Incident Response Plan

Prepared by: Isabelle Jaber

Date: September 9th, 2024

Table of Contents:

REVISION HISTORY

This Incident Response Plan has been modified as follows:

Date	Version	Modification	Modifier
11-09-2024	1.0	Plan Created	Isabelle Jaber

TESTING & REVIEW CYCLE

Testing of the Incident Response Plan biannually (twice per year) is necessary to ensure the CSIRT (Cyber Security Incident Response Team) is aware of its obligations. Unless real incidents occur, which test the full functionality of the process, this can be achieved using walkthroughs and practical simulations (via penetration testing) of potential incident scenarios.

1. The Incident Response Plan will be tested at least twice per year.
2. The Incident Response Plan testing will test the business response to potential incident scenarios to identify process gaps and improvement areas.
3. The CSIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Handler will ensure the Security Incident Response Plan is updated and distributed to CSIRT members.

PURPOSE & SCOPE

PURPOSE

This Incident Response Plan exists to ensure SPENDOLOGY SOLUTIONS is prepared to manage cyber incidents in an effective and efficient manner. Cyber security incidents are more frequent and sophisticated than ever. No organization globally is immune to attack. Organizations must ensure they are prepared to respond to incidents as well as prevent and detect. By having a plan, a team, and conducting exercises, we will be better prepared to respond to inevitable incidents. In addition, we will be able to contain the damage and mitigate further risk to the organization in our response. Resources must be deployed in an organized fashion with exercised skills and communication strategies.

This document describes the plans for responding to Ransomware, Data Leaks, and Malware incidents at SPENDOLOGY SOLUTIONS. It identifies the structure, roles and responsibilities, types of common incidents, and the approach to preparing, identifying, containing, eradicating, recovering, and conducting lessons learned in order to minimize the impact of cyber security incidents.

The goal of the Incident Response Plan is to ensure SPENDOLOGY SOLUTIONS is organized to respond to cyber security incidents effectively and efficiently.

SCOPE

This Incident Response Plan applies to the networks, systems, data, and stakeholders (i.e. employees, contractors, 3rd party vendors) that access these networks, systems, and data. Members of the organization who are part of the Cyber Security Incident Response Team (CSIRT) are expected to lead or participate in a cyber security incident response. CSIRT members must familiarize themselves with this plan and be prepared to collaborate with the goal of minimizing adverse impacts on the organization.

This document establishes incident handling and incident response capabilities and determines the appropriate response for common cyber security incidents that will arise. This document is not intended to provide a detailed list of all activities that should be performed in combating cyber security incidents.

AUTHORITY

The responsibility for the security of company and customer information resides with the CISO/Owner of SPENDOLOGY SOLUTIONS. During times when a high or critical cyber security incident is underway this responsibility is entrusted to the Cyber Security Incident Response Team (CSIRT).

DEFINITIONS

Term	Definition
Acceptable Interruption Window	In business continuity planning, is the amount of time in which basic functionality must be stored for critical systems. It is a major factor when planning a disaster recovery solution.
Confidentiality	A classification of data that typically refers to Personally Identifiable Information (PII). This may include information such as names, addresses, phone numbers, drivers license numbers, etc.
Cyber Security Event	An observable occurrence in a system or network. Events may include a user connected to a file share, a server receiving a request for a web page, a user sending an email, etc.
Cyber Security Incident	Any incident, accidental or otherwise, that impacts communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity, or availability of information, data, or services provided by SPENDOLOGY SOLUTIONS. This includes unauthorized access to use, disclosure, modification, or destruction of data or services used or provided by SPENDOLOGY SOLUTIONS.
Denial of Service (DoS)	Also known as a DoS attack, it seeks to make a remote service unavailable to its intended users by flooding its host with requests which overload the system.
Exploit	A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.
Indicators	Also known as “Indicators of Compromise” or IOCs, are forensic clues or symptoms left behind by security attacks or breaches in the company’s network or systems. These

