Cyber Incident Response Plan

Template

City of St. Paul, Minnesota

Table of contents

Plan Approvals

By their signatures below, the following senior-level officials certify that they approve this Cyber Incident Response Plan (CIRP) and fully understand the incident response procedures that are to be followed in the event of a cyber incident.

Approved:

_____ _____
Name/Title Date

Approved:

_____ _____
Name/Title Date

Approved:

_____ _____
Name/Title Date

A. Introduction

This Cybersecurity Incident Response Plan (CIRP) template for the City of St. Paul was developed by a Working Group representing different departments/disciplines of the City. The purpose of this CIRP is to help different departments and stakeholders of the City of St. Paul with operational resilience and specifically with cybersecurity incident response. This template could be applied and modified for any of the departments of the City.

Cyber incidents are events that occur on or are conducted through a computer network which then compromise integrity, confidentiality, and/or availability of computers. They may jeopardize communication and/or information systems and networks, virtual and/or physical infrastructure controlled by computers, and information residing on a network. Cyber incidents may or may not have a malicious intent.

The following activities are usually recognized as security policy breaches are:

- Attempts to access non-authorized systems and/or its data,
- Malicious or accidental disruption and/or denial of service,
- Unauthorized use of system for processing or storing of data, and
- Unauthorized changes to system firmware, software, or hardware.

Cyber Incident Response Lines of Efforts

The dependence on cyber in today's world, requires that the public as well the private sector exhibit heightened vigilance in managing, responding to, investigating cyber incidents, and sharing lessons learned. Partners and stakeholders can minimize the potential damage to their information systems and data with cooperation and shared intelligence.

Ensuring unity of effort during incident response requires a shared understanding of roles and responsibilities for all participating departments/agencies throughout the cyber incident lifecycle.

The four lines of effort that drive cyber incident response are:

- Threat Response,
- Asset Response,
- Intelligence Support, and
- Affected Entity Response.

These concurrent lines of effort provide the foundation that is required to synchronize the various response objectives before, during and after a cyber incident.

The table below describes each of the four Lines of Effort and associates them with entities/organizations associated with the efforts:

Table A - 1

Lines of Effort	Description	Associated Entities
Threat Response	Threat response activities include the appropriate law enforcement investigative activities for: ▪ Collecting evidence and gathering intelligence to provide attribution; ▪ Linking related incidents and identifying additional possible affected entities; ▪ Identifying threat pursuit and disruption opportunities; and ▪ Developing and executing courses of action to mitigate the immediate threat and facilitating information sharing and coordination with asset response efforts.	▪ Local Law Enforcement ▪ Fusion Center ▪ Minnesota IT Services (MNIT) ▪ Federal Bureau of Investigations (FBI) - Cyber Division ▪ Metro State University – MN Cyber Institute ▪ League of Minnesota Cities – Cybersecurity Services
Asset Response	Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents by: ▪ Identifying other entities possibly at risk and assessing their risk to the same or similar vulnerabilities; ▪ Assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; ▪ Facilitating information sharing and operational coordination with threat response; and ▪ Providing guidance on how best to utilize resources and capabilities in a timely, effective manner to speed recovery.	▪ Minnesota IT Services (MNIT) ▪ Metro State University – MN Cyber Institute ▪ League of Minnesota Cities – Cybersecurity Services ▪ U.S. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (DHS CISA)
Intelligence	Intelligence support facilitates the building of situational threat awareness and sharing of related intelligence to: ▪ Create an integrated analysis of threat tactics, techniques, and procedures; ▪ Identify and assist with the mitigation of knowledge gaps; and ▪ Suggest methods to degrade or mitigate adversary threat capabilities. ▪ Share indicators of compromise with other potential victims to increase their defense posture	▪ FBI Cyber Division ▪ Minnesota IT Services (MNIT) ▪ Metro State University – MN Cyber Institute ▪ MN BCA
Affected Entity Response	▪ An affected entity is highly encouraged to share information surrounding the event with other cybersecurity specialists. This will assist the effective cyber incident response. The affected entity is the data owner and retains responsibility to ensure appropriate actions and safeguards are in place to remediate threats and secure their information.	▪ CISO ▪ Information technology (IT) staff ▪ Management teams ▪ Cybersecurity operations staff

Incident Response Life Cycle

This CIRP describes protocols, procedures, and actions an organization should perform as a part of cyber incident response. They are based on the "System Administration, Audit, Network, and Security (SANS)" Institute (industry) standardized response steps of "Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned."

