Aberrant Open-ISM™

INCIDENT RESPONSE POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

PROPRIETARY

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 Overview 4
2 Scope 4
3 Purpose 4
4 Incident Response 5
4.1 Preparing for and detecting an Incident 5
4.1.1 Reporting Information Security Events 5
4.1.2 Reporting Information Security Weaknesses 5
4.1.3 Assessment of and decision on information security events 6
4.2 Responding to and Containing an Incident 6
4.2.1 Communication Mechanisms during Incident 8
4.3 Breach incidents 8
4.3.1 Criminal incidents 8
4.3.2 Data exfiltration 8
4.3.3 Forensic considerations 8
4.4 Vendor breach incidents 9
4.4.1 Vendor breach with data exfiltration 9
4.5 Recovery from an Incident 9
4.6 Post-Incident Activities and Awareness 10
4.7 Incident Response Review 10
4.8 Testing 10
5 Contact Information 11
6 Document RACI 11
7 License Information 12
Appendix A: Reference List 13
Appendix B: Data Breach Email Template 14
Appendix C: Post Incident Assessment Template 15

1 OVERVIEW

In accordance with regulations, the organization has established a formal policy regarding an Incident Response Policy. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the organization's needs and goals. This policy is to be implemented immediately and the provisions below set forth the framework for the policy. The policy is supplemental to <<Company Name>>'s Business Continuity and Disaster Recovery Policy.

2 SCOPE

The scope of this policy relates to <<Company Name>>'s processes for preparation, handling, and mitigating security incidents related to <<Company Name>>'s network infrastructure and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone who has access to <<Company Name>>'s network or systems. The scope of the policy includes externally-reachable systems, such as <<Company Name>>'s website or public facing APIs, as well as <<Company Name>>'s overall data environment.

3 PURPOSE

The purpose of this policy is to describe what steps must be taken to ensure that security incidents are detected and mitigated in order to minimize damage to <<Company Name>>, its customers and members. The policy includes:

- At a minimum, roles, responsibilities and communication strategies in the event of a compromise.
- Specific incident response, business recovery and continuity procedures and data backup processes.
- Legal requirements for reporting any compromises to the data environment.
- Coverage and response mechanisms for all critical system components and all other I.T. resources deemed critical by the organization.

4 INCIDENT RESPONSE

<<Company Name>> has developed and implemented a comprehensive Incident Response plan, which encompasses the following categories and supporting activities listed below. These policy directives will be fully enforced to ensure that Incident Response plan initiatives are executed in a formal manner and on a consistent basis for all system components within the data environment and all other I.T. resources deemed critical by the organization.

The five (5) main categories of the Incident Response plan include the following:

- Preparing for an incident;
- Detecting an incident;
- Responding to and containing an incident;
- Recovery from an incident;
- Post-incident activities and awareness.

Please note that all requirements for regulations for an Incident Response plan are included in the five (5) previously listed categories, which have been identified as a best of breed framework for developing and implementing an effective Incident Response plan.

4.1 PREPARING FOR AND DETECTING AN INCIDENT

4.1.1 REPORTING INFORMATION SECURITY EVENTS

Detecting an incident requires a true commitment by all employees to be constantly aware of their surroundings for any type of social engineering, physical or environmental threat. Additionally, detection also requires due diligence and consistency by authorized employees regarding the secure configuration and review of network and system logs, being aware of network traffic anomalies and any suspicious or disruptive network patterns or incidents. Employees, third party consultants, contractors or service providers who detect or suspect an information security event has occurred should immediately contact Incident Response Team.

The Incident Response Team can only respond to a given incident if they are made aware of the issue. Detection, therefore, is a vital component of the Incident Response Plan.

4.1.2 REPORTING INFORMATION SECURITY WEAKNESSES

All employees, contractors and third-party users shall note and immediately report any observed or suspected security weaknesses in information processing systems or services. Users shall not attempt to test or repair a security weakness on their own.

4.1.3 ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS

Information security events will be assessed by members of the Incident Response Team. A decision will be made if the event should be considered a security incident. As a rule of thumb, the following events are to be considered incidents:

1. Unauthorized physical access
2. System failure or loss
3. Malware activity
4. Denial of Service
5. Any degradation in the Confidentiality, Integrity or Availability of data classified as a CONFIDENTIAL per <<Company Name>>'s internal Data Classification System.
6. Presence of any Indicators of Compromise (IoC)

The Information Response Team is to have clear roles and responsibilities for properly responding to any incident. Preparation is just as important as the response to the incident. Other aspects of preparing for an incident include the necessary steps, processes and procedures to take once an incident has occurred. This also includes an understanding of what actions are to be taken with respective third parties, if necessary, such as clients, law enforcement agencies, local/federal/state agencies, if necessary; as well as the media and any other third parties considered to be in scope.