	clues are sometimes found in log entries, files, or databases.
Integrity	Refers to the maintenance or assurance of data accuracy, consistency, and its accessibility to authorized users for its entire life-cycle.
Maximum Tolerable Downtime	In business continuity planning, this specifies the maximum period of time that a given business process can be inoperative before the organization's survival is at risk.
Response Playbook	Introduces prescriptive cyber security measures and best practices that can be implemented to improve the organization's security posture. This playbook provides a set of standards to reference the organization, improves current systems and implement new ones.
Service Availability	Describes the state of a system being available and responsive to prospective users. The term is sometimes used to reference a measure of reliability of a system or network resource based on how often it is available as a % of time.
Service Level Agreement (SLA)	Used to describe a guaranteed measure of service availability. If service availability drops below the prescribed SAL, there are usually financial repercussions, like a money-back guarantee.
Stakeholder Relationship Map	A diagram that describes the relationship between individuals in an organization. With respect to cyber security, these diagrams are used to perform IF risk assessments to better inform preventative and reactive measures.
Vulnerability	A piece of code or bug within a system that causes unintended or unanticipated behavior. A vulnerability implies that this behavior can be taken advantage of for malicious reasons.
War Room	A dedicated meeting room where major incidents are handled together. It must have a door for privacy, must be available at all times, and must have good communications

	infrastructure (network, phone, etc.)
Zero-Day	A type of vulnerability that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has at least the potential to be exploited, if it has not already been exploited by cybercriminals.

HOW TO RECOGNIZE A CYBER INCIDENT

A cyber security incident may not be recognized straightaway; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within your environment, or that of your third-party service providers.

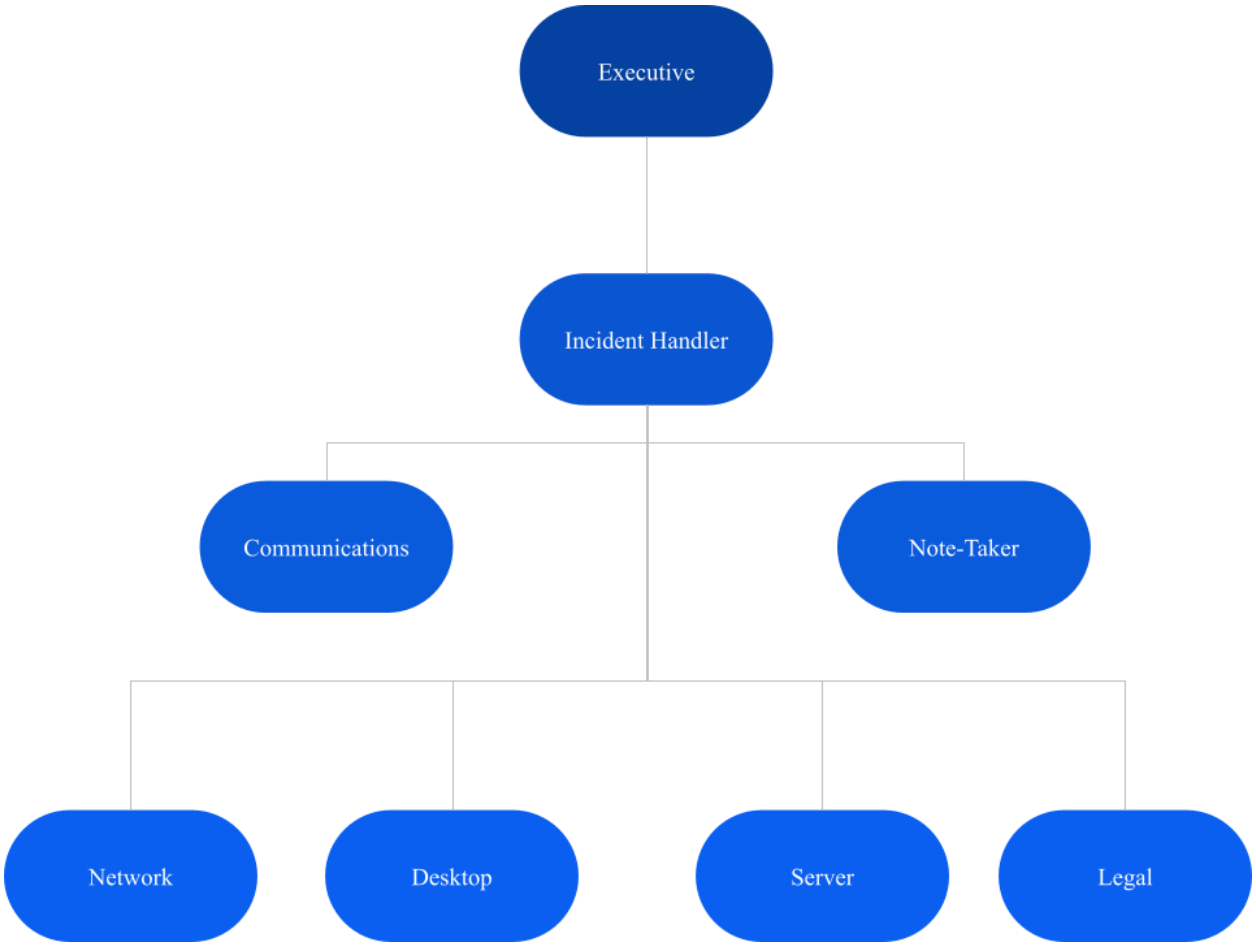
Look out for any indication that a security incident has occurred or may be in progress. Some of these are outlined below:

1. Excessive or unusual log-in and system activity, in particular from any inactive user IDs (user accounts).
2. Excessive or unusual remote access activity into your business. This could relate to staff or third-party providers.
3. The occurrence of any new wireless (Wi-Fi) networks visible or accessible from your environment.
4. The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executable files and programs. This could be on your networks or systems, including web-facing systems.
5. Hardware or software key-loggers found connected to or installed on systems.
6. Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain payment card data or other sensitive data.
7. Unusual network traffic communicating to or from potentially suspicious IP addresses.

CYBER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

CSIRT STRUCTURE

Common structure of a Cyber Security Incident Response Team (CSIRT).



CSIRT ROLES

CSIRT Role	Role Definition
Executive	Accountable Executive for protecting cyber security within the organization. Responsible for reporting to board directors and other executives. Within the CSIRT, this role is responsible for all issues requiring executive decision.
Incident Handler	The Incident Handler is the main triage role of the CSIRT. This role organizes the team and initiates the Incident Response Plan to investigate and respond to cyber security incidents.
Communications	The Communications Expert is responsible for both public relations and internal communications. They are the messenger to ensure that internal/external stakeholders, customers, and the public are informed in a timely and compliant fashion.
Note-taker	The note-taker records the progress of the CSIRT, including anything from meeting minutes, to post-mortem reports.
Network	The Network Engineer provides technical expertise to the response.
Desktop Technician	The Desktop Support Specialist provides technical expertise to the response.
Server Technical	The Server Support Specialist provides technical expertise to the response.
Legal Technician	Legal Counsel providing legal expertise to the CSIRT.

CSIRT RESPONSIBILITIES

EXECUTIVES

The Executives are/is responsible for:

1. Meeting with the board of directors to best understand what is needed from a security point of view based on the organization's business needs.
2. Regularly reporting any incidents and necessary cyber security actions to the board of directors and other executives.

3. Making decisions on the best way forward based on information provided by the CSIRT team.
4. Making sure that the roles within the CSIRT team are filled and the necessary tools/training are provided for employees to do their jobs.
5. Meeting with key roles within the CSIRT team to better understand what improvements can be made.

