Policy 5.17  
Enterprise Information Security Incident Response Policy

This policy version was not current at the time of printing. Please see http://policies.emory.edu/5.17 for the current version.

Responsible Official:  Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship
Administering Division/Department:  LITS: Library & IT Services
Effective Date:  April 28, 2015
Last Revision:  May 15, 2015

Policy Sections:

I. Overview
II. Applicability
III. Policy Details
IV. Definitions
V. Related Links
VI. Revision History

Overview

All information security incidents pose a risk to the Emory enterprise. The impact of these risks vary, but can lead to monetary loses, reputational impacts, identity theft, intellectual property theft, or misuse of resources to name a few. Some incidents pose minimal risks to the institution while others pose significant risks. A clearly defined incident response plan helps organizations react effectively and quickly when investigating an information security incident.

The primary goal of this policy is to establish the channels of communication, define response activities, and define roles and responsibilities during an incident as well as to ensure that regulatory and legal reporting requirements are met.

Applicability

This policy applies to all incident response activities conducted by Emory University and Emory Healthcare, referred to simply as “Emory” in the remainder of this document.

Roles and Responsibilities

LITS Enterprise Security  -  LITS-ES is responsible for developing and maintaining the enterprise incident response policy, as well as leading and coordinating all major incident response activities across Emory. LITS-ES will also act as a first point of contact for security incident reporting.

Emory Security Incident Response Team (ESIRT)  -  The ESIRT consists of representatives from a variety of constituencies across the enterprise, including but not limited to: Office of the General Counsel, Internal Audit, Human Resources, Communications & Marketing, Emory Finance, LITS Enterprise Security, Emory Healthcare IS, Emory Police, Development and Alumni Relations, and representatives from distributed IT organizations within the different academic schools and other major business units. The primary purpose of the ESIRT is to facilitate communications and act as central touch point for LITS-ES during major incidents. Representatives on the ESIRT are expected to provide expertise and input from their areas of responsibility, as well as coordinate incident response activities within those areas as required.

Data Breach Notification Team (DBNT)  -  The DBNT consists of a subset of the ESIRT, to include: Chief Information Officer, Chief Information Security Officer, Office of the General Counsel, University and Healthcare Privacy Officers,
Chief Risk Officer, and Emory Healthcare CIO. The purpose of the DBNT is to review incident risk assessments and make a recommendation about whether or not data breach notification is required for a given incident. The DBNT presents its recommendations to the President’s Cabinet for final approval.

**Policy Details**

a. **General**
   
i. LITS Enterprise Security is primarily responsible for the coordination and investigation of all enterprise incident response activities.
   
   ii. Any member of the Emory community who discovers a data breach or possible data breach must report the incident to LITS Enterprise Security within 24 hours of discovery.
   
   iii. Each school or business unit is expected to comply with instructions from LITS Enterprise Security during an incident.
   
   iv. Emory Information Systems are monitored for intrusions 24/7. LITS Enterprise Security reviews the resulting alerts on a daily basis (Monday through Friday). Alerts may be generated by, but are not limited to: Firewalls, IPS/IDS, SIEM, WAF, file integrity monitoring.
   
   v. The ESIRT and DBNT will perform a walkthrough of incident response procedures on at least an annual basis.
   
   vi. As required, LITS Enterprise Security may have to take extraordinary measures to protect the enterprise during an active incident. Examples include, but are not limited to: Blocking threat actors, removing systems from the network, blocking protocols, applications, or services, requiring stricter security controls enterprise-wide, or installing software enterprise-wide.
   
   vii. After each major incident the ESIRT will review lessons learned and recommend changes to the incident response process as needed to be able to respond more effectively in the future. Additionally, technical changes may be required in order to prevent a recurrence of the same incident in the future.

b. **Incident Communication Plan**
   
i. During an incident the primary mechanism for facilitating information flow is through the ESIRT.
   