This St. Paul CIRP actions and procedures fall into seven general stages:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activity

Each of the seven phases of cyber incident response have a dedicated chapter in this CIRP. Each chapter will describe the actions that comprise each stage and identify the personnel responsible for completing each action.

A Cyber Incident Response Checklist can be found in Appendix A. It consists of a list of sequential actions to be accomplished in the response stages of Detection, Analysis, Containment, and Eradication.

B. Maintenance of this Cyber Incident Response Plan (CIRP)

The Cyber Incident Response Plan (CIRP) CIRP will be reviewed and updated at least annually, but also at any time a major system update or upgrade is performed, and of course after a cyber incident has been responded to.
A member of the Cyber Incident Response Team (CIRT) will be assigned the responsibility for updating the plan. They will request information and updates from other members of the CIRT, other employees and departments in order to complete this task.

At a minimum, the maintenance of the CIRP will consist of the following:

- Ensuring that all team lists are complete and up to date;
- Making any required updates to directions and guidance to reflect changes in policies, personnel, priorities, and IT systems and equipment;
- Ensuring that the plan is compliant with all requirements specified in new laws or regulations;
- Ensuring that all points of contact for CIRT members are current.

C. Cyber Incident Response Team (CIRT)

Pre-identification of the necessary roles to be filled during an incident response and the designation of individuals with the required knowledge and skill sets is important. These individuals should always be available to respond to an incident. A single individual may perform several roles concurrently. Not all roles may be required to be activated for each incident and specific incident response requirements will dictate which roles are necessary.

The structure of the Cyber Incident Response Team (CIRT) mirrors the Incident Command System (ICS) and consist of Command Staff (Incident Commander and four command staff positions) and General Staff comprised of five functional areas (Management, Network, Database, Platform, and Application). Each Command and General Staff position is described here below together with pre-identified individuals and their points of contact (POC), including alternates.

Command Staff

Table C - 1

Role	Description	Point of Contact by Position Title
Incident Commander	Has authority to make high-level decisions and approve actions to be taken by the Incident Response Team.	……
Information Officer	Disseminates public and non-sensitive information to interested parties.	……
External Liaison Officer	Serves as the point of contact for other governmental and non-governmental agencies and organizations	……
Safety Officer (ISO)	Monitors incident operations and advises on matters related to operational safety	……
Legal Counsel	Advises incident command on legal matters	……

General Staff - Management

Responsible for the functional aspects of the incident command structure.

Table C - 2

Role	Description	Point of Contact by Position Title
Operations Chief - and Deputy	Directly manages all incident tactical activities	……
Deputy Operations Chief	Assists in managing all incident tactical activities	……
Lead Investigator	Gathers and analyzes technical evidence, determines the cause of the attack, and directs other analysts and IT components to implement system and service	……

Assistant Investigator	Assists Lead Investigator in her/his response role and activities	……..

General Staff - Network Group

Responsible for functional aspects of network management.

Table C - 3

Role	Description	Point of Contact by Position Title
Network Group Supervisor	Oversees Network Group team members	……..
Network Subject-Matter Experts (SMEs)	Persons with experience and authorization necessary to manage affected local area networks and firewalls	……..
Firewall Engineers	Designs, builds, and manages the security infrastructure of IT systems	……..

General Staff - Database Group

Responsible for functional aspects of database systems.

Table C - 4

Role	Description	Point of Contact by Position Title
Database Group Supervisor	Oversees Database Group team members	……..
Database SMEs	Person(s) with experience and authorization necessary to manage affected database systems	……..

General Staff - Platform Group

Responsible for functional aspects of server and workstation platforms.

Table C - 5

Role	Description	Point of Contact by Position Title
Platform Group Supervisor	Oversees Platform Group team members	……..
Server Platform SMEs	Person(s) with experience and authorization necessary to manage affected server platforms	……..
Workstation Platform SMEs	Person(s) with experience and authorization necessary to manage affected workstation platforms	……..

General Staff - Application Group

Responsible for functional aspects of server and client applications.

