Marshall University Information Technology Council

PROCEDURE No. ITP-19

INFORMATION SECURITY INCIDENT RESPONSE PROCEDURE

1. General Information

1.1. Scope:

This procedure applies to all university employees (faculty, staff, student, contract employee, or contract partner) who have access to university information and to systems that store, access, or process the information.

1.2. Authority:

W. Va. Code §18B-1-6, WVOT-PO1001, and MUBOG IT-2

1.3. Passage Date:

April 4, 2007

1.4. Effective Date:

April 13, 2007

1.5. Revision Date:

August 19, 2019

1.6. Controlling over:

Marshall University

1.7. History and Rationale:

The University's information resources are vital academic and administrative assets for which the Information Security Policy establishes guidelines and responsibilities for their protection and preservation. Paper-based systems, computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability, and confidentiality of the information. Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the University's information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate. This procedure defines the institution's protocol and procedure to

respond to incidents that might threaten these resources or expose the University, its students, faculty, staff, and other associates to liabilities.

1.7.1. Statutory References: Marshall University references the State of West Virginia Information Security Guidelines (http://www.technology.wv.gov/ProductsAndServices/Documents/WVStateInformationSecurityPolicy.pdf) issued by the Governor's Office of Technology as a baseline.

2. Procedure: Marshall University Information Security Incidence Response Plan

2.1. What is an incident?

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

2.1.2. attempts (either failed or successful) to gain unauthorized access to a system orits data unwanted disruption or denial of service

2.1.3. the unauthorized use of a system for the processing or storage of data

2.1.4. 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.

2.2. Benefits of an Incident Response Plan. It allows the institution to:

2.2.1. Respond to incidents systematically so that appropriate actions are taken.

2.2.2. Recover quickly and efficiently and minimize loss and disruption of services.

2.2.3. Use recommendations gathered from the post-mortem meeting to better prepare for future incidents

2.2.4. Provide stronger protections for University data and assets and

2.2.5. Deal properly with legal issues

2.3. Roles and Responsibilities

2.3.1. Level 1: Executive Response Team

2.3.1.1. Membership

2.3.1.1.1. President

2.3.1.1.2. Chief of Staff

2.3.1.1.3. Senior VP Academic Affairs/Provost

2.3.1.1.4. Chief Financial Officer

2.3.1.1.5. Chief Information Officer

2.3.1.1.6. Information Security Officer (ISO)

2.3.1.1.7. University Counsel

2.3.1.1.8. Director of Human Resources

2.3.1.1.9. Dean of Student Affairs

2.3.1.1.10. Chief of Police

2.3.1.2. Role

2.3.1.2.1. Make final determination regarding the Severity of the incident

2.3.1.2.2. Make final determination regarding notification and public information

2.3.1.2.3. Make final decision regarding involvement of external sources, agencies, consultants, and law enforcement.

2.3.1.2.4. Approve short and long-term plans and response to the incident.

2.3.1.2.5. Provide advice and direction to the IT Response Team.

2.3.2. Level 2: IT Response Team

2.3.2.1. Membership

2.3.2.1.1. Information Security Officer

2.3.2.1.2. IT Infrastructure Systems

2.3.2.1.3. IT Infrastructure Communications

2.3.2.1.4. IT Customer Service

2.3.2.1.5. IT Enterprise Applications

2.3.2.1.6. Affected Department Representative

2.3.2.2. Role

2.3.2.2.1. Coordinate the response to the incident while insuring compliance with this procedure.

2.3.2.2.2. Coordinate and perform the investigation of the incident with other internal or external entities.

2.3.2.2.3. Seek advice and consent from the MU Executive Response Team

2.3.2.2.4. Document the notification, investigation details, decisions, final short-term plan implementation and incident resolution.

2.3.2.2.5. Coordinate and document long-term improvements or modifications to security or other process resulting from the post-mortem analysis of the incident

2.4. Action Steps

2.4.1. Step 1 -Information Security office and the IT Response Team is notified that a potential or actual breach has occurred.

How are they informed?

2.4.1.1. Through the IT Service Desk

2.4.1.2. Via a direct contact -- e.g., Form https://www.marshall.edu/it/departments/information-security/incident-report-form/ or email to abuse@marshall.edu

2.4.1.3. From where, typically, do the notifications come?

2.4.1.4. Legal Counsel, Campus Police, or other Law Enforcement Agencies

2.4.1.5. Internal/External Audit groups

2.4.1.6. Human Resources

2.4.1.7. External Complaints

2.4.1.8. Internal Complaints or observations

2.4.1.9. An initial determination of Severity is made (see Appendix B). If a Severity Level 1 or 2 is suspected immediately notify the Executive Response Team.

2.4.2. Step 2 – The IT Response Team designate meets with the department to discuss and begin the investigation and documentation of the incident.