INCIDENT HANDLER

The Incident Handler is responsible for:

1. Making sure that the Incident Response Plan and associated response and escalation procedures are defined and documented. Ensure the handling of security incidents is timely and effective.
2. Making sure that the Incident Response Plan is up-to-date, reviewed and tested, at least once each year.
3. Making sure that staff with Incident Response Plan responsibilities are properly trained, at least once each year.
4. Leading the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan, as and when needed.
5. Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc. as required.
6. Authorizing on-site investigations by appropriate law enforcement or payment card industry security/forensic personnel, as required. This includes authorizing access to/removal of evidence from the site.

COMMUNICATIONS EXPERT

The Communications Expert is responsible for:

1. Writing and sending internal and external communications about any incident that occurred.
2. Reporting any cyber incidents to the authorities if needed.
3. Interfacing with executives and other board members to provide information.
4. Interfacing with customers to provide regular updates about any incidents that may affect their experience.
5. Collecting customer responses for impact of incidents, how they were handled and any tips/suggestions.
6. Collecting lessons learned from members of the CSIRT team and updating management.

CSIRT TEAM

Cyber Security Incident Response Team (CSIRT) members are responsible for:

1. Making sure that all staff understand how to identify and report a suspected or actual security incident.
2. Advising the Incident Handler of an incident when they receive a security incident report from staff.
3. Investigating each reported incident.
4. Taking action to limit the exposure of sensitive information or payment card data and to reduce the risks that may be associated with any incident.
5. Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures and controls.
6. Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
7. Reporting each security incident and findings to the appropriate parties. This may include the acquirer, card brands, third party service providers, business partners, customers, etc., as required.
8. Helping law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
9. Resolving each incident to the satisfaction of all parties involved, including external parties.
10. Initiating follow-up actions to reduce the likelihood of recurrence, as appropriate.
11. Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

ALL STAFF

All staff members are responsible for:

1. Making sure they understand how to identify and report a suspected or actual security incident.
2. Reporting a suspected or actual security incident to the Incident Handler (preferable) or to another member of the Cyber Security Incident Response Team (CSIRT).
3. Reporting any security related issues or concerns to line management, or to a member of the CSIRT.

Complying with the security policies and procedures of SPENDOLOGY SOLUTIONS. This includes any updated or temporary measures introduced in response to a security incident (For example, for business continuity, incident recovery or to prevent recurrence of an incident).

CONTACT INFORMATION

CSIRT CONTACTS

CSIRT Role	Name	Title	Phone	Email
Executive	Jennifer Crow	CISO/Owner	101-111-0001	jcrow@spendology.org
Incident Handler** Lead	Jennifer Crow	CISO/Owner	101-111-0001	jcrow@spendology.org
Incident Handler Backup	William Cooper	General Manager	101-111-0002	wcooper@spendology.org
Note-Taker	Patrick Coleman	Assistant Manager	101-111-0003	pcoleman@spendology.org
Communications	Susan Jones	PR Associate	101-111-0004	sjones@spendology.org
Network	Lucy Young	Cyber Vendor Ltd.	202-222-0001	lyoung@cyber.org
Desktop	Lucy Young	Cyber Vendor Ltd.	202-222-0001	lyoung@cyber.org
Server	Lucy Young	Cyber Vendor Ltd.	202-222-0001	lyoung@cyber.org
Legal	Theresa Taylor	Legal Firm Ltd.	303-333-0001	ttaylor@legal.org

EXTERNAL CONTACTS

Role	Organization	Name	Title	Phone	Email
Cyber Vendor Support Lead	Cyber Vendor Ltd.	Lucy Young	Support Lead	202-222-0001	lyoung@cyber.org
Lawyer	Legal Firm Ltd.	Theresa Taylor	Lawyer	303-333-0001	ttaylor@legal.org
Cyber Insurance Provider	Insurance Vendor Ltd.	Gerald Stokes	Account Manager	404-444-0001	gstokes@insurance.org
Credit Card Company	Bank Ltd.	John Reid	Client Assistant	505-555-0001	jreid@bank.org
Utility Company	Utilities Ltd.	Tami Green	Client Assistant	606-666-0001	tgreen@utilities.org
Law Enforcement (local)	New York City Police Department	NYPD		911	report@nypd.org
Law Enforcement (federal)	Federal Bureau of Investigation (FBI)	Internet Crime Complaint Center (IC3)			