Table C - 6

Role	Description	Point of Contact by Position Title
Application Group Supervisor	Oversees Application Group team members	……..
Web Application SMEs	Person(s) with experience and authorization necessary to manage affected web server applications	……..
Management Application SMEs	Person(s) with experience and authorization necessary to manage affected management information systems	……..
Desktop Application SMEs	Person(s) with experience and authorization necessary to manage affected workstation-based applications	……..

D. Lifecycle Stage One: PREPARATION

Preparation and planning for the Cyber Incident Response Team (CIRT) begins with the development of this CIRP in concert with other plans of the City's - e.g., Continuity of Operations Plan (COOP) and Continuity of Government Plans (COG). This preparation phase includes IT-specific training and exercising any potentially participating, collaborating, and cooperating cyber incident response personnel. It should also include relevant courses in the NIMS (National Incident Management System) and the ICS (Incident Command System).

The CIRT could also be utilizing outside resources to augment its CIRT, or it could completely outsource the cyber incident response. If this were the case, the third-party organization would be pre-identified and contracted per existing protocol and procedures. Ideally, such an arrangement would be in place before any cyber incident will occur and it would be based on a Service Level Agreement (SLA). That would grant the vendor engagement in/with St. Paul City's IT infrastructure and involvement in the testing of its CIRP.

Training for the CIRT:

The following "non-cyber" training courses are recommended for members of the CIRT:

- Command Staff – ICS 100, 200, 300, G-191 (or G-2200 or G-2300)
- General Staff – Management ICS 100, 200, 300
- Other General Staff – ICS 100, 200
- Other?

The following "Cyber" training is recommended for all members of the CIRT:

- AWR 376 – Understanding Targeted Cyber Attacks
- MGT 452 – Physical and Cybersecurity for Critical Infrastructure
- Other?

External resources:

Many times, external resources are as important as internal resources. Therefore, keeping and updated and comprehensive list of external partner agencies to ensure regular communication is key to establishing and managing effective partnerships, to foster open information sharing, and to facilitate support during a cyber threat/response.

Table D - 1

External Resource Organization	Point of Contact Email	Point of Contact Phone
Federal Bureau of Investigations (FBI) - Cyber Division		
Minnesota IT Services (MNIT)		
Minnesota Fusion Center		
League of Minnesota Cities – Cybersecurity Services		
Metro State University – MN Cyber Institute		
CISA Integrated Operations Coordination Center		
Multi-State Information Sharing and Analysis Center (MS-ISAC)		

Personnel Roster – St. Paul's Cyber Incident Response Team (CIRT)

In case of an actual or suspected cyber incident the individual CIRT members must be expeditiously and reliably contacted and mobilized. The previous chapter - "Incident Response Team" - listed the CIRT positions, described their roles, and included each member's email address and phone number.

Activation / mobilization of the CIRT will be accomplished using technology, such as the "Everbridge" alerting system. However, an old-style "calling tree" process could and should serve as a "fallback contingency" should technology be unavailable.

E. Lifecycle Stage Two: DETECTION

Early detection of deviations from normal operations, verification of such deviations, and identification of as a security incident is critical. It is important to expeditiously determine and execute containment and eradication of such incidents.

Vigilance can be enhanced by using a multitude of information sources to determine the existence and threat of cyber incidents. Aside from monitoring only inside sources, hazard and threat information may also be obtained from outside the organization. A list of cyber incident indicators including their likely sources paired with internal monitoring assignments are listed here below:

Table E - 1

Indicator	Likely Source	Monitoring Assigned To
Alerts from Monitoring and Detection Systems	• Intrusion Detection and Prevention Systems (IDS/IPS) • Security Information and Event Management (SIEM) and antivirus software and third-party monitoring system or service • Vulnerability assessment platforms	Primary …. Alternate ….
Logs	• Operating Systems (OS) • Applications • Web Servers • Network devices network monitoring system	Primary …. Alternate ….
Users	• Internal or external users, including non-IT or security-related staff • Customers can report possible incidents to the CIRT directly	Primary …. Alternate ….
Internal Teams	• IT Departments • IT Help Desks • CIRTs • Staff that may detect anomalies during their daily work	Primary …. Alternate ….
Managed Service Providers	• Internet Service Providers (ISP) • Telecommunication Service Providers • Suppliers	Primary …. Alternate ….
Mass Media	• Newspapers • Television • Social Media	Primary …. Alternate ….
Website	• Public security information websites • Websites by security researchers • Defacement archive websites	Primary …. Alternate ….

