OrganiZation Name

Incident Response Plan

DISCLAIMER

*CyberSecure Canada has developed this template for your use in relation to certification requirements for the Develop an Incident Response Plan security control area. It provides guidance as to how information can be organized and documented for certification. CyberSecure Canada does not guarantee a successful certification from use of this template. Organizations are not obliged to use this template and may provide the certification requirement(s) in a documented format best suited for them.*

# Template Instructions

*The purpose of this template is to help users in meeting the certification requirements for the* ***Develop An Incident Response Plan*** *security control area of CyberSecure Canada.*

*Instructions are provided in blue font within each section of this template. Upon completion of the template, delete these instructions.*

*It is recommended that users review the eLearning module* ***Develop An Incident Response Plan*** *and the completed example of an* ***Incident Response Plan.***

# Table of Contents

[Revision History 4](#_Toc77080012)

[Testing & Review Cycle 5](#_Toc77080013)

[Purpose & Scope 6](#_Toc77080014)

[Authority 7](#_Toc77080017)

[Definitions 8](#_Toc77080018)

[How to Recognize a Cyber Incident 11](#_Toc77080019)

[Cyber Security Incident Response Team (CSIRT) 13](#_Toc77080020)

[Incident Types 19](#_Toc77080034)

[Severity Matrix 20](#_Toc77080035)

[Incident Handling Process 22](#_Toc77080036)

[Approvals 26](#_Toc77080050)

[References 27](#_Toc77080053)

# Revision History

*It is a best practice for organizations to ensure their policies are reviewed and updated regularly. Document when changes are made, what changes and by whom.*

The Incident Response Plan has been modified as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modification | Modifier |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Testing & Review Cycle

*Determine how often your Cyber Security Incident Response Plan will be tested and how often reviews are required (Bi-annually, annually, etc.). At a minimum, an incident response plan should be reviewed & updated at least once every three years. Testing frequency is at an organization’s discretion.*

*Determine and document the process to test and review your Cyber Security Incident response plan. If appropriate to your organization, the example provided below can be used.*

*Insert Frequency of Testing, for example Bi-annually, Annually, etc.* testing of the Incident Response Plan 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 of potential incidents.

1. The Incident Response Plan will be tested at least once *Insert Frequency of Testing .*
2. The Incident Response Plan Testing will test your business response to potential incidents, identifying 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 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

*Describe the purpose of your organization’s Incident Response Plan. If appropriate to your organization, the example provided below can be used.*

This Incident Response Plan exists to ensure *Insert Organization Name* 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 detect, prevent, and respond to incidents. By having a plan, a team, and conducting exercises, we will be better prepared to respond inevitable incidents. In addition, we will be able to contain the damage and mitigate further risk to the organization. Resources must be deployed in an organized fashion with exercised skills and communication strategies.

This document describes the overall plan for responding to Cyber Security Incidents at *Insert Organization Name*. 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 *Insert Organization Name* is organized to respond to cyber security incidents effectively and efficiently.

## Scope

*Determine the scope of your plan, including all affected systems and stakeholders. You can refer to the example below and if appropriate, modify the scope as appropriate to your organization.*

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

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

# Authority

*Identify and document the individuals/role in your organization that will be responsible for handling an incident.*

Responsibility for the security of company and customer information resides with the *PRESIDENT/OWNER*. During times when a high or critical cyber security incident is underway, this responsibility is entrusted to the *GENERAL MANAGER.*

# Definitions

*Review the definitions below and retain or revise as required. If necessary, expand the list to best reflect your organization’s unique Cyber Security Incident Response Plan.*

Acceptable interruption window in business continuity planning, is the amount of time in which basic functionality must be restored for critical systems. It is a major factor when planning a disaster recovery solution.

Confidentiality is a classification of data that typically refers to personally identifiable information. It may include such things as social insurance numbers, drivers licence numbers, etc.

Cyber Security Event is an observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, or a user sending email.

Cyber Security Incident is any incident that occurs by accident or deliberately 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 within [ORGANIZATION NAME]. This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by [ORGANIZATION NAME].

