TEMPLE UNIVERSITY HEALTH SYSTEM
INFORMATION SERVICES AND TECHNOLOGY
POLICIES AND PROCEDURES

Number:	0314
Title:	Proactive Breach and Vulnerability Monitoring Response
Effective Date:	09-01-2014
Last Revised:	09-01-2014
Last Reviewed:	09-01-2014
References:	TUH-IS-0310, Systems Access Management Policy TUHS Corporate Compliance Program
Attachments:	N/A

PURPOSE

To maintain the security of the TUHS environment, Information Security will work with vendors, external monitoring agencies, Biomedical Engineering, Compliance, and Risk Management to craft proper mitigations to discovered issues across all of TUHS and Temple University Physicians (TUP).

POLICY

Information Security will work with the following departments and resources to receive information on information systems and computerized biomedical device vulnerabilities:

Vulnerability Type or Target	Resource
Biomedical Device or Specialized Health IT Applications (PACS, etc.)	Emergency Care Research Institute (ECRI) Databases and Alerts
Reported privacy and security breaches	Datalossdb.org mailing list, Department of Health and Human Services Office of Civil Rights (HHS OCR) Website (http://www.hhs.gov/ocr/privacy/ hipaa/administrative/breachnotificationrule/ breachtool.html), local news media.
Vulnerabilities of systems running Microsoft Windows	Microsoft Security Bulletins and Alerts, US Department of Homeland Security Computer Incident Response Team (US-CERT) Security Bulletins, the SecurityFocus BUGTRAQ vulnerability mailing list (BUGTRAQ), Infragard Alerts, Full Disclosure security mailing list
Breaches affecting 500 or more individuals (per HITECH)	HHS OCR Website (http://www.hhs.gov/ocr/privacy/ hipaa/administrative/breachnotificationrule/ breachtool.html)
Vulnerabilities of systems running Linux	BUGTRAQ, Red Hat Network, Full

	Disclosure security mailing list
Other reported software vulnerabilities	ECRI Databases, ECRI Alerts, BUGTRAQ mailing list, US-CERT Security Bulletins, US-CERT Current Activity, Infragard Alerts, Full Disclosure security mailing list
Vulnerabilities of systems running Oracle	Oracle Security Alerts mailing list, BUGTRAQ mailing list, Full Disclosure security mailing list.
Vulnerabilities of systems running other vendor software	Vendor reports, BUGTRAQ mailing list, US-CERT Security Bulletins, US-CERT Current Activity, Infragard Alerts, Full Disclosure security mailing list
Temple University Network	Temple University Network Services, Temple University Associate Director, Information Security Temple University Assistant Vice President for Infrastructure, Operations, and Security

Information Security is responsible for:

- When a security breach or vulnerability is identified at TUHS, Information Security will:
    - Notify affected staff, including:
        - Director, Corporate Applications, TUHS
        - Director, Biomedical Engineering, TUH
        - IS&T Application Managers
        - Director, Network Services, Temple University
        - Director, Information Security, Temple University
        - Biomedical Engineering, Jeanes/FCCC Campus
        - Director, Risk Management, TUH
        - Director, Risk Management, Jeanes/FCCC Campus
        - Director, IS&T Technical Services
        - Director, IS&T Customer Support
        - Corporate Compliance and Privacy Officer, TUHS
        - Customers
    - Develop mitigation plans with the appropriate staff to reduce or eliminate the impact of the vulnerabilities for affected applications.
    - Execute mitigation plans with the involved parties.
    - Verify the mitigation of the issue.
    - Communicate risks to the Corporate Compliance and Privacy Officer that cannot be mitigated in accordance with agreed-upon IT policies and procedures.

<u>Compliance to Related Standards and Regulations</u>

- Paragraph 164.308(a)(2) of the HIPAA Security Rule requires organizations to identify a security official responsible for the development and implementation of the policies and procedures required by this subpart for the entity. The CISO of TUHS fulfills the role of the responsible security official.

- Paragraph 164.308(a)(6)(i) of the HIPAA Security Rule requires organizations to implement policies and procedures to address security incidents.

- Paragraph 164.308(a)(6)(ii) of the HIPAA Security Rule requires organizations to identify and respond to suspected or known security incidents, mitigate, to the extent practicable, the harmful effects of security incidents, and document the incidents and their outcomes.

POLICY APPROVAL PAGE

Recommended by:

Mitchell Parker, CISSP
Chief Information Security Officer, TUHS
Date:

Maribel Valentin
Corporate Compliance and Privacy Officer, TUHS
Date:

APPROVED BY:

David Kamowski
VP / Chief Information Officer, TUHS
Date:

NOTE:

Refer to the on-line version of this policy for the most current information. Printed copies of this policy may not be current.

Use of this document is limited to Temple University Health System staff only. It is not to be copies or distributed outside of the institution without Administrative permission.