OTHER STAKEHOLDER CONTACTS

Role	Organization	Name	Title	Phone	Email
Shareholder	Spendology Solutions	Jennifer Crow	CISO/Owner	101-111-0001	jcrow@spendology.org

INCIDENT TYPES

Type	Description
Ransomware	A specific type of malicious code that infects a computer and displays messages demanding a fee be paid in order for the system to work again.
Sensitive Data Leaks	An incident that involves real or suspected loss of personal information.
Malware	Installation of malicious software (i.e., a virus, worm, Trojan, or other code/files).

INCIDENT SEVERITY MATRIX

When CSIRT determines the severity of the incident, they will consider the following:

- Whether a single system is affected or multiple.
- The criticality of the system(s) affected.
- Whether impacting a single person or multiple.
- Whether impacting a single team/department, multiple teams/departments, or the entire organization.

The Incident Handler must consider the relevant business context and what else is happening with the organization at the time to fully understand the impacts and urgency of remedial action.

The CSIRT will consider the available information to determine the known magnitude of impact compared with the estimated size, along with likelihood of the effect spreading and the potential pace of such spread. The CSIRT will determine the potential impacts to the organization, including financial damage, brand and reputational damage, and other types of harm.

The incident may be the result of a sophisticated or unsophisticated threat, an automated or manual attack, or may be nuisance/vandalism.

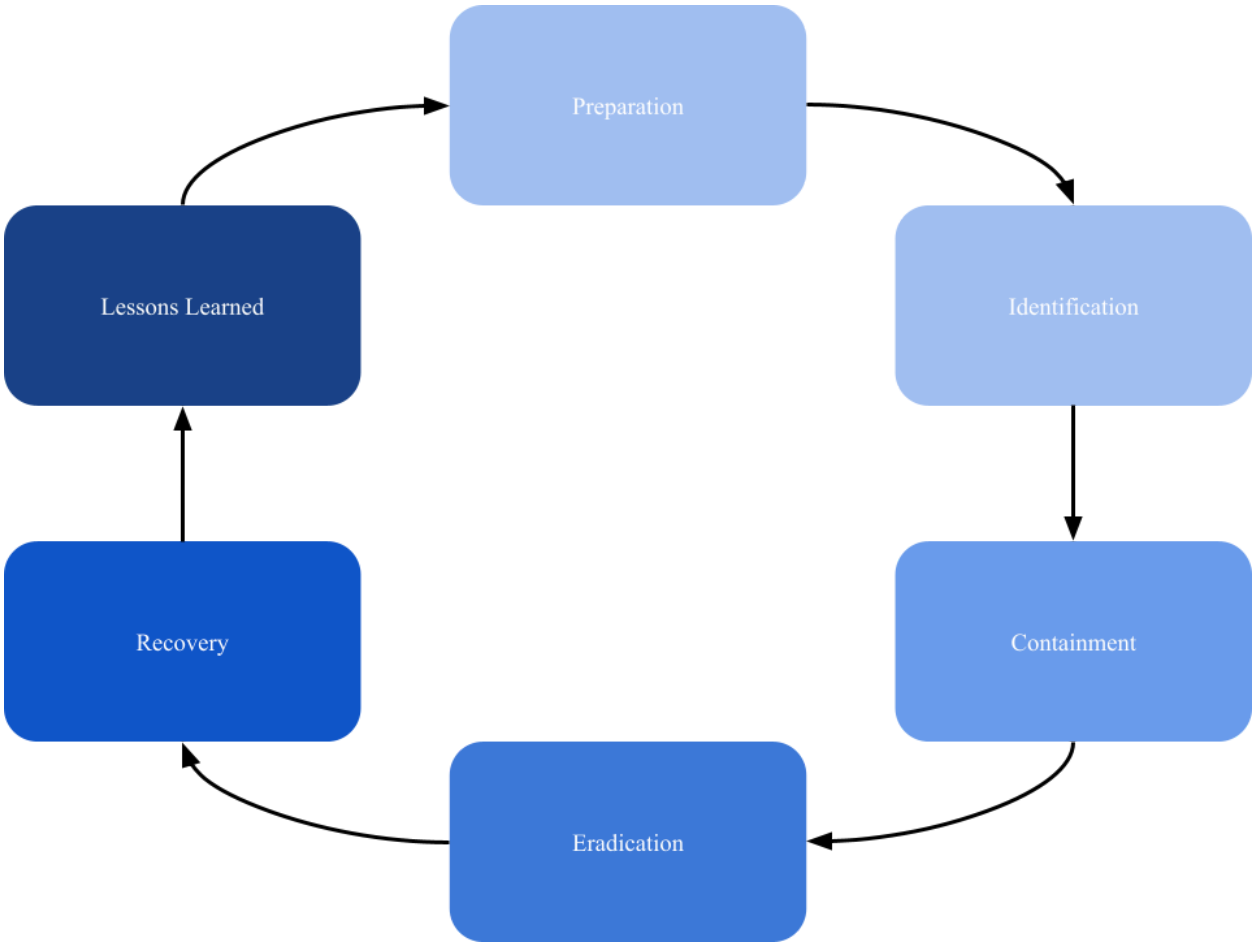
The CSIRT will also determine the following:

