ITS Policy 2.3
Information Security Event Response Policy

Category: Information Security
Title: Information Security Event Response Policy
Responsible Unit: Information Technology Services
Effective: April 25, 2016
Revision History: None
Review Date: April 2019

INFORMATION TECHNOLOGY SERVICES POLICY 2.3
INFORMATION SECURITY EVENT RESPONSE POLICY

1. PURPOSE & SCOPE:

1.1 ***Purpose***. West Virginia University (WVU) has purchased information systems and IT assets that support academic, administrative and research operations. WVU is committed to maintaining the availability and security of these resources. This policy establishes the responsibilities that all WVU academic, administrative and research organizations must follow when an information security event adversely affects one, or more, information system or IT asset.

1.2 ***Scope***. This policy applies to all University staff, faculty, and students as well as any third-parties who are doing work on behalf of the University who use information systems and IT assets purchased on behalf of WVU.

2. POLICY:

2.1 WVU's Chief Information Security and Privacy Officer is responsible for managing the response to all information security events involving WVU-purchased information systems and IT assets. Examples of an information security event could be, but may not be limited to, the following:

2.1.1 An outside entity makes an information system unusable by limiting access to the system or introducing malicious code to the system.

2.1.2 An outside entity breaches an information system and discloses or compromises stored data.

2.1.3 An employee or affiliate of a WVU organization opens an email attachment which activates malicious code that renders an IT asset or information system unusuable.

2.1.4 An employee or affiliate of a WVU organization clicks on a link in an email that leads to the inadvertent disclosure of the employee's or affiliate's personally identifiable information to an unauthorized entity.

2.1.5 An employee or affiliate of a WVU organization improperly stores personally identifiable information of WVU employees or students in an unsecure location, which leads to the disclosure of this information to an unauthorized entity.

2.2 If a WVU organization, its employee(s) or affiliate(s) suspect an information security event has occurred, the first step is to contact Information Security Services by email at defendyourdata@mail.wvu.edu or phone at 304-293-4457/304-293-4444.

2.3 Unless instructed by Information Security Services, the WVU organization, its employee(s) or affiliate(s) who reported the information security event **should not** do anything to the affected WVU information system or IT asset.

2.4 Upon validation of the incident, WVU's Chief Information Security and Privacy Officer may take the following actions:

2.4.1 Notify WVU senior management.

2.4.2 Form the incident response team which will include, but not be limited to, representatives from management, regulatory and technology units.

2.4.3 Initiate and coordinate communications, and when applicable, send notices to individuals who may be impacted by the incident.

2.4.4 Isolate the affected information system or IT asset.

2.4.5 Determine the scope of the incident.

2.4.6 Develop and implement a remediation plan.

2.4.7 Assist with implementing the remediation plan and monitoring remediation progress.

2.4.8 Work with the information system or IT asset owner to identify options in the event remediation is unsuccessful.

2.4.9 Provide a post-incident report.

---

3. DEFINITIONS:

3.1 **Information security event:** Any real or suspected event that may adversely affect the availability and security of WVU's information systems or IT assets that support academic, administrative or research operations.

3.2 **Information system:** The hardware, software and related technology that support academic, administrative and research operations.

3.3 **IT asset:** A server, computer, laptop, tablet or mobile device used to enter or access information from a WVU information system.

3.4 **Personally identifiable information (PII):** A WVU employee's or student's Social Security number, credit card number(s) or electronic health information.

3.5 **WVU-purchased:** A purchase of an on-site or vendor-hosted information system or IT asset made on behalf of WVU, regardless of the funding source.

3.6 **WVU third-party:** An individual or an entity that has an affiliation with WVU (e.g., retirees, consultants, presenters, camp attendees, vendors).

---

4. ENFORCEMENT:

4.1 WVU's Chief Information Officer, supported by the Chief Information Security and Privacy Officer, will coordinate with appropriate University entities on the implementation of this policy.

4.2 Violation or non-compliance with this policy will be addressed in accordance with established WVU disciplinary policies, procedures and enforcement authorities. Failure to comply with this or other related standards may result in disciplinary action up to and including termination of employment or studies.

4.3 In the event that an information security event is determined to have been the result of a malicious act the appropriate WVU legal entities will be contacted to determine subsequent actions.

---

5. CROSS REFERENCES:

5.1 All other University policies are also applicable to the electronic environment. Relevant institutional policies include, but are not limited to:

5.1.1 ITS Policy 1.0 – Acceptable Use of Technology Data and Resources

5.1.2 ITS Policy 1.1 – Email Policy

5.1.3 ITS Policy 2.0 – Information Security

5.1.4 National Institute of Standards and Technology