Denial of Service (attack) also known as a DoS attack, seeks to make a remote service unavailable to its intended users by flooding its host with superfluous requests, thereby overloading the system.

Exploit in cyber security terms is 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 cybersecurity 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 profile. 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. For example, 99.97% service availability means that a system is available 99.97% of the time.

SLA stands for service level agreement and is used to describe a guaranteed measure of service availability. If service availability drops below the prescribed SLA, there are usually financial repercussions, like a money-back guarantee.

Stakeholder relationship map is a diagram that describes the relationship between individuals in an organization. With respect to cyber security, these diagrams are used to perform IT risk assessments to better inform preventative and reactive measures.

Vulnerability is a piece of code or bug within a system that causes unintended or unanticipated behavior. A vulnerability implies that this behaviour can be taken advantage of for malicious reasons.

War room is 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 is 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

# How to Recognize a Cyber Incident

*Review and retain the indicators that are applicable to your organization. Expand the list of indicators as appropriate to your organization.*

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. Suspicious or unusual activity on, or behaviour of web-facing systems, such on as e-commerce websites
7. Point-of-Sale (POS) payment devices, payment terminals, chip & PIN/signature devices, or dip/swipe card readers showing signs of tampering
8. Any card-skimming devices found in your business
9. Lost, stolen, or misplaced merchant copy receipts or any other records that display a full payment card number or card security code (the three- or four-digit number printed on the card)
10. Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain payment card data or other sensitive data

Cyber Security Incident Response Team

(CSIRT)

# Cyber Security Incident Response Team (CSIRT)

## CSIRT Structure

Provide the organization structure of your CSIRT Team. At a minimum, it must contain an Executive, an Incident Handler and a communication spokesperson as outlined in the common structure below.

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

## CSIRT Roles

* Define the roles and responsibilities, and provide the respective contact information for each member of the CSIRT in the provided space. A table is provided with examples of best practices
* Each role should have a secondary and often a tertiary alternative identified
* Some CSIRT roles may be fulfilled by third part vendors or contracted individuals
* Note, the Incident Handler is not usually the company President/CEO, but rather the head of an IT Team. For organizations that do not have dedicated IT personnel, the President/CEO can assume the role
* List key external contacts and stakeholders that you may need to contact during an incident (for example, legal representative, financial insertions, key clients, staff, IT provider, etc)

### 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. |
| [If applicable insert Note-Taker] |  |
| [If applicable insert Network Technician] |  |
| [If applicable insert Desktop Technician] |  |
| [If applicable insert Server Technician] |  |
| [If applicable insert Legal Technician] |  |

## CSIRT Responsibilities

The responsibilities described below are organized by role within Organization Name.

### Executives

The Executives are/is responsible for:

1. Insert Responsibilities of Executives
2. Insert Responsibilities of Executives
3. Insert Responsibilities of Executives
4. Insert Responsibilities of Executives
5. Insert Responsibilities of Executives
6. Insert Responsibilities of Executives

### Incident Handler

The Incident Handler is responsible for:

1. Insert Responsibilities of Incident Handler
2. Insert Responsibilities of Incident Handler
3. Insert Responsibilities of Incident Handler
4. Insert Responsibilities of Incident Handler
5. Insert Responsibilities of Incident Handler
6. Insert Responsibilities of Incident Handler

### Communications Expert

The communications expert is responsible for:

1. Insert Responsibilities of Communications Expert
2. Insert Responsibilities of Communications Expert
3. Insert Responsibilities of Communications Expert
4. Insert Responsibilities of Communications Expert
5. Insert Responsibilities of Communications Expert
6. Insert Responsibilities of Communications Expert

### CSIRT Team

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

1. Insert Responsibilities of CISRT Team members
2. Insert Responsibilities of CISRT Team members
3. Insert Responsibilities of CISRT Team members
4. Insert Responsibilities of CISRT Team members
5. Insert Responsibilities of CISRT Team members

All staff members are responsible for:

1. Insert Responsibilities of All Staff members
2. Insert Responsibilities of All Staff members
3. Insert Responsibilities of All Staff members
4. Insert Responsibilities of All Staff members
5. Insert Responsibilities of All Staff members

## Contact Information

### CSIRT Contacts

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CSIRT Role | Name | | Title | Phone | | Email |
| *Incident Handler\*\* (lead)* |  |  | | |  |  |
| *Incident Handler (backup)* |  |  | | |  |  |
| *Note-taker* |  |  | | |  |  |
| *Communications* |  |  | | |  |  |
| *Network* |  |  | | |  |  |
| *Desktop* |  |  | | |  |  |
| *Server* |  |  | | |  |  |
| *Legal* |  |  | | |  |  |
| *Executive* |  |  | | |  |  |
| *Additional as required* |  |  | | |  |  |

### External Contacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role | Organization | Name | Title | Phone | Email |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Other Stakeholder Contacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role | Organization | Name | Title | Phone | Email |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Incident Types

# Incident Types

Review the incidents listed below and their description to determine which are appropriate to be included in your Plan. The types can be expanded as necessary.

|  |  |
| --- | --- |
| Type | Description |
| Unauthorized Access or Usage | Individual gains physical or logical access to network, system, or data without permission. |
| Service Interruption or Denial of Service | Attack that prevents access to the service or otherwise impairs normal operation. |
| Malicious Code | Installation of malicious software (for example, virus, worm, Trojan, or other code). |
| 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. |
| Distributed Denial of Service (DDoS) | Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable. Symptoms are widespread connectivity failures or system unavailable errors. |
| Network System Failures (widespread) | An incident affecting the confidentiality, integrity, or availability of networks. |
| Application System Failures | An incident affecting the confidentiality, integrity, or availability of applications or systems. |
| Unauthorized Disclosure or Loss of Information | An incident affecting the confidentiality, integrity, or availability of data. |
| Privacy Breach | An incident that involves real or suspected loss of personal information. |
| Information Security/Data Breach | An incident that involves real or suspected loss of sensitive information. |
| Account Data Compromise | A data breach incident specific to payment card data. Such events result in unauthorized access to or exposure of payment card data (cardholder data or sensitive authentication data). |
| Other | Any other incident that affects networks, systems, or data. |

# Incident Severity Matrix

*Review the sample best practice process below to determine if applicable for your organization’s. Revise to align with your organization.*

The CSIRT will determine the severity of the incident. They will consider:

1. whether a single system is affected or multiple
2. the criticality of the system(s) affected
3. whether impacting a single person or multiple
4. 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 business 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 determine:

1. whether there is evidence of the vulnerability being exploited
2. whether there is a known patch
3. whether this is a new threat (for example, zero day) or a known threat
4. the estimated effort to contain the problem

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Indicators | Scope | Action |
| 1 – Critical | Data loss, Malware | Widespread and/or with critical servers or data loss, stolen data, or unauthorized data access | Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide |
| 2 – High | Theoretical threat becomes active | Widespread and/or with critical servers or data loss, stolen data, or unauthorized data access | Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide |
| 3 – Medium | Email phishing or active spreading infection | Widespread | Implement CSIRT, Incident Response Plan, create Security Incident,  Organization-wide |
| 4 - Low | Malware or phishing | Individual host or person | Notify CSIRT, create Cyber Security Incident |

Incident Handling Process

# Incident Handling Process

## Incident Handling Process Overview

*Develop a process and document action’s taken to handle incidents within your organization. Include the following phases: preparation, identification, containment, eradication, recovery and lessons learned (PICERL model).*

*Refer to the Cyber Incident Response Plan Example to determine processes that may be applicable to your organization.*

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

### Preparation

The preparation phase focuses on preparing your team to handle an incident.

Insert your organization’s unique processes/procedures.

### Identification

The identification phase outlines how your organization will detect and determine if an incident has occurred. This phase requires you to gather information from various sources such as log files, error messages, intrusion detection system reports, and firewalls, which may produce evidence to determine if an incident has occurred.

Insert your organization’s unique processes/procedures.