- Whether there is evidence of the vulnerability being exploited.
- Whether there is a known patch.
- Whether this is a new threat (for example, zero day) or a known threat.
- The estimated effort to contain the problem.

Category	Indicators	Scope	Action
Critical	Data loss, Malware, Ransomware	Widespread and/or with critical servers or data loss, stolen data, unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
High	Theoretical threat becomes active	Widespread and/or with critical servers or data loss, stolen data, unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
Medium	Email phishing or active spreading infection	Widespread	Implement CSIRT, Incident Response Plan, create Security Incident, Organization-wide
Low	Malware or phishing	Individual host or person	Notify CSIRT, create Cyber Security Incident

INCIDENT HANDLING PROCESS

In the event of a Cyber Security Incident the Cyber Security Incident Response Team will adhere to the PICERL process as follows.



PREPARATION

In preparation for a cyber security incident my organization commits to:

- Build an Incident Response Plan
    - Establish mandate, delegate authority decision making process and chain of command
- Create a soft and hard copy of the Incident Response Plan
- The hard copy of the plan is located at Head Office, on the Office Manager's Desk
- Review/update the incident response plan annually. Record the last revision date on the Revision History section
- Ensure a cyber security incident response team is created
    - Dedicated, virtual, or on-retainer

    - Provide training as necessary
- Document roles and responsibilities
    - Delegate authority
    - Provide training as necessary
- Conduct exercises, drills regularly
    - Consider that most incident types are known in advance
    - Prepare for the known so the CSIRT can focus on the unknown
    - Test the plan, team and tools
- Understand the environment
    - Diagrams, location of critical systems and data
    - Ensure adequate visibility into networks and systems to respond to an incident
    - Vendor environment
    - Understand dependencies
- Understand what controls are in place
    - Are they sufficient to mitigate risk to an acceptable level?
- Understand impacts
    - Determine Maximum Tolerable Downtime (MTD) (max. time a business can be disrupted without causing significant harm) and Acceptable Interruption Window (AIW) (max. time a system can be unavailable)
    - Prioritized list of assets and downtime
- Prepare war room and/or conference bridge(s)
    - Determine and prepare a location to convene, physically or digitally
    - Ensure location is secure and appropriately equipped
- Establish communications plan in advance
- Establish agreements in advance
    - Incident Response Contacts on retainer
    - Ensure annual plan review/update
    - Regular exercises
    - Familiarity with environment in advance
    - Preferred pricing
    - Established service-level agreement (SLA), response times
- Ensure a central point of contact exists for employees to report real or suspected cyber security incidents
- Ensure all employees are required to report cyber security events
    - Information security incidents must be reported, without delay, to the Incident Handler (preferable) or to another member of the Cyber Security Incident Response Team (CSIRT). The member of the CSIRT receiving the report will advise the Incident Response Handler (or the Backup) of the incident

