Information Security Incident Response Plan

Purpose
It is the objective of the university to maintain secure systems and data. In order to comply with federal, state, and local law and contractual obligations, the division of information services is responsible for a coordinated response to a breach or potential compromise of systems or data. This incident response plan supplements the Administrative Policy on Electronic Information Security (3342-9-01.4) and provides guidance for identification, containment, notification, verification, communication, investigation, and remediation of such incidents.

Responsibility
Any university employee or any other person or entity who believes a breach or potential compromise (electronic or physical) of any type or form of system or data has occurred is required to adhere to the steps outlined in this plan.

Resilience
It is imperative that prior to an incident occurring, adequate protections are put in place to ensure the continuity of business operations before, during, and following the detection of a security incident. The Division of Information Technology has taken steps to perform ongoing monitoring and detection of university information technology systems and developed the following procedures in effort to minimize the impacts when security events occur. Upon verification of a security incident, steps will are taken to neutralize the incident – which in many cases will result in processing delays or system outages – however, these effects are minimized through the coordinated response efforts. In the event of a significant incident (as determined by the incident response team), it may become necessary to enact a full recovery by initiating the disaster recovery process.

Identification
Identification of a breach or potential compromise of data is the first step in an incident response. Identification can occur by, but is not limited to, the following:

(1) Report from a third party (such as a law enforcement agency),
(2) Anonymous complaint of unauthorized use or misuse of data,
(3) Alerts from security monitoring systems including, but not limited to, intrusion-detection, intrusion prevention, firewalls, file-integrity monitoring systems, and network infrastructure devices that detect rogue wireless access (wireless access points physically connected to the network that are used to intentionally subvert University policy and/or security controls)
(4) Routine monitoring (examination of activity and/or access logs),
(5) Vulnerability scans, or
(6) Suspicious circumstances beyond normal processes.

Containment

Containment is the next critical step to limit exposure, preserve potential evidence, and prepare for an investigation of the incident. Containment steps include:

(1) If an electronic device:

(a) Do not access or alter the compromised device,
(b) Do not power off the device,
(c) Do terminate its network connection (unplug network connection from the device or disable the wireless adapter),
(d) Isolate the device from access by others,
(e) Document how the event was detected and the device's state at that time, and
(f) Document steps taken to contain and isolate the device.

(2) If data is believed to have been compromised by loss of physical property, follow the steps outlined in the section for Internal Notification.

Initial Notification

In the event of a breach or potential compromise of data, notification of the appropriate KSU personnel will ensure a coordinated and unified response in determining the scope of the breach, business continuity, internal and external communications, and remediation. Notification must be made to the office of security and access management at 330-672-5566 during normal business hours. Do not leave a voicemail message if the call goes unanswered. If the call is not answered or it is being made outside of normal business hours, contact the division of information services data center at 330-672-2552. An email notification should also be sent to securityescalation@kent.edu.

(1) If the data breach involves loss of physical property (theft of physical media or a device containing credit card data), report this to the law enforcement agency having jurisdiction where the loss occurred.

(2) Cross reference each notification. Provide law enforcement with contact information used for internal university notification. Include law enforcement department and report number in notification to university.

Response Team

The recipient(s) of notification of a breach or potential compromise of data should immediately contact the manager of security and access management who will contact the members of the Response Team to begin the requisite response activities. The Response Team will be comprised of representation from the office of security and access management, division of information services, general counsel, and compliance and risk management department. The department of public safety/ police services will be a member of the Response Team if the breach or potential compromise of data occurs on any Kent State University owned or leased property or until such jurisdiction is determined. In the absence of the manager of security and access management, responsibility for contacting the Response Team will fall to the members of the team in

the order listed. The Response Team will convene immediately to initiate a response and will involve others in the university community as circumstances warrant.

Verification

(1) The division of information services will lead preliminary efforts in verifying a breach occurred. If and upon the discovery of evidence indicating a criminal offense was committed, the department of public safety / police services will be notified. Police services may collaborate with other federal, state, and local law enforcement agencies as appropriate. A criminal investigation may be conducted in parallel, supersede, or require authorization for any further action taken by the university.

(2) The theft of physical media or a device containing sensitive university data will be reported to the appropriate law enforcement agency. A criminal investigation will be at the discretion of said agency. The division of information services will be responsible for attempts to determine the type and scope of data potentially compromised. Additionally, the division of information services in conjunction with the person having control over the device will determine the availability of remote access to the device.