### Containment

The containment phase is where your organization will outline the action/s it will take to limit the damage and prevent further damage from the incident.

Insert your organization’s unique processes/procedures.

### Eradication

The eradication phase is where your organization will outline how it will remove and restore its affected systems.

Insert your organization’s unique processes/procedures.

### Recovery

The recovery phase is where your organization will outline how it will restore the affected systems to operational status. Consider important factors such as how you plan to test, monitor and validate the systems you are restoring, ensuring they are not still infected by malware or compromised by some other means.

Insert your organization’s unique processes/procedures.

### Lessons Learned

The Lessons Learned phase involves taking stock of the incident; getting to the root of how and why it happened; evaluating how well your Incident Response Plan worked to resolve the issue; and identifying improvements that need to be made.

Insert your organization’s unique processes/procedures

## Incident Specific Handling Processes

Provide the steps for handling specific incidents as defined by your organization.

* Review the list of common types of incidents below and determine which are applicable to your organization. Provide additional incident types as necessary.

Refer to the example of a completed Cyber Incident Response Plan to determine processes that may apply to your organization.

### Data Breach

*If CSIRT investigations confirm that a Data Breach security incident has occurred, please execute the following additional steps:*

*Insert your organization’s unique processes/procedures.*

### Ransomware

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

*Insert your organization’s unique processes/procedures.*

### Tampering of Payment Terminals

*If CSIRT investigations confirm that tampering of pin pads or payment terminals has occurred, please execute the following additional steps:*

*Insert your organization’s unique processes/procedures.*

### Widespread Service Interruption

If CSIRT investigations confirm that widespread service interruption security incident has occurred, please execute the following additional steps:

*Insert your organization’s unique processes/procedures.*

### Loss of Equipment

If CSIRT investigations confirm that loss of equipment or theft has occurred, please execute the following:

*Insert your organization’s unique processes/procedures.*

Approvals

# Approvals

## Responsible Party

*Determine who will be responsible for the development, updating and enforcement of the Incident Response Plan.*

Responsibility for the security of company and customer information resides with the following Responsible Party:

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible Party Name and Title | Responsible Party Signature | Version | Date |
|  |  |  |  |
|  |  |  |  |

The Responsible Party has reviewed the Incident Response Plan and delegates the responsibility for mitigating harm to the organization to the Incident Handler.

During times when a high or critical cyber security incident is underway this responsibility is entrusted to the Incident Handler or their delegate.

## Incident Handler

*Identify who the Incident Handler is for your plan and their respective responsibilities. If appropriate, you can use the example below.*

The Incident Handler has reviewed the Security Incident Response Plan and acknowledges that, when a high or critical cyber security incident is underway, responsibility for managing the incident is entrusted to the Incident Handler or their delegate.

The Incident Handler or their delegate is expected to handle the incident in a way that mitigates further exposure of the organization. The incident will be handled according to process including identification, containment, eradication, recovery, and lessons learned.

|  |  |  |  |
| --- | --- | --- | --- |
| Incident Handler Name and Title | Incident Handler Signature | Version | Date |
|  |  |  |  |
|  |  |  |  |

# References

* National Institute of Standards and Technology (NIST), NIST Special Publication 800-61 Revision 2, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
* SysAdmin, Audit, Network & Security (SANS), <https://www.sans.org/reading-room/whitepapers/incident>
* SysAdmin, Audit, Network & Security (SANS), <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>
* SANS incident handling forms (SANS), <https://www.sans.org/score/incident-forms>
* The Office of the Privacy Commissioner of Canada – The Personal Information Protection and Electronic Documents Act (PIPEDA), <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronicdocuments-act-pipeda/>
* The Office of the Privacy Commissioner of Canada – PIPEDA: What you need to know about mandatory reporting of breaches of security safeguards, <https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-yourbusiness/gd_pb_201810/>
* Government of Canada – Canada's Anti-Spam Legislation (CASL), <https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home>
* SANS GIAC Certifications – Incident Handler’s Handbook, <https://sansorg.egnyte.com/dl/6Btqoa63at/>?