    - In the event that a security incident or data breach is suspected to have occurred, staff member shall discuss their concerns with their line manager, who in turn may raise the issue with a member of the CSIRT
- Ensure all employees know they are required to report cyber security incidents and how
- Ensure all employees report cyber security incidents in a timely fashion

IDENTIFICATION

In the event that a cyber security incident is identified, my organization commits to:

- Bring together those who are aware of the incident
- Engage Cyber Security Incident Response Team members
- Remind all with responsibility to maintain need-to-know
    - Failure to do so leads to managing misinformation
- Communicate effectively and efficiently
- Convene in war room or conference bridges
    - Ensure location is secure and appropriately equipped
- Often more than one location is required for different needs (for example, the management and technical team)
- CSIRT to investigate and determine whether an incident has occurred
    - Is it an event or an incident?
    - Search for correlating information to increase confidence there is a real incident
- Perform triage and ensure common understanding of how it was detected and who is aware
- Analyze the precursors and indicators
- Perform research (for example, search engines, knowledge base)
- Document the investigation and evidence gathering
- Prioritize handling of incidents based on relevant factors (functional impact, information impact, recoverability effort, etc.)
    - Please execute special response steps, if the following cyber security incidents are confirmed. Please consult the sections below for each specific incident type
- Determine severity, urgency and initial impact
- Review information and actions taken to date
- Report incident to appropriate internal personnel and external organizations

CONTAINMENT

In the event of a cyber incident my organization commits to:

- Invoke a communications plan respecting need-to-know

- Develop stakeholder relationship map, to determine the level of stakeholder involvement
- Ensure reported information is factual based on evidence available at the time
- Ensure a point of contact knows the current status at all times
- Implement incident response playbook
- Prevent further damage by containing the incident
- Determine the source, what vulnerability was exploited and implement repairs
- Continue impact/damage assessment and confirm the scope of the incident
- Determine what was changed (for example, files, connections, processes, accounts, access)
- Acquire, preserve, secure and document evidence and preserve the chain of custody
- Continue taking notes, ensuring a detailed log about what was found and what you did about it

For additional assistance:

- In the event that CSIRT requires help in containment, contact Network Security Vendor Support Lead or Helpdesk (see External Contact List). They will help with additional expertise.

ERADICATION

In the event of a cyber incident my organization commits to:

- Eradicate the incident
- Remove all traces of the infection or other incident
    - Identify and mitigate all vulnerabilities that were exploited
    - Remove malware, inappropriate materials, and other components
- If more affected hosts are discovered (for example, new malware infections), perform the identification steps on the newly identified examples, then contain
- Ensure the incident cannot re-occur
- Further understand the attack method and exploited vulnerabilities
- Continue taking notes, ensuring a detailed log
- Ensure any compromised machines are removed or formatted before placing back into service
    - Ensure necessary evidence has been collected

For additional assistance:

- In the event that the CSIRT requires help in eradication, contact Network Security Vendor Support Lead or Helpdesk (see External Contact List). They will provide additional help and expertise

RECOVERY

In the event of a cyber incident my organization commits to:

- Return affected systems to an operationally ready state one by one
- Monitor closely to ensure incident does not re-occur and is not still ongoing
- Ensure systems are restored from a trusted source
- Confirm the affected systems are functioning normally
- Implement additional monitoring to look for future related activity if necessary
- If necessary, contact cyber security insurance company to file a claim