Internal Notification

Communication strategies begin upon the verification of a data breach or compromise. Once a potential breach has been reported and verified per the Internal Notification and Verification procedures, Information Services Leadership Team will facilitate communications to other university areas. The following institutional members will ALL be informed of the breach or compromise of data and will be provided with periodic updates of significant findings from Information Services Leadership Team during the investigation and remediation processes:

- Vice President for Information Services,
- Senior Vice President for Finance and Administration, (The SVP for Finance and Administration will notify the President and the President's office will determine if notification of Trustees is warranted based on the circumstances.)
- Vice President or executive responsible for functional area of breach,
- General Counsel,
- Director of Public Safety / Police Services,
- Senior Vice President for Strategic Communications and External Affairs,
- Insurance company providing cyber liability coverage,
- Respective Data Steward(s) based on affected systems or data,
- Respective reporting agencies as required by law or contractual obligation

Investigation

The investigation will be the responsibility of the division of information services, the appropriate law enforcement agency, or a combination of both. The investigation will include, but is not limited to, the following:

(1) Interview of the person or entity learning of or discovering the breach or compromise of data.

(2) Collect and preserve evidence:

(a) Photograph or video record the scene as is,
(b) Collect affected hardware,
(c) Acquire activity and/or access logs and network logs for device,
(d) Acquire recent history of users of device,
(e) Retain documentation of any associated alerts from security monitoring systems,
(f) Obtain video surveillance history and key swipe logs of area accessed without authorization, and
(g) Maintain chain of custody records for evidence collected.

(3) Minimize scope:

(a) Determine if breach or compromise is likely to be duplicated,
(b) Determine if breach or compromise is beyond a single device,
(c) Cease operation of certain hardware or physical areas where there is a reasonable belief the breach or compromise could be repeated, and
(d) Provide alternatives to affected area to maintain business operations.

(4) Forensics:

(a) Forensics should support the overall investigation in determining the origination of the breach or compromise, the devices and or systems affected, the data compromised, and the possibility of re-occurrence.

(b) A forensic consultant may be contracted at the discretion of the division of information services and the division of business and finance in the absence of or in conjunction with a criminal forensic process. The need for a forensic consultant will be determined based on the type and scope of the breach or compromise or may be contractually required by one or more of the involved reporting agencies.

Recovery/ External Notification / Remediation

The information gathered during the investigation will allow for assessment of functional impact, informational impact, and remediation.

(1) The division of information services and the division of finance and administration will be jointly responsible for the following:

(a) Formal documentation of event.
(b) Notifying the cyber liability insurance carrier and coordinating the services provided under the policy with internal stakeholders.
(c) In consultation with the office of general counsel, notification and delivery of documentation will be made to the relevant reporting agencies as appropriate based on the nature and magnitude of the breach.
(d) In consultation with the division of university relations, prepare notification in the form deemed most appropriate and expedient to be sent to affected individuals.
(e) If deemed appropriate by legal statute or otherwise decided, prepare to offer free credit report resources to affected users.
(f) Determine if a call center, website, or email service should be offered to affected individuals.
(g) Coordinate regular update meetings during the investigative process and a debriefing meeting approximately two to four weeks post event.

(2) The division of information services will be responsible for the following:

(a) Remediate any compromise to network or device security.
(b) Document scope of compromised data including names and contact information of affected individuals.
(c) Backup and provide any necessary network, log, scan, and device data to any investigative body within the legal requirements.
(d) Aid in providing resources necessary for the university to coordinate communication to all entities listed within this plan (for example: website, call center, email development and support).

(3) The division of university relations will assume responsibility for disseminating information to the media in consultation with the division of finance and administration and the division of information services.

(4) The division of information services with guidance from the office of general counsel will assume responsibility for the review and compliance of applicable state (Ohio Revised Code 1347.12) and federal statutes related to data breaches.

Incident Response Plan Distribution and Review

(1) The Incident Response Plan will be available on the office of security and access management website (https://www.kent.edu/is/policies-and-procedures)

(2) Incident Response Plan training will occur annually or during employment orientation.

(3) A mock event will be held annually to test the Incident Response Plan.

(4) As part of the mock event, event controllers will be present not only to observe the plan in action, but also to assess the content, structure, and usability of the plan.

(5) The division of information services will maintain current information on Information Security standards and policies as well as current contact information for the reporting agencies.

(6) Training assessment, mock event evaluation, lessons learned from actual incidents, and security standards organizations as well as federal and state law will be used to appropriately modify existing controls and the Incident Response Plan as needed, at a minimum annually.

Review and Revision History

- Original document – 7/11/2018
- Revision 1, citing policy and resilience – 10/25/2018