**SAMPLE INCIDENT RESPONSE PLAN/PROCEDURES**

*\*Note: Change highlighted areas to specific information related to your organization to tailor the PLAN/PROCEDURES for a quick, easy plan.*

1) Any individual who discovers the indicators of a cyber security incident will notify Notified Entity.

2) Notified Entity will provide an initial analysis by documenting responses to the following questions as they pertain to affected information systems/assets.

1. Please summarize the incident?
2. How was the incident discovered?
3. Names of systems being targeted, along with operating system, IP addresses, and locations.
4. IP address and any information about the origin of the attack.

(1) What Personally Identifiable Information (PII) or Protected Health Information (PHI) is known or suspected to be involved?

A) Information that can be documented in our systems

 1) Names

 2) Usernames

B) Only the type of Information can be documented in our systems

1) Health Information

2) Social Security Numbers

3) Credit Card or Bank Account Information

4) Driver’s License or other Government Issued Identification Numbers

 5) Passwords

(2) How many individuals’ information was affected by the security breach?

(3) Was the information encrypted?

(4) Is the breach on-going?

(5) Notified Entity will conduct initial Business Impact Analysis (BIA)

1. Is the equipment affected business critical?
2. What is the severity of the potential impact?
	* 1. A threat to public safety or life.
		2. A threat to sensitive data
		3. A threat to computer systems
		4. A disruption of services

(6) Notified Entity assigns the incident to the Security Team

(7) The Notified Entity will contact the Security Team On-Call for on-going breaches, threats to public safety or life, or threats to sensitive data on information systems

3) Security Team members will document and use forensically sound tools and techniques when analyzing evidence. This analysis typically includes, but is not limited to, reviewing system logs, looking for gaps in logs, and interviewing personnel to identify contributing factors to the incident. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

4) Security Team members, in consultation with Notified Entity, will determine a response strategy. If strategy involves the full incident response team (IR Team), the Incident Commander and the following individuals will be alerted and engaged as defined below:

Incident Commander – Joe R. Manager, 515-555-8888, jmanager@abccom.com

Network Administrator -

Firewall Administrator -

Server Administrator -

Desktop Administrator -

Application Administrator -

Cloud Administrator -

 Key considerations will include, but are not limited to:

a) Validation of an incident and potential for success

b) Continuation of activity

c) Identification of data or property is threatened and its’ criticality

d) Reevaluate BIA based on additional information obtained

e) Identification of systems targeted including physical and logical location on the network

f) Evaluation of immediate response actions cost benefit analysis

 1) What damage is likely to occur if immediate actions are not taken?

 2) What capabilities have the attackers demonstrated?

 3) What courses of action are available to the attackers if a security response is detected?

5) Security Team members will update the incident ticket. The incident will be categorized into the highest applicable level of one of the following categories:

a) Category one - A threat to public safety or life.

b) Category two - A threat to sensitive data

c) Category three - A threat to computer systems

d) Category four - A disruption of services

6) Security Team members will validate and follow response procedures based on their assessment of the incident:

a) Worm response procedure

b) Virus response procedure

c) System failure procedure

d) Intrusion response procedure - Is critical data at risk?

e) Phishing response procedure

f) System abuse procedure

g) Property theft response procedure

h) Website denial of service response procedure

i) Database or file denial of service response procedure

j) Spyware response procedure

The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for that type of incident.

7) Security Team, in consultation with Notified Entity, will recommend changes to management that are likely to preserve evidence, contain the breach, and prevent similar breaches from occurring. Examples of recommendations may include, but are not limited to, the following:

1. Take memory snapshots
2. Remove hard drives
3. Copy Virtual Machines
4. Rebuilding affected systems
5. Restore affected systems data from backups if necessary.
6. Changing passwords
7. Disabling or removing unused services
8. Installing system patches
9. Installing Endpoint Detection and Response (EDR) tools
10. Enable / Validate system logging

8) Security Team will determine if the incident is deemed too big or outside the realm of expertise of the organization. In this event the Security Team will recommend the Company Management engage outside help from the following organization:

Cybersecurity Company

111 E Main St

Des Moines, IA 50319

515-555-0123

9) Company Leadership will determine if prosecution is a desired outcome (and contact law enforcement to insure evidence is collected in accordance with law enforcement requirements), evaluate recommendations, and approve or reject recommendations.

10) Company Management will direct designated technical contacts to move forward documenting any modifications to affected systems, implementing approved changes to preserve evidence (if desired), containing the breach, and modifying configurations to prevent similar breaches from occurring.

11) Security Team, in conjunction with Company Leadership, will be responsible for aggregating and documenting the following information:

a) Incident discovery

b) Incident category

c) Incident progression

d) Incident Origin / attacker information

e) Implemented response procedures

f) System recovery actions

g) Effectiveness of the response

12) Incident Commander/Company Leadership will notify proper external agencies—*SEE APENDIX A*.

13) Company Leadership will aggregate damage and cost from their business units—assess the damage to the organization and estimate the cost of the damage, containment, and recovery.

14) Security Team will review response and update policies— The intent is to take preventative steps to decrease the probability of a similar intrusion. The response will be assessed by addressing at least the following points

a) Identify additional controls (administrative or technical) that would likely have prevented the intrusion.

b) Identify if existing controls were not implemented/employed which allowed the intrusion, and then consider what modifications could increase the probability that these controls are implemented/employed.

c) Was the incident response appropriate? How could it be improved?

d) Was every appropriate party informed in a timely manner?

e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

g) Have changes been made to prevent a new and similar infection?

h) Should any security policies be updated?

i) What lessons have been learned from this experience?

**ICN INFORMATION SECURITY INCIDENT/BREACH CHECKLIST**

**Preliminary Assessment**

* When and where did the information security breach occur?
* What devices, websites, or printed documents were lost, stolen or breached?
* What personally identifiable information is involved?
1. Name
2. Social Security Number
3. Credit Card Information or Bank Account Information
4. Driver’s License Number or other State Issued Identification Number (Medicaid ID, Student ID etc.)
5. Health Information
6. User name and password
* How many individuals were affected by the information security breach?
* Was the information encrypted?
* Is the breach on-going?

**Internal and Local Notifications**

* Notify Company Incident Response Team
* Notify Company Executive Team
* Notify Company Board
* Notify Customer(s) Affected
* Contact local law enforcement if breach is criminal in nature.
1. Local law enforcement number
* Contact the Attorney General’s Office if at least 500 Iowans are affected 515-281-5926.

**Federal Notifications**

* Contact the Federal Bureau of Investigation, 515-223-4278, if:
1. The security incident appears to have foreign government sponsorship.
2. The security incident appears to have a terrorist connection.
* Contact the Internal Revenue Service
1. 1-800-366-4484, if federal tax information is involved.
2. 1-800-908-4490, social security numbers are exposed
* Contact the Social Security Administration, 1-877-697-4889, if SSA provided data is involved.
* Contact the Department of Health & Human Services if unprotected health information is involved. <https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf>

**Public Notification**

* Does the breach trigger Iowa Code 715C PERSONAL INFORMATION SECURITY BREACH PROTECTION

<https://www.legis.iowa.gov/docs/code/715c.pdf>.

* Designate a contact person for releasing information.
* Issue a press release.
* Arrange for credit monitoring for affected individuals.
* Create data breach section on agency website with frequently asked questions.
* Establish a toll free number\call center.
* Send notification letter to affected individuals.

**Report**

* Complete a summary report after breach investigation is complete.