Title	Role and Responsibility of the Incident Response Team
CISO or VP of Information Security	IT Crisis Coordinator. Manages response team and facilitates communications.
CTO	Backup IT Crisis Coordinator.
Network Security Engineer	Incident investigator.
Operations Security Engineer	Incident investigator.

4.2 RESPONDING TO AND CONTAINING AN INCIDENT

Any incident deemed to be a relevant threat to the organization requires a rapid response from authorized personnel, such as the Incident Response Team. This rapid response will follow a standard course of action designed to minimize the impact of the incident to the organization's critical network and system infrastructure.

The following documented response mechanisms serve as the Standard Operating Procedures (SOP) for responding to any incident within the organization:

1. For any incident that has been detected, the Incident Response Team is to be immediately notified.

2. The Incident Response Team is to formally assume control and to identify the threat and its severity to <<Company Name>>'s information systems and track the incident in JIRA (<<Company Name>>'s Incident Tracking System).
3. In identifying the threat, the Incident Response Team is to specifically identify which resources are at risk, both internal and external, and which harmful processes are currently running on resources that have been identified as at risk.
4. The incident response team should determine as to whether or not they need to escalate the incident.
5. The Incident Response Team is to make a determination if the resources at risk (hardware, software, etc.) require physical or logical removal. Resources which pose a significant threat to the continuity of the business are to be immediately removed or isolated, either physically or logically.
6. Information gathered during the incident response shall not be reported publicly without obtaining proper authorization from the Primary Crisis Manager / Communication Coordinator.

Resources which may require physical or logical removal or isolation may include, but are not limited to the following:

- All IP addresses in use;
- Firewalls;
- Routers and switches;
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS);
- Any enterprise-wide applications (CRM systems, etc.);
- Remote access;
- Point-to-point secure data transmission methods used for data traversing back and forth on the network;
- Wireless networking or networks;
- Authentication servers (RADIUS);
- Web servers;
- Proxy servers;
- File servers;
- E-mail servers;
- DNS servers;
- Operating systems;
- Databases;
- Applications.

4.2.1 COMMUNICATION MECHANISMS DURING INCIDENT

The Incident Response Team will determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident.

4.3 BREACH INCIDENTS

If the incident could affect <<Company Name>>'s ongoing operations or the security or integrity of data maintained by <<Company Name>, the Incident Response Team must notify members of the Crisis Response Team established under <<Company Name>>'s Business Continuity and Disaster Recovery Policy and must coordinate with members of that team to properly notify appropriate authorities or other affected parties. In particular:

4.3.1 CRIMINAL INCIDENTS

If the incident has in any way resulted in a criminal matter that may be readily identified, <<Company Name>> must immediately report it to law enforcement officials. This may include, but is not limited to the following:

1. Local law enforcement;
2. The United States Secret Service (for credit card fraud);
3. The Federal Bureau of Investigation (FBI).

4.3.2 DATA EXFILTRATION

If the Incident Response Manager and Legal Counsel have determined that customer data or other personal data subject to data protection regulation has been compromised it is the responsibility of the Incident Response Manager to notify members of the Crisis Response Team so that affected customers and/or individuals can be made aware of the incident in accordance with applicable law and with a targeted deadline of no more than 24 hours from the time the incident was detected.

4.3.3 FORENSIC CONSIDERATIONS

Investigating the incident is also a critical process within the Incident Response plan. Proper investigative techniques are to include, but are not limited to the following:

- Understanding how the incident occurred and what led to the compromise;
- Reviewing all necessary system documentation, such as logs, audit trails, rule sets, configuration and hardening standards and all other supporting documentation;
- Interviewing personnel as needed;

- Examining any third party providers and their respective products and services that are utilized within <<Company Name>>'s network architecture;
- If warranted, a third-party resource for assisting in the investigation of the incident may be utilized (this will be done at the management's discretion).
- Collecting evidence for dissemination to law enforcement.

4.4 VENDOR BREACH INCIDENTS

In certain situations, <<Company Name>> may be notified of a security incident at a 3rd party or vendor. In this case, an assessment must be performed to determine the impact of the breach (if any) to <<Company Name>>'s information assets. In addition to the standard Incident Response Lifecycle, the following steps should be taken to assess the situation:

1. Identify all network connectivity to the 3rd party
    1. Determine protocols and ports used between <<Company Name>> and the 3rd party
    2. Identify any Site-To-Site VPN tunnels
2. Identify all credentials provisioned to the 3rd party
3. Determine business impact of connectivity
    1. Check with various business units to determine criticality of network connectivity and services.
4. Perform containment by denying all inbound traffic for bi-directional channels (IPSec tunnels)
    1. Outbound traffic may be permitted if it is determined to be critical from step 3.1.
5. Review authentication logs to determine if any Indicators of Compromise (IoC) exist.
    1. Disable any provisioned accounts for the 3rd party. Accounts MUST not be re-enable until an impact assessment has been completed and approved by the CISO.

