INFORMATION SECURITY
INCIDENT MANAGEMENT PROCESS

BRANDEIS UNIVERSITY

The Heller School FOR SOCIAL POLICY AND MANAGEMENT

Effective Date June 9, 2014

INFORMATION SECURITY INCIDENT MANAGEMENT PROCESS OF THE HELLER SCHOOL FOR SOCIAL POLICY AND MANAGEMENT

Table of Contents

1. Executive Summary

The purpose of this document is to establish the Heller School's Information Security Incident Management Process. The goal is to report, respond, and resolve incidents, as well as to comply with the Heller School's Information Security Policy. This process applies to all Operations of the Heller School and any applicable External Parties.

The scope of this process provides a structured and planned approach to:

- detect, report and assess information security incidents;
- respond to and manage information security incidents;
- resolve the information security event or issue in a timely manner

When information security events are detected, they must be categorized and classified as 'minor' or 'major'. **Quickly reporting an information security incident will allow the timely resolution of a security event**. In the case of a 'major' security incident, the Heller Information Security Committee will be notified, along with the Data Custodian, the Heller Dean, and the University IRB.

Information security incidents may be deliberate or accidental (e.g. caused by error or acts of nature), and may be caused by technical or physical means. Their consequences may include the disclosure, modification, destruction, or unavailability of information in an unauthorized manner, or the damage or theft of organizational assets. See Appendix II for examples of some information security incidents.

Effective information security incident management requires an informed Heller community. Toward this end, Heller faculty, staff and students will be trained so that individuals are able to recognize an incident, and know what to do in case of an incident. Furthermore, there will be briefings and updates in the Heller bulletin. Awareness training sessions will be incorporated into the general information security training and will be repeated annually.

The information security incident management reporting log tracks the record of incidents both electronically as well as in paper-based format. The objective is to maintain a running record of the incident assessments as well as to support information sharing.

2. Detecting and Reporting Incidents

The first phase of an information security incident management process involves the detection of, collecting information associated with, and reporting on occurrences of information security events.

The information reported during each activity must be as complete as possible at the time, to ensure that there is a good base available for the assessments and decisions to be made, and of course the actions taken.

DETERMINE IF IT IS A 'MINOR' OR 'MAJOR' INCIDENT. SEE APPENDIX II –Examples of Information Security Incidents

A **Major** incident is one that involves Level 3 data as defined in the Information Security Policy. Level 3 data are strictly confidential and are of the highest level of sensitivity. FERPA, PII, PHI, PCI, and HIPAA-identified data are in this category. Some examples might include: Machine hacked, serious virus, stolen equipment.

A **Minor** incident is defined as all other incidents. These are less serious, but still reportable events. Some examples might include: Lost encrypted data, lost password.

Information on vulnerabilities and their resolutions must be entered into the information security event/incident/vulnerability log.

Fill out form 6 and inform the Points of Contact (POC) David Reynolds (reynolds@brandeis.edu) and Jennifer Perloff (perloff@brandeis.edu). They will notify Debbie DeWolfe, the administrative point of contact, who maintains the electronic and paper-based incident management reporting logs.

The POC will determine whether the incident should be classified as 'minor' or 'major'. In the case of a 'major' security incident, the POC will notify Ron Etlinger, Heller COO, along with the Data Custodian on the DUA (if applicable), the Heller Dean, and, if necessary, the Waltham police.

At this time, it will be determined if other stakeholders need to be made aware of the security incident. These could include both internal stakeholders (LTS, management staff etc.), and external stakeholders (funders, partners, etc.).

If it is a 'minor' security incident, the POC will evaluate the incident and determine an appropriate response.

3. Assessing and Responding to Information Security Incidents

After an information security event is detected, reported, and the relevant information is collected, the response begins.

Assessment and decision phase

1. Determine whether the event is an actual information security incident or a false alarm. If it is not a false alarm, assess whether incident is to be classified as ‘minor’ or ‘major’.

2. The POC also to identify the impact to individual assets, research, and applications, and the possible effects on Heller.

3. This is followed by decisions on how the confirmed information security incident must be dealt with, by whom, and in what priority.

Responding

1. Define all internal and external functions and organizations that must be involved during the management of an incident.

2. Conduct information security forensics analysis, as required.

3. Ensure that all involved activities are properly logged for later analysis, and that the information security incident management log is kept up-to-date.