The characteristics of various cyber events, incidents, and attacks will determine the type of triage methodologies and what levels of response escalation need to be executed. Here below is a suggested list of most common incident characteristics, a brief description thereof, possible exploring methodologies, and suggested assignments to members of the CIRT.

Table E - 2

Characteristics	Description	Exploratory Method	CIRT Responsibility
Authentication	Unusual or unauthorized logon attempts, logon activities after hours, remote session attempts, unauthorized privilege escalation, etc.	Review of the logs to understand the account in question and reason for error and advise the Information Security Officer (ISO)	Primary …. Alternate ….
Data Handling	Abnormal ad-hoc requests, unauthorized access or attempted access, inappropriate disclosure, inappropriate destruction of sensitive data, etc.	Review the logs to understand the nature of the requests – could simply be the case of user rights management issues or it could lead to an investigation.	Primary …. Alternate ….

Data Exfiltration	Large amounts of data leaving the network by an authorized (or unauthorized) user.	May immediately cease all applicable activities related to the incident in question, secure workstation(s) or area and contact the appropriate ISO to begin preserving the information or evidence of questionable activities. Do not turn off power to the device to allow conduct of forensics.	Primary …. Alternate ….
System Availability	Web defacements, denial of services, hacking activities, modification of software or systems, suspicious activities	Review logs to understand the activity in question and prepare to restore services from a backup and actively review firewall logs.	Primary …. Alternate ….
Physical	Power outages, physical damage, sabotage, physical loss or theft of information or systems	Coordinate with the ISO and facility services to understand the nature of the event and understand how to implement secondary power and possibly provide security personnel to protect the physical perimeter and sensitive areas.	Primary …. Alternate ….
Other	Social engineering, Trojan or virus infections, harassment, elevated data disclosure, improper disposal of documents.	Disable the user account, take a screenshot and turn in, unplug the computer from the network, actively log authentication and access actions, etc.	Primary …. Alternate ….

F. Lifecycle Stage Three: ANALYSIS

During this stage resources should be assigned to investigate the incident. Analysis should determine the incident type and its scope, and assess which networks / systems / applications are affected, who or what originated the incident, and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited).

Immediately after the determination that a cyber incident has occurred the CIRT will initiate an investigation of the incident, which will include a threat and impact analysis in order to categorize the impact of the event on the organization.

Cyber Incident Types

A cyber incident can be defined as any security related event that has an actual or potential adverse effect on any computing resource or the data contained therein, or the violation of an explicit or implied security policy. Incidents could be classified according to the five criteria listed above and any incident may fit more than one type.

Table F - 1

Incident Type	Description
Denial of Service	An incident by which authorized access to systems or data is prevented or impaired. Usually a denial of service (DoS) incident is a security event if the DoS is due to malicious intent. Not all events that prevent or hinder authorized access to systems or data are security incidents. The mechanical, electrical, or administrative failure of a system or access mechanism may not be a security incident.

Unauthorized Access	An incident where unauthorized access is attempted or gained to systems or data, such as a phising attack. This access can be logical or physical in nature. Unauthorized access is any access for which permission has not been granted. Such permissions would include connect, authenticate, read, write, create, delete, modify, etc. This unauthorized access can be by an individual or another system.
Inappropriate Usage	An incident by which acceptable use policies are violated. Acceptable use policies may include what types of data may be accessed or transmitted, how information may be accessed or transmitted, and where information may be received from or transmitted to.

While incident types could be categorized more granularly, most types seem to fall into one of the above listed three incident types.

Analyzing Impact and Overall Severity

Categorization of impacts may be identified as:

- Functional Impacts - affecting confidentiality, integrity, and availability of the organization's information
- Information Impact - affecting the confidentiality, integrity, and availability of information
- Recovery Impact - affecting the amount of time and resources spent on recovering (depends on the size of the incident and the type of resources needed to recover)

These three impact categories can be evaluated and qualified as to their impact levels ranging from "no impact" to "high/severe impact."

Additionally, the incident severity can be scored and quantified for five criteria, i.e.:

- Potential number of affected parties
- Probability of widespread escalation
- Past history of similar incident
- Potential damage and/or loss
- Business impact

Both, the qualitative impact analysis and the quantitative determination of the overall incident severity should be used by the CIRT during the "Analysis" stage of the Incident Response Life Cycle. The CIRT can use the attached "Incident Analysis Checklist" in Appendix B to prioritize the incident according to its severity level. Dependent on the severity rating of the incident, timelines for initial response actions can then be established.