   ii. Members of the ESIRT are responsible for communicating information in a timely manner to their executive layers and IT personnel, as well as providing feedback to LITS Information Security as requested/necessary.
   
   iii. Any interactions with the Press regarding incidents will be facilitated through Emory Marketing and Communications.

c. **Standard Incident Response Process**
   
i. After a potential incident is identified, LITS Enterprise Security will begin the process of confirming that an incident has in fact taken place, and scope the incident in order to understand the scale.
   
   ii. If required, external vendors may be engaged for incident response assistance.
   
   iii. LITS Enterprise Security will coordinate and take actions necessary to contain and remove any active threats in the environment.

d. **Reportable Incidents**
   
i. Incidents that are potentially reportable will be reviewed according to a standardized risk assessment process. This process will take many factors of the incident into account, including legal incident reporting requirements.
   
   ii. The DBNT team will review all risk assessments and, based on all of the assessment factors, produce a breach reporting recommendation. The recommendation of the DBNT will undergo a final review by the University President’s Cabinet.
   
   iii. Emory will identify and retain a breach notification vendor that will be used to facilitate notifications should they be warranted.
   
   iv. The cost incurred for breach notification will be the responsibility of the department, business unit, or academic school in which the breached data originated.
e. PCI-DSS

i. In the event of a breach of cardholder data, Emory will notify the major credit card brands within 24 hours of detection.

ii. Emory will identify and retain a PFI (PCI Forensics Investigator) firm who will be engaged in the event of a breach of cardholder data.

iii. If a PFI must be engaged they will work directly with LITS Enterprise Security to respond to the incident and investigate the scope of the breach.

f. HIPAA

i. In the event of a potential data breach involving electronic Protected Health Information, Emory will conduct its incident response efforts in accordance with the procedures documented in Emory’s Potential ePHI Data Breach Notification Policy.

ii. Emory’s breach notification vendor will be engaged to facilitate setup and staffing of the required toll-free hotline.

iii. Any required media outlet notification will be facilitated through Emory Marketing and Communications.

iv. Emory will notify the Secretary of the U.S. Department of Health and Human Services (HHS) using the electronic forms located on the HHS website.

Sanctions:

Failure to comply with Emory’s Information Security Incident Response policy may result in:

- Suspension or termination of access;
- Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy;
- Civil or criminal prosecution.

Definitions

**Information Security Incident** – An information security incident can be defined as any violation, or imminent threat of violation, of computer systems or other information technology resources or data that pose a threat to the whole or part of the Emory enterprise. Examples include but are not limited to:

- Data loss, theft, or misuse
- Unauthorized changes to hardware, software, firmware, or data
- Unauthorized changes, exposure, or deletion of information assets
- Activities that violate Emory’s Information Technology Conditions of Use policy
- Degradation of services

**Reportable Incident** – An information security incident in which regulated data, or data that could lead to identity theft are compromised and require that affected individuals or organizations be notified of the incident. Examples may include data regulated by HIPAA and the HITECH act, or the Payment Card Industry Data Security Standard (PCI-DSS).

Related Links

- Current Version of This Policy: [http://policies.emory.edu/5.17](http://policies.emory.edu/5.17)
- Cardholder Data Environment Remote Access Policy: [https://policies.emory.edu/5.18](https://policies.emory.edu/5.18)
- Payment Card Information Security Policy: [https://policies.emory.edu/5.19](https://policies.emory.edu/5.19)
- PCI Risk Assessment Policy: [https://policies.emory.edu/5.20](https://policies.emory.edu/5.20)
- Payment Card Processing and Compliance Policy: [https://policies.emory.edu/2.2](https://policies.emory.edu/2.2)
- Retention and Disposal: [http://records.emory.edu/retention-schedules/index.html](http://records.emory.edu/retention-schedules/index.html)
- H.1.F.1 [https://hipaa.emory.edu/home/Policies/emory_security_policies.html](https://hipaa.emory.edu/home/Policies/emory_security_policies.html)