South Dakota Public Assurance Alliance

Cyber Incident Response Plan

Effective July 14, 2022

Plan Purpose:

The South Dakota Public Assurance Alliance (SDPAA) serves SDPAA Members who are all local government entities in South Dakota. The SDPAA recognizes its responsibility to protect against theft of Member data and malware threats to its information systems, such as viruses and spyware applications, for any SDPAA business operations. The SDPAA also recognizes its responsibility to its fellow Members to ensure its continued operations to the maximum extent possible in the event of a cybersecurity incident. The SDPAA Board of Directors hereby adopts this Cyber Incident Response Plan (Plan) to further define the methods for identifying, tracking, and responding to technology-based security incidents. Incorporated by reference are the SDPAA Data Security Policy (Data Policy) and SDPAA Continuing Operations Plan (COOP).

This Plan is not to be considered comprehensive as every situation cannot be addressed in one plan. Rapid developments in technology and the advent of new methods for cyberattacks make the ability to provide an all-encompassing Plan impossible. The SDPAA expects SDPAA team members to use sound judgment and to act in ways that protect the SDPAA's information, assets, and communication systems.

Failure to act in ways that protect SDPAA information, assets, and communication systems, or failure to cooperate with inquiries or investigations, can result in corrective action, which may include termination of employment or cancellation of a vendor services agreement with the SDPAA.

This Plan is established to assist in protecting the integrity, availability, and confidentiality of technology and assist in complying with statutory, regulatory, and contractual obligations. Responding quickly and effectively to an incident is critical to minimizing the spread of the incident and/or the business, financial, legal, and/or reputational impact. Incident Response includes the following phases:

1. Detection, reporting, and analysis.
2. Legal.
3. Forensics.
4. Containment, Eradication, and Recovery.

5. Other Responses (i.e., Public Relations).
6. Post-Incident Review.

Scope

This Plan governs incidents that have a significant negative impact on information technology systems and/or sensitive information (hereinafter, "incidents.") Incidents can include denial of service, malware, ransomware, and/or phishing attacks that can significantly impact operations and/or result in the unintended disclosure of sensitive data (e.g. Member data, Personally Identifiable Information, credit card data, and law enforcement records).

Minor events (e.g., routine detection and remediation of a virus, a minor infraction of a security policy, or other similar issues that have little impact on day-to-day business operations) are not considered an incident under this Plan.

Incident Identification

A security incident is an event that is a cybersecurity breach, or a cyber extortion threat, or a data breach.

1. **<u>Cybersecurity breach</u>**

A cybersecurity breach is any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

2. **<u>Cyber extortion threat</u>**

A cyber extortion threat is a threat against the network to:

a. Disrupt operations.
b. Alter, damage, or destroy data stored on the network.
c. Use the network to generate and transmit malware to third parties.
d. Deface the Member's website.
e. Access personally identifiable information, protected health information, or confidential business information stored on the network, made by a person or group whether acting alone or in

collusion with others, demanding payment, or a series of payments in consideration for the elimination, mitigation, or removal of the threat.

3. Data Breach

A data breach is the actual or reasonably suspected theft, loss, or unauthorized acquisition of data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

4. Other Cybersecurity incidents

Other cybersecurity incidents include:

a. Attempts from unauthorized sources to access systems of data.
b. Unplanned disruption to a service or denial of a service.
c. Unauthorized processing or storage of data.
d. Unauthorized changes to system hardware, access rights, firmware, or software.
e. Presence of a malicious application, such as ransomware, or a virus.
f. Presence of unexpected/unusual programs.

Designation of an Incident Response Manager

The SDPAA hereby designates the SDPAA's Information Technology vendor as its Incident Response Manager, who shall be readily available to employees in the case of a cybersecurity event. Responsibilities of the Incident Response Manager include:

1. Determining whether an event, or a series of security events, is declared an incident.
2. Ensuring this Plan is followed.
3. Establishing an Incident Response team as needed to support the execution of this Plan.
4. The Manager and/or team will execute this Plan in accordance with and at the direction of the Manager.

The Executive Director will ensure end-users have sufficient knowledge to recognize a potential security incident and report it in accordance with this Plan. Employees are responsible to report potential security incidents in a timely manner and provide any requested support during Plan execution.

