T.H. Chan School of Public Health Information Security Incident Response Policy

I. Purpose

This policy governs the actions required of the T.H. Chan School of Public Health (SPH) personnel reporting or responding to security incidents involving SPH information and/or information technology resources to insure effective and consistent reporting and handling of such events.

II. Scope

This policy applies to all SPH personnel, departments, and affiliates using SPH IT resources or data.

III. Policy

All members of the SPH community are responsible for reporting known or suspected information or information technology security incidents and complying with Harvard's Information Security Policy.

All security incidents at SPH must be promptly reported to SPH's IT Helpdesk by phone and/or email and handled appropriately based on the type and severity of the incident in accordance with SPH security incident policies.

All individuals involved in reporting or investigating a security incident are obliged to maintain confidentiality.

Handling of security incidents involving confidential data will be overseen by the Incident Response Team and may have additional legal, policy, and/or contractual requirements for handling the incident and notifying affected parties. (i.e. HISP, HRDSP, PCI, SLA, DUA, GDPR, stat laws, etc.)

IV. Definitions

A security incident is any real or suspected event that may adversely affect the security of SPH information or the systems that process, store, or transmit that information.

Examples include:

- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet

• Reconnaissance activities such as scanning the network for security vulnerabilities Denial of Service attack

• Web site defacement

• Violation of a SPH security policy

• Security weakness such as an un-patched vulnerability

• Suspicious behavior

• Unusual incidents in audit logs

• User or anonymous reports of problems

• Unauthorized security configuration changes

• Unusual traffic or activity

• Lapsed physical security

• Sensitive information in the wrong place or hands

• User complaint which triggers an investigation.

HISP – Harvard Information Security Policy

HRDSP – Harvard Research Data Security Ploicy

PCI – Payment Card Industry

SLA – Service Level Agreement

GDPR – General Data Protection Regulation

DUA – Data Use Agreement

HRCI – High Risk Confidential Information

CI - Confidential Information

DSL – Data Security Level

VI. Incident Response Team (IRT)

The Incident Response Team a team of technical representatives assembled to investigate a security incident.

A. IRT has the following priorities in investigating the incident:

- First priority is preventing any further damage if the breach is ongoing.
- Second priority is closing any vulnerabilities exploited
- Third priority is investigating what caused the problem and what data was compromised during the breach.

➢ *B. Incident Response Team Responsibilities*

1) SPH CIO is the team leader. All incidents or potential incidents are reported to the team leader. He determines if an incident has taken place and if it involves PCI or HRCI. If PCI then reference the PCI Security Breach Business Process document. If HRCI or CI reference the HISP. If the incident is a lost or stolen laptop reference the procedures in the HISP: http://security.harvard.edu/files/it-security-new/files/reporting_a_lost_laptop_advisory.pdf. Any technical forensic investigations of systems are conducted primarily by HUIT Security/School IT representatives. Ensure that the system compromised has been removed from the network until its vulnerability has been corrected.
2) If possible, make a backup copy of the disk of the breached machine then preserve the original disk for forensics and evidence - switch the system to run on the copy
3) Write down all actions taken while working on compromised machines.
4) Preserve all logs and electronic evidence.
5) Through reviewing system and network logs, configuration of the compromised system, application audit trails, and other evidence determine the cause and extent of the compromise.
6) Identify potential remedies.
7) If needed, work with any law enforcement agencies involved in the breach. Support their investigations under the direction of the Office of the General Counsel.
8) Have all compromised systems scanned for vulnerabilities prior to allowing them to be placed back into production. Perform other tests or probes of the system as appropriate.
9) If the investigation reveals that other systems are at risk, notify the individuals or the university community as appropriate of the potential risk and suggested steps to take to minimize it.

See Appendix for IRT contacts and escalation.

VI. Reporting Security Incidents

Any member of the SPH community who suspects the occurrence of a security incident must report incidents through the following channels:

- All suspected high severity events as defined in the incident classification system, including those involving possible breaches of personal identity data, should be reported directly to the Information Security Manager as quickly as possible by phone, e-mail, or in person.

All other suspected incidents must also be reported to the Information Security Manager or by sending e-mail to helpdesk@hsph.harvard.edu. These incidents may be first reported to departmental IT support personnel who can then contact the Information Security Manager.

VII. Incident Classification System

Security incidents will be classified according to incident categories and severity of incident. Incident response will be based on classification.

A. Incident Categories

The following categories will be used to describe IT security incidents at SPH. A single incident may have several different categories. The examples listed in each category are not meant to be definitive.

a. Confidential data exposure (reference: HISP)

- Social Security Numbers with or without names
- Credit Card information
- Identity theft
- Other

b. Criminal activity/investigation (*Please note: under University policy, law enforcement requests/personnel must contact Office of the General Counsel to determine how to respond)

- Subpoena, search warrant, or other court order
- Litigation hold request (ala e-Discovery)
- Online theft, fraud
- Threatening communication
- Child pornography
- Physical theft, break-in

c. Denial of Service

- Single or distributed (DoS or DDoS)
- Inbound or outbound

d. Digital Millennium Copyright Act (DMCA) violation

- Official DMCA notification received from the Harvard DMCA Agent.
- Illegal distribution of copyrighted or licensed material (movies, music, software, games)
- Illegal possession of copyrighted or licensed material

e. Malicious code activity (IT Staff will try and determine method of 'infection' and will also investigate if PC with user's credentials have more than standard access, i.e. access to another system , application or server)