4. Communicating and sharing the results of review within the Heller community to avoid similar problem in the future.

5. Communicate the information security incident and relevant details to other internal and external shareholders.

6. Identifying the lessons learned from the information security incident and vulnerabilities. This information should be used to make improvements to the organization’s existing infrastructure, processes and procedures.

Once the incident has been successfully dealt with, formally close it and recorded this in the information security incident management log.

4. Resolving Incidents and Managing to a Conclusion

The POC has the responsibility for ensuring that incidents are resolved.

When information security events are first reported, the POC deals with them in the detection and reporting phase. The POC must review the information gathered and make the initial assessment as to whether events should be classified as incidents or not. The POC will then respond. The responses could be made immediately, in real-time or in near real-time, and some could well involve information security forensics analysis.

For the Responses phase, the POC must ensure that the key activities are followed:

- Review by the ISIRT to determine if the information security incident is under control, and
- Investigate the required response, if it is under control. This could be an immediate response, which could include the activation of recovery procedures, and/or issuing communications to relevant involved personnel, or a later slower time response (for example, in facilitating full recovery from a disaster), While ensuring all information is ready for post-incident review activities.
- Figure out how to fix the problem. Get help from LTS or from outside consultant if necessary.
- Documentation of an information security incident, of the subsequent actions, and updating of the information security event/incident/vulnerability database.

Once any information security incident has been dealt with successfully, it must be formally closed and this recorded in the information security incident management log.

Escalation

In extreme circumstances, matters may have to be escalated to accommodate incidents that are out of control and a potential for serious impact. In this case, the POC will confer with the Heller School COO to decide on recommended actions to deal with the information security incident.

Activity logging and change control

Activity logging is performed for all aspects of an incident, from detection to resolution, as a key for communication, accountability to ourselves and our partners, and the improvement of the system and process for everyone. The critical components of any response is in communicating the suspected or known incident as quickly as possible so decisions and responses can be made in a timely fashion.

The log contains not only the date and time of the event as well as who it was reported by, but the results of the root cause and any security forensic analysis that is pertinent.

5. Appendices

APPENDIX I - Definitions

The following are terms and definitions necessary for understanding this process.

- **Access** – To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of information resources.
- **Information security forensics** - Application of investigation and analysis techniques to capture, record, and analyze information security incidents.
- **Information Security Incident Response Team (ISIRT)** - Team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle.
- **Information security event** - Identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant.
- **Information security incident** - Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- **Point of Contacts (POC)** - The POC are the leaders of the Information Security Incident Management Process. As of this date, they are David Reynolds and Jennifer Perloff, and they are the point-of-contact for reporting incidents, coordinating resources throughout the organization, coordinating resources outside the organization, and any other activities and/or decision processes involved throughout the life cycle of the incident management process.

APPENDIX II –Examples of Information Security Incidents

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are a broad category of incidents with a common thread. Such incidents cause a system, service or network to fail to continue operating in its intended capacity, most often with complete denial of access to legitimate users. There are two main types of DoS/DDoS incidents caused by technical means: resource elimination and resource starvation. Some typical examples of deliberate technical DoS/DDoS incidents include:

- Pinging network broadcast addresses in order to fill up network bandwidth with response traffic,
- Sending data in an unexpected format to a system, service or network in an attempt to crash it, or disrupt its normal operation,
- Opening up multiple authorized sessions with a particular system, service or network in an attempt to exhaust its resources (i.e., to slow it down, lock it up or crash it).

Such attacks are often performed through Botnets, a collection of software robots (malicious code) that run autonomously and automatically. Botnets can relate to some hundreds to millions of affected computers.

Some technical DoS incidents may be caused accidentally, for example caused by operator misconfiguration or through incompatibility of application software, but most of the time they are deliberate. Some technical DoS incidents are intentionally launched in order to crash a system or service, or take down a network, while others are merely the by-products of other malicious activity. For instance, some of the more common stealth scanning and identification techniques can cause older or misconfigured systems or services to crash when scanned. It should be noted that many deliberate technical DoS incidents are often executed anonymously (i.e. the source of the attack is 'faked'), since they typically do not rely on the attacker receiving any information back from the network or system being attacked.

DoS incidents caused by non-technical means, resulting in loss of information, service and/or facilities, could be caused, for example, by:

- breaches of physical security arrangements resulting in theft or willful damage and destruction of equipment,
- accidental damage to hardware (and/or its location) by fire or water damage/flood, extreme environmental conditions, for example high operating temperatures (e.g. due to air conditioning failure),
- system malfunctions or overload,
- uncontrolled system changes,
- malfunctions of software or hardware.