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

2.4.2.1.1. What happened?

2.4.2.1.2. What systems, devices, etc., were compromised?

2.4.2.1.3. What is the net damage and costs?

2.4.2.1.4. Was information lost or stolen? If yes, what?

2.4.2.1.5. Was the information sensitive or PI?

2.4.2.1.6. How was the information acquired?

2.4.2.1.7. How was the system or device configured?

2.4.2.1.8. What are the maintenance procedures?

2.4.2.1.9. Do log files exist?

2.4.2.1.10. Who was affected by the breach?

2.4.2.2. The investigation proceeds as rapidly as possible to a highly probable conclusion of Severity Level. A preliminary report and Severity Level determination is provided to the Information Security Officer and the Chief Information Officer within 48 hours.

2.4.2.2.1. If a Severity Level 3 then notify the Executive Response Team and handle issue under standard operating procedures

2.4.2.2.2. If a Severity Level 1 or 2 then notify the Executive Response Team, seek advice and consent, and continue investigation to conclusion.

2.4.2.3. In addition to detailed documentation it is important to preserve evidence. The preservation of evidence is important if you intend to:

2.4.2.3.1. Continue to analyze the problem after the initial intervention, and cleanup process has ended.

2.4.2.3.2. File criminal charges.

2.4.2.3.3. Involve law enforcement.

2.4.2.3.4. We will be developing standard methods to preserve evidence with time limitations.

2.4.3. Continue Investigation to a decision step or conclusion. Decision steps include:

2.4.3.1. A new Severity level can be assigned with confidence

2.4.3.2. Is external information or expertise needed?

2.4.3.3. Is Sensitive Information involved or possibly exposed?

2.4.3.4. Is this a probable criminal act?

2.4.3.5. Are there victims of this incident, i.e., possible or probable harm, embarrassment, exposure of sensitive information, identity theft, or other forms of possible liability

2.4.3.6. At a decision point seek advice and consent from the Executive Response Team and continue investigation

2.4.3.7. 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.

2.4.3.8. If necessary, and with approval from the Executive Response Team the IT Response Team involves appropriate Law Enforcement.

2.4.4. Step 4 – Conclusion - IT Response Team submits final report and Severity Level to Information Security Officer and the Asst. VP of Information Technology and then to the Executive Response Team

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

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

2.4.4.3. Severity Level 2 Response Plan: Internal Remediation and Communication Procedures:

2.4.4.3.1. 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.

2.4.4.3.2. Notify general counsel, the President's office, and the director of WV Office of Security of the incident.

2.4.4.3.3. Inform the department's management team that the incident is reportable.

2.4.4.3.4. If necessary, contact the appropriate law enforcement agencies to file a report.

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

2.4.4.4. Severity Level 1 Response Plan: External Remediation and Communication Procedures:

2.4.4.4.1. 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.

2.4.4.4.2. Notify general counsel, the President's office, and the director of WV Office of Security of the incident.

2.4.4.4.3. Inform the department's management team that the incident is reportable.

2.4.4.4.4. If necessary, contact the appropriate law enforcement agencies to file a report.

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

2.4.4.5. Contents **of the Notification Letter.** The notification letter contains the following pieces of information:

2.4.4.5.1. Description of the breach.

2.4.4.5.2. Contact information for the major credit reporting agencies:

- Trans Union
- Experian
- Equifax

2.4.4.5.3. Recommendations:

- Place a fraud alert on the credit report
- Monitor credit reports
- Seek additional information as needed from a University contact

2.4.4.6. **Distributing the notice of a breach** Notifications are sent to individuals in one of two ways:

2.4.4.6.1. If 50,000 or fewer individuals: Send a letter to each individual on University letterhead via first class mail.

2.4.4.6.2. 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; and Notify statewide media including television, radio and print media

2.4.4.7. **Training Staff to Respond to Inquiries.** University Staff will be trained to answer several basic questions:

2.4.4.7.1. What happened?

2.4.4.7.2. Who attacked us?

2.4.4.7.3. When did it happen?

2.4.4.7.4. How did they breach our security?

2.4.4.7.5. How widespread is the breach?

2.4.4.7.6. What steps are you taking to determine what happened?

2.4.4.7.7. What steps are we taking to prevent this from happening again?

2.4.4.7.8. What is the estimated monetary cost of this incident?

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

2.4.4.8.1. Do not offer unsolicited information or comments to inquirers.

2.4.4.8.2. Advise the inquirer that the incident is under investigation (if this is the case).

2.4.4.8.3. Direct the inquirer to a web site, www.marshall.edu/InfoSec Include Best Practices, Tips, Form, etc.

2.4.4.8.4. Direct inquiries from law enforcement to the University Police department.

2.4.4.8.5. Direct inquiries from the media to the Director of Public Affairs.

2.4.4.8.6. Direct inquiries from vendors to the Information Security Office.

2.4.5. Step 5: Post-Mortem review and plan implementation

At the end of the investigation and concurrent with the notification and training step an analysis of the incident will be performed by a group selected by the Executive Response Team. Considerations of the group should include:

2.4.5.1. Possible Litigation and Liability.

2.4.5.2. Prosecution

2.4.5.3. Negotiation

2.4.5.4. Additional Notification

2.4.5.5. Process Improvements

2.4.5.6. Financial Impacts

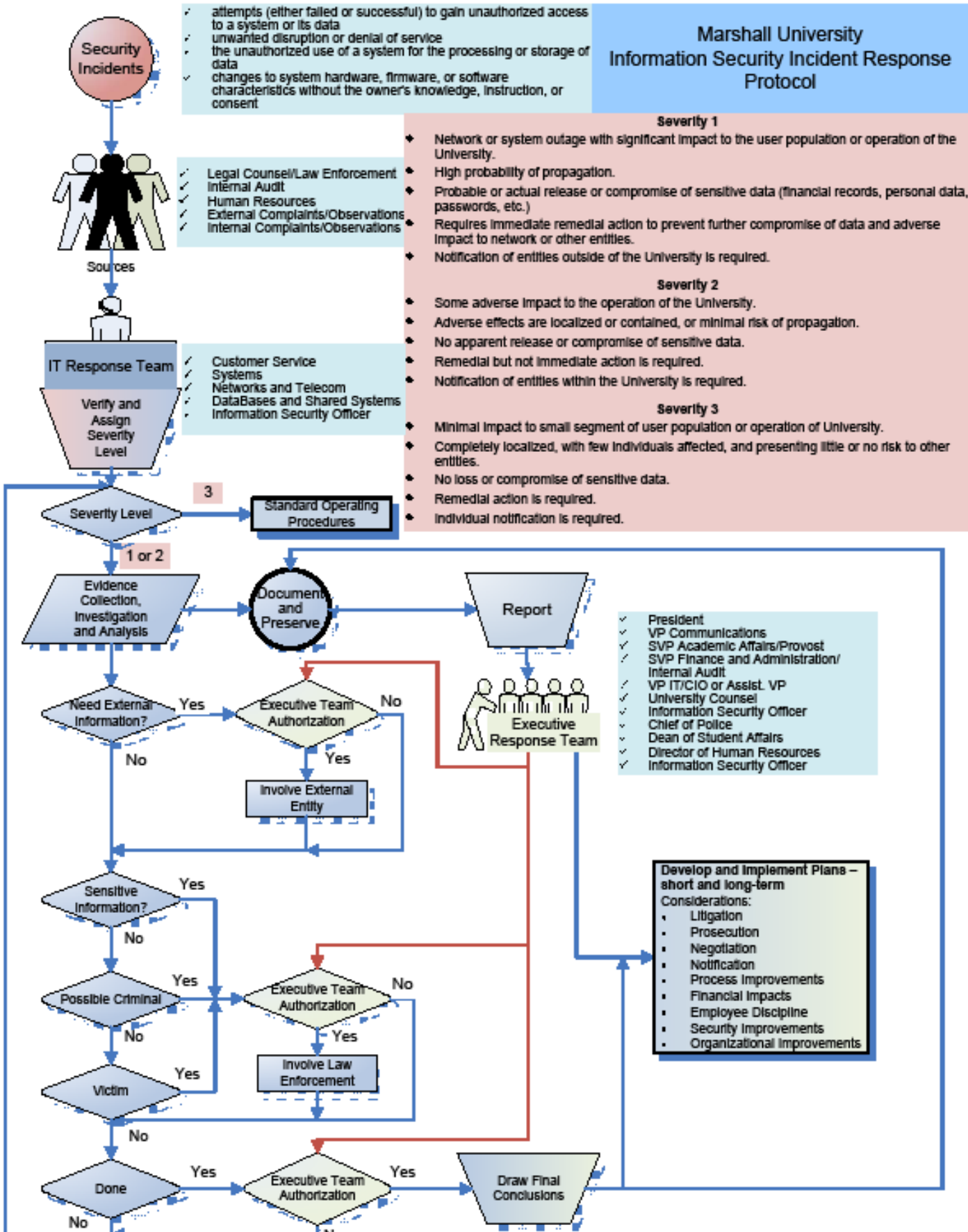
2.4.5.7. Employee Discipline

2.4.5.8. Security Improvements

2.4.5.9. Organizational Improvements

Recommendations should be forwarded to the Executive Response Team for consideration of action.

Appendix A Process Diagram



Appendix B Incident Severity

Severity	Symptoms
1	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	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	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.