

Marshall University Information Security Incident Response Protocol

- ✓ 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

Severity 1

- Network or system outage with significant impact to the user population or operation of the University.
- High probability of propagation.
- Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.)
- Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities.
- Notification of entities outside of the University is required.

Severity 2

- Some adverse impact to the operation of the University.
- Adverse effects are localized or contained, or minimal risk of propagation.
- No apparent release or compromise of sensitive data.
- Remedial but not immediate action is required.
- Notification of entities within the University is required.

Severity 3

- Minimal impact to small segment of user population or operation of University.
- Completely localized, with few individuals affected, and presenting little or no risk to other entities.
- No loss or compromise of sensitive data.
- Remedial action is required.
- Individual notification is required.

- ✓ Legal Counsel/Law Enforcement
- ✓ Internal Audit
- ✓ Human Resources
- ✓ External Complaints/Observations
- ✓ Internal Complaints/Observations

- ✓ Customer Service
- ✓ Systems
- ✓ Networks and Telecom
- ✓ DataBases and Shared Systems
- ✓ Chief Security Officer

- ✓ Legal Counsel
- ✓ Information Security Officer
- ✓ MUPD
- ✓ Internal Audit
- ✓ CIO or Assist. VP
- ✓ Student Affairs
- ✓ Human Resources
- ✓ Academic Affairs

Develop and Implement Plans – short and long-term

- Considerations:
- Litigation
 - Prosecution
 - Negotiation
 - Notification
 - Process Improvements
 - Financial impacts
 - Employee Impacts
 - Security Improvements
 - Organizational Improvements