- Worm, virus, Trojan
- Botnet
- Keylogger
- Rootkit

f. Policy violation

- SPH policy violation
- Violation of student code of conduct

- Personnel action/investigation

g. Reconnaissance activity

- Port scanning
- Other vulnerability scanning
- Unauthorized monitoring

h. Rogue server or service

- Rogue file/FTP server for music, movies, pirated software, etc.
- Phishing scam web server
- Botnet controller

i. Spam source

- Spam relay
- Spam host
- SPH computer on a block list

j. Spear Phishing

- Scam e-mail targeting a relatively large number of K-State e-mail addresses

k. Unauthorized access

- Abuse of access privileges
- Unauthorized access to data
- Unauthorized login attempts
- Brute force password cracking attempts
- Stolen password(s)

l. Un-patched vulnerability

- Vulnerable operating system
- Vulnerable application
- Vulnerable web site/service

- Weak or no password on an account

m. Web defacement

- Defacement of web site
- Inappropriate post to wiki, blog, etc
- Redirected web site

n. No Incident

- When investigation of suspicious activity finds no evidence of a security incident

B. Incident Severity

The severity of incident is a subjective measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

- Scope of impact – how many people, departments, or systems does it affect?
- Criticality of the system or service – how important is it to the continuing operation of the institution? What would be the impact on the business, either functional or financial, if this system or service were unavailable or corrupted?
- Sensitivity of the information stored on or accessed through the system or service – does it contain confidential data, such as personal identity information or credit card information?
- Probability of propagation – how likely is it that the malware or negative impact will spread or propagate to other systems, especially to other systems off campus?

Security incidents will be classified by four categories of incident severity – high, medium, low, and NA (“Not Applicable”).

a) High

The severity of a security incident will be considered “high” if any of the following conditions exist:

• Significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)

• Threatens confidential data (for example, the compromise of a server that contains HRCI or DSL 3 or 4))

• Adversely impacts an enterprise system or service critical to the operation of a major portion of the school or university (for example, e-mail, student information system, financial information system, human resources information system, learning management system, Internet service, and a major portion of the campus network)

• Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.

• Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

High severity incidents require an immediate response and focused dedicated attention by the CISO and other appropriate University officials and IT security staff until re-mediated. These incidents also have extensive notification and reporting requirements. A Post-Incident Report is required. If the incident involves the possible exposure of personal identity data, it may require notification of individuals according to state or government laws and/or DUA. Notifications to be determined by Harvard’s Office of General Counsel.

b) Medium

The severity of a security incident will be considered “medium” if any of the following conditions exist:

• Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building

• Adversely impacts a non-critical enterprise system or service

• Adversely impacts a departmental system or service, such as a departmental file server

• Disrupts a building or departmental network

• Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruptions

Medium severity incidents require a quick response by appropriate personnel, usually from the affected unit, who have primary responsibility for handling the incident. Notification requirements are outlined in the table below. A Post-Incident Report is not required unless requested by the CIO.

c) Low

Low severity incidents have the following characteristics:

• Adversely impacts a very small number of systems or individuals

• Disrupts a very small number of network devices or segments

• Has little or no risk of propagation, or cause minimal disruption or damage in their attempt to propagate

Since a single compromised system can “wake up” and negatively affect other systems at any time, appropriate personal (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day. Notification requirements are outlined in the table below. A Post-Incident Report is not required unless requested by the CIO.

d) NA (“Not Applicable”)

This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found. This usually corresponds to the incident category, “No Incident.”

Appendix:

IRT Contacts/Escalation

IRT Leader: **Deane Eastwood**

Title: Chief Information Officer

Office Phone: 617-998-6901

Cell Phone: 617-201-4209

Email: deastwoo@hsph.harvard.edu

IRT Asst Leader: **Matthew Ronn**

Title: Director of Infrastructure Services

Office Phone: 617-998-6901

Cell Phone: 617-780-9060

Email: mronn@sdac.haravrd.edu

IRT Coordinator: **Andrew Ross**

Title: Info Security Manager

Office Phone: 988-6912

Cell Phone: 617-201-4310

Email: aross@hsph.harvrard.edu

Primary Network contact: **HUIT Network Services**

Business Hours Phone: 617-495-3574

After Hours Phone: 844-484-8662

Email: netmanager@harvard.edu

Primary Server contact: **Brian Pedranti**

Title: Server Manager

Office Phone: 998-6909

Cell Phone: 617-201-4308

Email: bpedrant@hsph.harvard.edu

Secondary Server contact: **Nathan Varney**

Title: Systems Administrator ll

Office Phone: 998-6911

Cell Phone: 617-646-9200

Email: nvarney@hsph.harvard.edu

Primary Web Contact: **TBD**

Title: Manager, Web Development

Office Phone:

Cell Phone:

Email:

References:

Harvard's Enterprise Information Security Policy - http://www.security.harvard.edu/

DMCA Compliance Policy for Staff - http://www.dmca.harvard.edu/compliance.php

Harvard University Personnel Manual - http://harvie.harvard.edu/Policies_Contracts/Staff_Personnel_Manual/

Harvard Research Data Security Policy - https://vpr.harvard.edu/pages/harvard-research-data-security-policy

Harvard’s PCI Data Security Breach Process - http://hwpi.harvard.edu/files/otm/files/pci_security_breach_process_.pdf