G. Lifecycle Stage Four: CONTAINMENT

Following detection and analysis, the incident will need to be contained in order to minimize continued impact and/or disruption of services and to reduce the possibility of continued contamination of other services. Tactical response efforts supporting the immediate local isolation and containment are vital to slowing, and hopefully stopping the proliferation of the attack.

The CIRT will strategically address risk at every level, starting with the infected computing device all the way to examining the viability of the complete network. Any affected computing devices may require

immediate isolation or removal from the network in order to support the necessary response efforts. Some commonly employed network tactics involve disconnecting or isolating network segments, creating additional firewall rules, following active guidelines from intrusion detection/prevention systems, or simply disconnecting the infected workstations or server from the network(s).

Key strategic components of "Containment" are:

- Short-term containment - limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production server and routing to failover.
- System backup - taking a forensic image of the affected system(s) and only then wipe and reimage the systems. This will preserve evidence from the attack that can be used in court, and also for further investigation of the incident and lessons learned.
- Long-term containment - applying temporarily fixes to make it possible to bring systems back up. The primary focus is removing accounts or backdoors left by attackers on the systems, and addressing the root cause - for example, fixing a broken authentication mechanism or patching a vulnerability that led to the attack.

Based on the type of incident, the CIRT will employ tactical containment operations. Also, depending on the overall incident severity (as determined during the Analysis stage), goals for containment timelines are established. In cases where multiple incidents are occurring simultaneously or in close succession, containment of those incidents that will cause the most serious impacts to mission performance will be prioritized over less severe incidents.

H. Lifecycle Stage Five: ERADICATION

Based on locating and eliminating the root cause of the breach, the goal of Eradication is to actually remove malware or other artifacts introduced by the attacks and to fully restore all affected systems. After the Detection, Analysis, and Containment of an incident, the CIRT can determine how to effectively and safely remove the source of the incident from the computing device and how to protect the network from being affected in the future.

The Eradication process must include measures to not only remove the infection from the primary device but to utilize various methods to scan every device on the affected network segment and thus ensure the relevant risk is addressed. This step should take place after all external and internal actions are completed. There are two important aspects of eradication: cleanup and notification. Cleanup typically consists of running antivirus software, uninstalling the infected software, rebuilding the operating system, and/or replacing the entire hard drive and reconstructing the network.

This sample checklist identifies several considerations that could guide the eradication process and it lists specific members of the CIRT to address these:

Table H - 1

Eradication Consideration	CIRT Responsibility
Have infected systems been hardened with new patches or updates?	Primary …. Alternate ….
Do any systems or applications need to be reconfigured?	Primary …. Alternate ….
Have all possible entry points been reviewed and closed up?	Primary …. Alternate ….

Have all processes to eradicate the threat(s) been covered?	Primary …. Alternate ….
Are any additional defenses needed to support the eradication of the threat(s)?	Primary …. Alternate ….
Has all malicious activity been eradicated from affected systems?	Primary …. Alternate ….

Key components and actions during the Eradication phase are accomplished by members of the CIRT. A recommended order of these components to be implemented by the CIRT is here below.

Table H - 2

Component	Description	CIRT Responsibility
Re-imaging	Complete wipe and re-image of affected system hard drives to ensure any malicious content is removed.	Primary …. Alternate ….
Preventing the root cause	Full understanding of what caused the incident, preventing future compromise, for example by patching a vulnerability exploited by the attacker.	Primary …. Alternate ….
Applying basic security	Example: upgrading old software versions and disabling unused services.	Primary …. Alternate ….
Scan for malware	Use of anti-malware software, or Next-Generation Antivirus to scan affected systems and ensure all malicious content is removed.	Primary …. Alternate ….

I. Lifecycle Stage Six: RECOVERY

Because our technological environments are so dynamic and because multiple platforms are utilized for information management, the CIRT focuses now on data recovery, service recovery, and site recovery in order to resume normal operations as soon as possible. The sooner the CIRT is able to start these necessary recovery activities, the shorter this recovery stage will be, and the quicker mission-critical operations can be fully re-established.