Unauthorized access- In general this category of incidents consists of actual unauthorized attempts to access or misuse a system, service or network. Some examples of technically stimulated unauthorized access incidents include:

- attempts to retrieve password files,
- buffer overflow attacks to attempt to gain privileged (e.g., system administrator) access to a target,
- exploitation of protocol vulnerabilities to hijack or misdirect legitimate network connections,
- attempts to elevate privileges to resources or information beyond what a user or administrator already legitimately possess.

Unauthorized access incidents caused by non-technical means, resulting in direct or indirect disclosure or modification of information, breaches of accountability or misuse of information systems, could be caused, for example, by:

- breaches of physical security arrangements resulting in unauthorized access to information,
- poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware.

Malicious code- identifies a program or part of a program inserted into another program with the intent to modify its original behavior, usually to perform malicious activities as information and identify theft, information and resource destruction, Denial of Service, Spam, etc. Malicious code attacks could be divided into five categories: viruses, worms, Trojan horses, mobile code and blended.

While a few years ago viruses were created to target any vulnerable infected system, today malicious codes are used to perform targeted attacks. This is sometimes performed modifying an existing malicious code, creating a variant that often is not recognized by malicious code detection technologies.

Inappropriate usage- This kind of incident occurs when a user violates the Organization's information security policies. Such incidents are not attacks in the strict sense of the word, but are often reported as incidents and should be managed by an ISIRT. Inappropriate usage could be:

- downloading and installing hacking tools,
- using University e-mail for spam or promotion of personal business,
- using University resources to set up an unauthorized web site,
- using peer-to peer activities to acquire or distribute pirated files (music, video, software).

Information gathering- In general terms, the information gathering category of incidents includes those activities associated with identifying potential targets and understanding the services running on those targets. This type of incident involves reconnaissance, with the goal being to identify the:

- existence of a target, and understand the network topology surrounding it, and with whom the target routinely communicates, and
- potential vulnerabilities in the target or its immediate network environment that could be exploited.

Typical examples of information gathering attacks by technical means include:

- dumping Domain Name System (DNS) records for the target's Internet domain (DNS zone transfer),
- pinging network addresses to find systems that are ‘alive’,
- probing the system to identify (e.g., fingerprint) the host operating system,
- scanning the available network ports on a system to identify the related services (e.g. e-mail, FTP, web, etc.) and the software version of those services,
- scanning for one or more known vulnerable services across a network address range (horizontal scanning).

In some cases, technical information gathering extends into unauthorized access if, for example, as part of searching for vulnerabilities the attacker also attempts to gain unauthorized access. This commonly occurs with automated hacking tools that not only search for vulnerabilities but also automatically attempt to exploit the vulnerable systems, services and/or networks that are found. Information gathering incidents caused by non-technical means, resulting in:

- direct or indirect disclosure or modification information,
- theft of intellectual property stored electronically,
- breaches of accountability, e.g. in account logging,
- misuse of information systems (e.g. contrary to law or Schneider Heller School policy),
- could be caused by breaches of physical security arrangements resulting in unauthorized access to information, and theft of data storage equipment that contains important data, for example encryption keys, poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware, resulting in internal or external personnel gaining access to information for which they have no authority.

APPENDIX III – Classification of Information Security Events and Incidents

It is important to document information security incidents in a consistent manner, in order to share the information on information security incidents, make it easier to automate incident reporting and responses, and identify the severity levels of information security incidents using a consistent criteria.

Based upon the classification factors, information security incidents are classified by severity using a scale. The Heller School scale is simple, and classifies events as ‘major’ or ‘minor’.

6. Incident Management Reporting Form

Heller School Incident Management Reporting Form

Date of Event _____ Event Number _____

Reporting Person Information

1. Name (print) _____
2. Organization within Heller _____
3. Email and Phone number _____

Security Event Description. Please include: what occurred, how it occurred, what assets were affected.

_____

_____

_____

Date and Time the Event occurred _____

Was the Event MINOR MAJOR

For Information Security Committee only:

Steps Taken to Resolve _____

Resolution of Event _____

Is response to this event closed? YES NO

If NO, when will event be closed? (Details)

In the case of a MAJOR security incident, notify the Heller Information Security Committee, the Data Custodian, the Heller Dean, and the University IRB.

Effective Date June 4, 2014