Incident Response Team

The Incident Response Team will be able to quickly respond to cybersecurity incidents and shall gather the needed resources and make the appropriate decisions to resolve the incident. The SDPAA's Incident Response team shall consist of the following:

SDPAA IT Vendor

SDPAA Executive Director/Deputy Director (one or both depending on availability)

SDPAA General Counsel

AXA XL Data Breach Hotline 1-855-566-4724

The SDPAA Executive Director will notify the SDPAA Board of Directors of any cybersecurity incident within a reasonable time as practical under the circumstances. The Incident Response team will be responsible to ensure proper notifications required by law.

Incident Response Phases

1. **<u>Detection, Reporting and Analysis</u>**

   a. If a user, employee, contractor, or vendor observes a potential security event they should notify the SDPAA Executive Director immediately. If the Executive Director is not available, then the event(s) should be immediately reported to another member of the SDPAA internal team.
   b. The Executive Director will immediately report it to the Incident Response Manager. The Executive Director is responsible for communicating the incident, its severity, and developing the action plan with consultation from the Incident Manager.
   c. If the Incident Manager or Executive Director/Deputy Director are not available, a user should isolate the affected devices from the network or

internet by removing the network cable from the device. If operating via wireless, the user should turn off the wireless connection. If isolating the machine from the network is not possible, then the user should unplug the machine from its power source.

d. If the Incident Manager or Executive Director/Deputy Director determine or suspect a cybersecurity breach, cyber extortion threat, or a data breach as defined in this Plan, then the team will proceed to part e. below. If it is not suspected to be a security incident, then the team will proceed to part f. below.
e. For an actual or suspected security breach, the AXA XL Data Breach Hotline will be contacted immediately. If no answer, the team will leave a message with their contact information. When the Hotline responds, the team shall follow their directions.
f. If the incident is determined not to be a security threat, then the Incident Manager will work with the Incident Response team to assess the incident, develop a plan to contain the incident, and ensure the action plan is communicated and approved to all users.
g. The Incident Response Manager will ensure that all actions are documented as they are taken and the Executive Director/Deputy Director, Incident Response team, and outside support are regularly updated.

2. Containment, Eradication, and Recovery

a. Containment

Containment is the act of limiting the scope and magnitude of the attack as quickly as possible. Containment has two goals: preventing data of note from being exfiltrated and preventing the attacker from causing further damage. The steps for **immediate triage**:

1. Immediately contact the Incident Response Manager to report the event and follow their instructions. The Incident Response Manager will notify the Executive Director/Deputy Director of the incident and to execute the security incident response plan.

2. If the Incident Response Manager is not available, a user shall isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. A User will not turn off the device or remove the power source unless instructed by the Incident Response Manager.
3. The Incident Response team assembles and assesses if the incident is a cyber security breach, cyber extortion threat, or data breach. If it is, or if there is any question the incident may or may not be one, the Executive Director/Deputy Director contacts the AXA XL Hotline. The Incident Response team will work with the breach coach and the other partners they suggest to help resolve the incident.
4. Document all actions as they are taken.

b. Eradication

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the OS and applications is preferred.

c. Recovery

Recovery allows business processes affected by the Incident to recover and resume operations. It generally includes:

1. Reinstall and patch the OS and applications.
2. Change all user and system credentials.
3. Restore data to the system.
4. Return affected systems to an operationally ready state.
5. Confirm that the affected systems are functioning normally.

Forensics

Security incidents of a significant magnitude may require that a forensics investigation take place.

Once that need has been established all additional investigation/containment activities need to be directed and/or performed by a forensics specialist to ensure that the evidence and chain of custody is maintained. The Executive

Director/Deputy Director in consultation with the Incident Response Manager and/or XL will advise if engaging a forensics firm is required.

Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

a. Information about the Incident type
b. A description of how the Incident was discovered.
c. Information about the systems that were affected.
d. Information about who was responsible for the system and its data.
e. A description of what caused the Incident.
f. A description of the response to the Incident and whether it was effective.
g. A timeline of events, from detection to Incident closure
h. Recommendations to prevent future Incidents.
i. A discussion of lessons learned that will improve future responses.

Periodic Review

This Plan and associated subordinate procedures will be reviewed at least annually by the Executive Director/Deputy Director and the Incident Response Manager to adjust processes considering new risks and security best practices. Any changes in this Plan shall be approved by the SDPAA Board of Directors.

Special Situations/Exceptions

Any personally owned devices, such as PDAs, phones, wireless devices, or other electronic devices which have been used to access organizational data and are determined to be relevant to an incident, may be subject to retention until the Incident has been eradicated.

Adopted by the South Dakota Public Assurance Alliance Board of Directors on July 14, 2022.

Source: July 14, 2022 Board of Directors meeting Minutes.