4.4.1 VENDOR BREACH WITH DATA EXFILTRATION

If no persistent network connectivity has been established with the 3rd party and the suspected breach involves exposure of <<Company Name>> data, the following steps must be performed:

1. Perform Business Impact Analysis (BIA) by assessing impact to various business units.
2. Contact <<Company Name>>'s legal counsel to determine reporting requirements to external authorities.
3. Engage <<Company Name>>'s legal counsel to determine any applicable restitution requirements.

4.5 RECOVERY FROM AN INCIDENT

Recovery procedures will include, but are not limited to the following:

- Restoring systems from CLEAN backups (a trusted source only, verify integrity);
- Completely rebuilding systems as needed and warranted;
- Replacing systems as needed (this includes all system components within the data environment and any other I.T. resources deemed critical by the organization);
- Reconfiguring network security (stronger, more adaptive configuration and hardening rules) for all system components within the data environment and any other I.T. resources deemed critical by the organization.

Change management requests are opened for issues that require mitigation. The recovery procedures will be commensurate with the incident that has occurred. This will be conducted on a case-by-case basis with all aspects of the recovery process fully documented.

4.6 POST-INCIDENT ACTIVITIES AND AWARENESS

A formal and documented Incident Response Report (IRR) is to be compiled and given to management of the organization within an acceptable time frame following the incident. The IRR should be generated as a ticket in an issue tracking system and must contain the following elements:

- Detailed description of the incident;
- Response mechanisms undertaken;
- Reporting activities to all relevant third parties as needed;
- Recovery activities undertaken for restoring affected systems;
- Creation of one or more 'Corrective Action' tickets necessary to prevent similar incidents in the future; and,
- An after-action review of the incident with the objective of mitigating the likelihood of future incidents.

4.7 INCIDENT RESPONSE REVIEW

For continuous improvement, incident response and escalation procedures are reviewed at least annually to evaluate their effectiveness.

4.8 TESTING

<<Company Name>> will perform annual testing of incident response processes based on appropriate scenarios that are well planned with clearly defined aims and objectives.

5 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

6 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

7 LICENSE INFORMATION

APPENDIX A: REFERENCE LIST

- National Institute of Standards and Technology, n.d. "Special Publications (800 Series)." http://csrc.nist.gov/publications/PubsSPs.html
- Massachusetts' General Law 93H, http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm
- Massachusetts' Office of Consumer Affairs and Business Regulation 201 CMR 17, http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf
- American National Standards Institute, "ISO/IEC 27001:2013."

APPENDIX B: DATA BREACH EMAIL TEMPLATE

Attorney General <<Attorney General's Name>>
Office of the Attorney General
<<Address of the Attorney General>>

Dear Attorney General <<AG's Last Name>>:

Pursuant to M.G.L. c. 93H, we are writing to notify you of [a breach of security/an unauthorized access or use of personal information] involving [number] Massachusetts resident[s].

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

[This paragraph should provide the date of the incident, a summary of the nature of the incident, a description of the categories of personal information involved in the incident, and whether the personal information that was the subject of the incident was in electronic or paper form].

NUMBER OF MASSACHUSETTS RESIDENTS AFFECTED

[This paragraph should specify the number of affected individuals residing in Massachusetts whose personal information was the subject of the incident. This paragraph should also indicate that these Massachusetts residents have received or will shortly receive notice pursuant to M.G.L. c. 93H, s. 3(b) and should specify the manner in which Massachusetts residents have or will receive such notice. You should also include a copy of the notice to affected Massachusetts residents in your notification to the Attorney General].

STEPS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

[This paragraph should outline all the steps <<Company Name>> has taken or plans to take relating to the incident including, without limitation, what you did when you discovered the incident; whether you have reported the incident to law enforcement; whether you have any evidence that the personal information has been used for fraudulent purposes; whether you intend to offer credit morning services to consumers; and what measures you have taken to ensure that similar incidents do not occur in the future.]

OTHER NOTIFICATION AND CONTACT INFORMATION

[Finally, your letter should indicate whether you have provided similar notification to the Director of Consumer Affairs and Business Regulation. You should also include the name and contact information for the person whom the Office of the Attorney General may contact if we have any questions or need further information.]

APPENDIX C: POST INCIDENT ASSESSMENT TEMPLATE

The following information is required for a post incident analysis by management. This information should be stored in <<Company Name>>'s documentation repository.

Date of incident		
General description of the incident		
Root Cause of Incident		
Areas Affected		
Extent of Damage		
Operational Impact		
Plan for Recovery		
Personnel Requirements		
External Support Requirements		
Estimated Time of Recovery		
Lessons Learned		