**Information Security Incident Response Plan**

**Purpose**

It is the objective of the college to maintain secure systems and data. In order to comply with federal, state, and local law and contractual obligations, the Incident Response Team is responsible for a coordinated response to a breach or potential compromise of systems or data. This incident response plan provides guidance for identification, containment, notification, verification, communication, investigation, and remediation of such incidents.

**Responsibility**

Any college 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 data security incident. The Information Technology Services department has taken steps to perform ongoing monitoring and detection of college 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 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. Notification by member of campus community
2. Report from a third party (such as a law enforcement agency)
3. A notification or complaint of unauthorized use or misuse of data
4. 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 College policy and/or security controls)
5. Routine monitoring (examination of activity and/or access logs)
6. Vulnerability scans
7. Unusual activity outside of normal business systems, workflows, processes, transactions, or communications
8. Notification of cyber breach or data compromise from business partners

**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 cyber-breach or malware is suspected on an electronic device (e.g. PC, laptop, smartphone):
   1. Immediately discontinue use of the device. Do not touch any controls or interfaces (keyboard, mouse, pointers) for any reason
   2. Terminate the network connection of the device (unplug network connection from the device) if possible
   3. Physically isolate the device to prevent access by others if possible
   4. Notify Information Technology Services at x7293 or Public Safety x7000
   5. Note: How the event was detected, the time, any account information, what activity was occurring, on-screen messages Do not access or alter the compromised device,
   6. **Do not power off the device or attempt to reboot**
2. If data is believed to have been compromised by loss of physical property
   1. Note potential data that may be at risk or exposed
   2. Notify the Public Safety Office (x7000)
   3. Notify the ITS department (x7293) and via email HelpDesk@Augustana.edu

**Initial Notification**

In the event of a breach or potential compromise of data, notification of the appropriate Augustana 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 ITS department (309-794-7293) 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 Office of Public Safety at 309-794-7000 who will notify members of the Incident Response Team. An email notification should also be sent to Helpdesk@Augustana.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 college notification. Include law enforcement department and report number in notification to college.

**Incident Response Team**

The Incident Response Team will be comprised of representation from ITS, Finance, General Counsel, and Marketing / Communications. Upon notification of a suspected breach or potential compromise of data the Chief Information Officer will ensure communication with other members of the Response Team to begin the requisite response activities. The Response Team will convene as soon as possible to initiate a response and will involve others in the college community as circumstances warrant. The Response Team will determine the need and pace of all official communication.

**Verification**

1. The Information Services department will lead preliminary efforts in verifying a breach or compromise of data occurred. If and upon the discovery of evidence suggesting a criminal offense was committed, the Department of Public Safety or other law enforcement services may be notified. Law enforcement 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 college.
2. The theft of physical media or a device containing sensitive college data will be reported to the appropriate law enforcement agencies. A criminal investigation will be at the discretion of said agencies. The Information Technology Services department will be responsible for attempts to determine the type and scope of data potentially compromised. Additionally, ITS in conjunction with the person having control over the device will determine the availability of remote access to or from the device.

**Internal Notification**

Internal communication strategies begin upon the verification of a data breach or compromise. Once a potential breach or compromise has been reported and verified per the Internal Notification and Verification procedures, the Incident Response Team will facilitate communications to other college areas. Communication will be at a pace consistent with the investigation and resolution process. The following institutional members will be informed of the breach or compromise of data and will be provided with periodic updates of significant findings by the Incident Response Team during the investigation and remediation processes:

* Vice President for Finance and Administration, (The VP 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.)
* Chief Information Officer
* General Counsel
* Vice President of Communications / Marketing
* Vice President or executive responsible for functional area of breach
* Insurance company providing cyber liability coverage
* Respective reporting agencies as required by law or contractual obligation
* Respective Data Steward(s) based on affected systems or data
* Chief of Augustana Police Services

**Investigation**

The investigation will be the responsibility of Incident Response Team, the Information Technology Services department, appropriate law enforcement agency, or a combination of all. 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:
   1. Photograph or video record the scene as is
   2. Collect affected hardware
   3. Acquire activity and/or access logs and network logs for device
   4. Acquire recent history of users of device
   5. Retain documentation of any associated alerts from security monitoring systems,
   6. Obtain video surveillance history and key swipe logs of area accessed without authorization, and
   7. Maintain chain of custody records for evidence collected.
3. Minimize scope:
   1. Determine if breach or compromise is likely to be duplicated,
   2. Determine if breach or compromise is beyond a single device,
   3. Cease operation of certain hardware or physical areas where there is a reasonable belief the breach or compromise could be repeated, and
   4. Provide alternatives to affected area to maintain business operations.
4. Forensics:
   1. 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.
   2. A forensic consultant may be contracted at the discretion of the Response Team, recommendations by Information Technology Services, and College leadership. The need for a forensic consultant will be determined based on the type and scope of the breach or compromise, the guidance of college insurance providers, as well as obligations contractually required by one or more of involved reporting agencies or business partners.

**Recovery/ External Notification / Remediation**

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

1. The members of the Incident Response Team will be responsible for the following:
   1. Formal documentation of event.
   2. Notifying the cyber liability insurance carrier and coordinating the services provided under the policy with internal stakeholders.
   3. Notification and delivery of documentation to the relevant reporting agencies as appropriate based on the nature and magnitude of the breach.
   4. In consultation with affected campus offices, developing notifications in the form deemed most appropriate and expedient to be sent to affected individuals.
   5. Determining if a call center, website, or other resources should be offered to affected individuals.
   6. Coordinating regular update meetings during the investigative process and a debriefing meeting approximately two to four weeks post event.

1. The Information Technology Services department will be responsible for the following:
   1. Remediating any compromise to network, data, or device security.
   2. Documenting scope of compromised data including names and contact information of affected individuals.
   3. Archiving and providing any necessary network, log, scan, and device data to any investigative body within the legal requirements.
   4. Aiding in the provision of resources necessary for the college to coordinate communication to all entities listed within this plan (for example: website, call center, email development and support).
2. The Communication and Marketing department will assume responsibility for disseminating information to the media in consultation with the VP of Finance and Administration, General Counsel, and Information Technology Services.
3. The Response Team will assume responsibility for the review and compliance of applicable state and federal statutes related to data breaches.
4. Suggested post-event review questions:

* Could additional/modified policy have prevented the incident?
* Was a procedure or policy not followed which allowed the incident? Then what could be changed to be sure the procedure or policy is followed in the future?
* Have changes been made to prevent a new and similar situation?
* Was the incident response appropriate? How could it be improved?
* Was every appropriate party informed in a timely manner?
* Were the incident response procedures detailed and cover the entire situation? How can they be improved?
* Have changes been made to prevent a recurrence? Are all systems patched, systems locked down, passwords changed, anti-virus updated, etc.?
* Should any security policies be updated?
* What lessons have been learned from this experience?

**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.Augustana.edu/its/policies>)
2. Incident Response Plan information will be shared annually or during employment orientation.
3. Lessons learned from a cyber- incident 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

Updated: 03/04/2021