Data Recovery

The key to an effective data recovery strategy begins with a well planned and executed backup strategy. A back-up strategy based on the data type, location, sensitivity, availability requirements, and/or who owns the data. Clear contractual agreements (e.g., Scopes of Work) should exist if the backup media are located externally possibly with an external data recovery vendor.

Service Recovery

If this recovery relies on third-party services during normal operations, then those vendors will also play an important role during technology recovery after an incident.

Site Recovery

The actions required for site recovery are based on the type of recovery site, e.g., cold site, warm site, or hot site.

Consideration should also be given to establish a dedicated Recovery Committee to address concerns and topics such as confidentially agreements, non-disclosure agreements, potential legal issues, and possibly needed changes or additions to current policies regarding cyber security.

J. Lifecycle Stage Seven: POST-INCIDENT ACTIVITY

Following an incident, the St. Paul CIRT should perform "After Action" activities, such as facilitating a "Hotwash" of all involved response participants while all event details are still fresh in their memory. Additional "Lessons Learned" meetings help set the stage for improving security measures and the incident handling processes, determining the root cause of a cyber incident, and identifying recommendations and any shortfalls notified during the incident response process.

Questions to be brought up and attempted to be answered in these meetings include:

- How well did staff and management perform?
- Were documented procedures followed? Were procedures adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators will be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Root Cause Analysis

A root cause is a fundamental, underlying, system-related reason why an incident occurred, and it will enable the identification of one or more correctable system failures. By conducting a root cause analysis following a cyber incident and addressing the root causes, St. Paul may be able to substantially or completely prevent the same or a similar incident from occurring in the future.

The CIRT's Incident Commander or Operations Chief should lead the root cause analysis and facilitate the review of logs, forms, reports, and other incident documentation. When doing so, the focus should be on:

- Identifying recorded precursors and indicators;
- Determining if the incident caused damage before it was detected;
- Determining if the actual cause of the incident was identified;
- Determining if the incident is a recurrence of a previous incident;
- Identifying measures, if any, that could have prevented the incident.

Recommendations

It is “Best Practice” to assemble an After-Action Report (AAR) based on information gleaned from the post-incident activities listed above. Such an AAR usually ends with an “Improvement Plan” (IP) that identifies specific improvements that can be made to fix deficiencies and to make incident response actions that worked well even more successful. AAR/IPs may trigger a possibly needed update of this CIRP, conducting additional training for the CIRT, and sharing information with cybersecurity partners for them to use as lessons learned. The listed items in the “Improvement Plan” will identify responsibilities and benchmarks for implementation of the recommendations. It is recommended that AAR/IPs should be completed within 4-6 weeks of the resolution of an incident.

Appendix A:

Incident Response Checklist

This Appendix presents a sequential list of sample tasks that should be addressed and/or performed during the incident response by the Cyber Incident Response Team (CIRT). Based on resources, staff, procedures, protocols, and priorities this list should be expanded and tailored to the requirements of individual departments within the jurisdiction of St. Paul.

In an actual incident, some of the listed tasks may be performed before this list suggests that they should be performed.

Table Appendix A - 1

Step	Needed Action	Responsibility	Completed
1.	Detection		
1.1	Report signs of a security incident to the CISO	Data Base Supervisor	O
1.2	Performs an initial assessment to determine source of cyber threat	Lead Investigator	O
1.3	….. additional Actions as needed……..		O
2.	Analysis		
2.1	Begin steps for evidence preservation and containment	Lead Investigator	O
2.2	Perform detailed impact analysis to properly prioritize additional response activities that may be required	Network Subject-Matter Experts (SMEs)	O
2.3	….. additional Actions as needed……..		O
3.	Containment		
3.1	Document evidence from the incident	Lead Investigator	O
3.2	Complete a full system shutdown	Operations Chief	O
3.3	….. additional Actions as needed……..		O
4.	Eradication		
4.1	Identify and prioritize vulnerabilities for mitigation	Operations Chief	O
4.2	Remove malware, inappropriate materials, and other components	Database SMEs	O
4.3	….. additional Actions as needed……..		O

Appendix B:

Incident Analysis Worksheet

This Incident Analysis Worksheet may be used by the Cyber Incident Response Team (CIRT) to document an incident, categorize its impacts, and ultimately calculate its severity. Once the incident is categorized it is prioritized according to its severity level and the appropriate response may be implemented.

