office.

Step 5: Post-Mortem review and plan implementation

Appendix A Process Diagram

Appendix B Incident Severity

Severity	Symptoms
1	<ul style="list-style-type: none">A. Network or system outage with significant impact to the user population or operation of the University.B. High probability of propagation.C. Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.)D. Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities.E. Notification of entities outside of the University is required.
2	<ul style="list-style-type: none">A. Some adverse impact to the operation of the University.B. Adverse effects are localized or contained, or minimal risk of propagation.C. No apparent release or compromise of sensitive data.D. Remedial but not immediate action is required.E. Notification of entities within the University is required.
3	<ul style="list-style-type: none">A. Minimal impact to small segment of user population or operation of University.B. Completely localized, with few individuals affected, and presenting little or no risk to other entities.C. No loss or compromise of sensitive data.D. Remedial action is required.E. Individual notification is required.