For additional assistance:

- In the event that the CSIRT requires help in recovery, contact Network Security Vendor Support Lead or Helpdesk (see External Contact List). They will provide additional help and expertise

LESSONS LEARNED

In the event of a cyber security incident my organization commits to:

- Hold a meeting to discuss lessons learned within 2 weeks
- Create a follow up report
- Walk through and review play-by-play of incident report
    - How the incident was detected, by whom, and when
    - Scope and severity of incident
    - Methods used in containment and eradication
- Identify opportunities for improvement to better prepare for next time
- Ensure accountability to follow up on identified opportunities for improvement

* Multiple sources including NIST Special Publication 800-61 revision 2 and SANS

INCIDENT-SPECIFIC HANDLING PROCESS

RANSOMWARE

If CSIRT investigations confirm that a Ransomware security incident has occurred, please execute to the following additional steps:

1. Disconnect devices identified with ransomware from the network immediately
2. Examine the ransomware and establish how it infected the device. This will help you to understand how to remove it from the device
3. Contact local authorities to report the incident and cooperate with their investigation
4. Once the ransomware has been removed, a full system scan must be performed using the most up-to-date anti-virus, anti-malware, and any other security software available, to verify it has been removed from the device
5. If the ransomware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by malware
6. If data is critical and must be restored, but cannot be retrieved from unaffected backups, search available decryptors from nomoreransom.org
7. If there are no backups or decryptors available, contact the Ransomware Decryption Vendor in the External Contact list. Our company policy is to never pay the ransom even if it means permanent data loss
8. Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack

SENSITIVE DATA LEAKS

If CSIRT investigations confirm that a Sensitive Data Leak security incident has occurred, please execute to the following additional steps:

1. Determine the source of the breach and how access was gained to retrieve sensitive data.
    a. If the leak is suspected to have occurred by the theft of a device with access to company data, initiate remote wipe or remote lock capabilities where available.
2. Once the source is found, contain the incident by disconnecting it or isolating it.
    a. It is important to not shut down any affected machines in any effort to contain the incident. This may result in the loss of data which may be crucial in a forensic investigation of the incident.
3. Maintain continuous monitoring activities to ensure that the threat has been eradicated.
4. Scan various sources to see if the sensitive data, leaked in the breach, is posted or sold online.
5. Review and update access policies and controls to prevent future leaks.

6. Notify any parties affected or concerned by the leak. This could include, but is not limited to, users, employees, and stakeholders.
    a. Contact the legal department.
    b. File a report with the Internet Crime Complaint Center (IC3).
    c. If credit card data was stolen during the incident, contact the Credit Card Company (see External Contacts list).

MALWARE

If CSIRT investigations confirm that a Malware security incident has occurred, please execute to the following additional steps:

1. Identify the affected system and isolate and disconnect it from the network to prevent it from spreading.
    a. This includes shutting down Personal Area Networks (e.g. Bluetooth) to minimize the spread of malware.
2. Identify how the malware affected the system to determine how to remove it properly.
3. Restore the affected data from backups after verifying that the backup data is free of malware.
4. If the backup data is infected with malware, return to step 2 to remove it so that the data can still be restored.
5. Investigate the impact of the malware and communicate this, and any other relevant information, with necessary parties that might have been affected or who can help contain, eradicate, and recover.

REFERENCES

- Bright Minds Learning Center IRP
    - https://docs.google.com/document/d/1MvPxQaRxBZQULT1kpIyUDM86-Y414gYF/edit
- Federal Bureau of Investigations: Internet Crime Complaint Center
    - https://www.ic3.gov/
- NIST Special Publication 800-184: “Guide for Cybersecurity Event Recovery”
    - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
- CIS Controls Mobile Companion Guide
    - https://www.cisecurity.org/insights/white-papers/cis-controls-mobile-companion-guide-2