Incident Overview

In order to accurately identify incident impacts, identify the incident type (e.g., Denial of Service, Unauthorized Access, etc.) and enter description the incident here:

Table Appendix B - 1

Incident Type	Description of the Incident
e.g., Denial of Service, Unauthorized Access, etc.	Brief description of what occurred

Functional Impacts

Incidents may affect the confidentiality, integrity, and availability of information. Classify the incident's functional impact as None, Low, Medium, or High here:

Table Appendix B - 2

Category	Description
None	No effect to the organization's ability to provide all services to all users.
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide more than one critical service to any users.
Functional Impact Category	*Add here the category relevant for this incident*

Information Impact

Classify the impact of the incident as None, Privacy Breach, Proprietary Breach, or Integrity Loss here:

Table Appendix B - 3

Category	Description
None	No information was exfiltrated/leaked, disclosed, changed, deleted, accessed, or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Privacy Breach	Sensitive PII of taxpayers, employees, beneficiaries, etc., was accessed or exfiltrated/leaked, or Protected Health Information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Proprietary Breach	Unclassified proprietary information, such as PCII, was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes.
Integrity Loss	Sensitive or proprietary information was changed or deleted accidentally or intentionally.
Information Impact Category	*Add here the category relevant for this incident*

Recovery Impact

The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. Classify the recoverability impact of the incident here:

Table Appendix B - 4

Category	Description
Regular	Time to recovery is predictable with existing resources.
Supplemented	Time to recovery is predictable with additional resources.
Extended	Time to recovery is unpredictable; additional resources and outside help are needed.
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly); launch investigation.
Recovery Impact Category	*Add here the category relevant for this incident*

Summary of Overall Impact Severity

A severity rating can be established by adding the scores for the evaluation criteria listed in the table below:

Table Appendix B - 5

ACTION	SCORE
Potential number of affected parties: How much productivity is impacted by this incident?	
Less than 1% of systems; less than 1% of workforce	1
More than 1%, but less than 10% of systems; more than 1% but less than 10% of workforce	2
More than 10% of systems; more than 10% of workforce	3
Probability of widespread escalation: Potential for incident to spread to as yet unaffected systems?	
Minimal	1
Moderate	2
High	3
Commonality: Has this occurred in the past; is there experience in mitigating this particular incident?	
Commonly Seen	1
Occasionally Happens	2
Rare	3
Potential for damage / loss: Expected cost of the incident- both in lost production and in mitigation costs.	
Minimal	1
Moderate	2
High	3
Business impact: Expected negative impact on the overall health of the enterprise both in short- and long-term	
Minimal	1
Moderate	2
High	3

Once the analyses described above are complete, it is possible to prioritize the incident according to its severity level. The appropriate response to an incident is dependent on the severity rating of the incident. The table below describes the four levels of severity and identifies the timelines for initial action for incidents at each severity level.

Table Appendix B - 6

Priority Guideline	Cumulative Severity Score	Suggested Initial Action
Severe: Extreme impact on enterprise	13 – 15	Immediately
High: Loss of a major service	11 – 12	Immediately
Medium: Some impact some portion of enterprise	8 – 10	Within 4 hours
Low: Minor impact on a small portion of enterprise	5 - 7	Within 24 hours
Incident Severity Score	*Enter Overall Severity Score for this Incident*	

Appendix C:

Acronyms

Table Appendix C - 1

Acronym	Definition
AAR	After Action Report
AAR/IP	After Action Report / Improvement Report
CIRP	Cyber Incident Response Plan
CIRT	Cyber Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COG	Continuity of Government
COOP	Continuity of Operations Plan
DHS	U.S. Department of Homeland Security
DoS	Denial of Service
FBI	Federal Bureau of Investigation
ICS	Incident Command System
IP	Improvement Plan
ISO	Incident Safety Officer
ISP	Internet Service Providers(s)
IT	Information Technology
MN BCA	Minnesota Bureau of Criminal Apprehension
MNIT	Minnesota IT Services
MS-ISAC	Multi-State Information Sharing & Analysis Center
NIMS	National Incident Management System
OS	Operating System
PCII	Protected Critical Infrastructure Information
POC	Point(s) of Contact
SANS	System Administration, Audit, Network, and Security
SME	Subject Matter Expert(s)