Organization Logo (Optional)

Incident Response Plan

Organization Name

Date

Created by: CYBERSAFE SQUAD

**** Cybersafe Squad has developed this fillable template as part of the CyberSecure Blueprint process for educational purposes only. This template is intended to provide guidance on how to organize and document information for log management policies. Please note that the use of this template does not guarantee successful certification or compliance with any regulatory requirements. Organizations are not obligated to use this template and may choose to provide certification requirements in a format that best suits their needs and REQUIREMENTS. ****

Instruction for this template:

This template is intended to assist users in fulfilling the certification requirements for the Develop An Incident Response Plan security control area of *CyberSecure Blueprint process* Canada. The purpose of this document is to guide users in creating an effective incident response plan for their organization.

To ensure clarity and simplicity, instructions have been included in red font within each section of the template. These instructions provide detailed guidance on the information that needs to be included in each section. Once the template has been completed, it is recommended that these instructions are removed to provide a clear and concise incident response plan.

To gain a thorough understanding of the development of an incident response plan, it is recommended that users review the eLearning module Develop An Incident Response Plan. This eLearning module provides comprehensive training on how to create an effective incident response plan.

Additionally, it is suggested that users review the completed example of an incident response plan. This example can serve as a reference point for users as they develop their own incident response plan.

Overall, this template serves as a valuable tool for organizations looking to enhance their incident response capabilities. By following the guidelines provided within this document, users can create an effective incident response plan that will help their organization to quickly and efficiently respond to cyber security incidents.

Index

Revision History

Revision history is a log or record of changes made to the incident response plan document. It documents the history of revisions and updates made to the plan over time, including the date of each revision, the name of the person who made the revision, and a brief description of the changes.

1. Start with a clear heading titled "Revision History."
2. State that this section is to document the history of changes made to the incident response plan.
3. Provide a table with the following columns: Date, Version, Author, and Description.
4. Instruct the team to fill out the table with the date of each revision, the version number, the name of the person who made the revision, and a brief description of the changes made.
5. Emphasize the importance of maintaining an accurate revision history to ensure that all team members have access to the most up-to-date version of the incident response plan.
6. Finally, specify that the revision history should be updated every time changes are made to the plan, and that it should be included at the beginning of the document.

Date	**Version**	**Modification**	**Modifier**

Testing & Review Cycle

As an organization, it is essential to have a Cyber Security Incident Response Plan in place to mitigate the risks associated with cyber threats. In order to ensure the effectiveness of the plan, it is important to determine the frequency at which it will be tested and reviewed. While the testing frequency is at the organization's discretion, it is recommended that the plan is reviewed and updated at least once every three years.

To establish a robust process for testing and reviewing the plan, it is necessary to document the procedures to be followed. The process should be tailored to the specific needs and requirements of the organization. If appropriate, the example provided below can serve as a starting point for developing the process:

1. Define the scope and objectives of the testing and review process.
2. Identify the team responsible for conducting the testing and review.
3. Develop a testing plan that outlines the scenarios to be tested and the methods used for testing.
4. Execute the testing plan, including simulation exercises to evaluate the effectiveness of the plan.
5. Document the results of the testing and identify any gaps or weaknesses in the plan.
6. Based on the results of the testing, update the plan as necessary to address any identified issues.
7. Conduct a review of the updated plan and document the changes made.
8. Establish a schedule for ongoing testing and reviews of the plan, taking into consideration any changes to the organization's risk profile or threat landscape.

It is important to note that the testing and review process should involve stakeholders from across the organization, including IT, security, legal, and business teams. By regularly testing and reviewing the Cyber Security Incident Response Plan, organizations can ensure that they are prepared to respond effectively to cyber threats and minimize the impact of any incidents.

Testing the Incident Response Plan is a crucial component in ensuring the readiness of the Cyber Security Incident Response Team (CSIRT). Through testing, CSIRT members are made aware of their obligations and can identify potential process gaps and areas for improvement. While real incidents provide the most comprehensive testing of the plan, practical simulations and walkthroughs can also effectively achieve this objective.

To ensure that the Incident Response Plan remains effective and up-to-date, it is recommended to test it at least once a year, or as frequently as necessary to meet your organization's risk management requirements. The testing process should aim to evaluate the effectiveness of your business's response to potential incidents and identify any shortcomings in the plan.

During testing, the CSIRT should record observations made, including any steps that were poorly executed or misunderstood by participants and areas requiring improvement. These observations should be thoroughly analyzed to identify opportunities for enhancing the plan and mitigating risk. The Incident Handler should take ownership of the plan's upkeep and ensure that updates are made and distributed to CSIRT members.

In summary, testing of the Incident Response Plan is a necessary exercise to ensure the preparedness of the CSIRT and the effectiveness of the plan in mitigating cyber threats. Regular testing and continuous improvement of the plan can help organizations proactively manage and mitigate risks, ultimately protecting their assets, reputation, and customers.

Purpose & Scope

Purpose

Please provide an explanation of the objective behind your organization's Incident Response Plan. In case it is applicable to your organization, you may use the following example.

The purpose of this Incident Response Plan is to establish a framework for Insert Organization Name to respond promptly and effectively to cyber security incidents. Given the increasing frequency and complexity of cyber threats, no organization is completely immune to potential attacks. Therefore, it is imperative that organizations take proactive measures to detect, prevent, and respond to incidents in order to minimize damage and mitigate future risks.

By having a comprehensive plan in place, as well as a skilled and prepared incident response team, we can better manage and respond to any cyber security incidents that may arise. It is important to ensure that resources are deployed in an organized and efficient manner, utilizing exercised skills and effective communication strategies.

This document outlines the overarching plan for responding to cyber security incidents within our organization. It identifies the appropriate structure, roles, and responsibilities necessary for a coordinated and effective response to common incidents. The plan also outlines the process for preparing, identifying, containing, eradicating, recovering, and conducting lessons learned in order to minimize the impact of cyber security incidents.

The goal of this Incident Response Plan is to ensure that Insert Organization Name is well-equipped and organized to respond to any cyber security incidents that may occur. By establishing a clear and effective plan, we can work together to minimize the impact of these incidents on our organization and our stakeholders. We recognize that preparedness is critical to effective incident response, and we are committed to ongoing training, practice, and improvement in this area.

Scope

To begin planning, it's important to identify the extent of the plan, which includes all of the relevant systems and individuals who will be impacted by it. You can refer to the sample plan provided as a reference, but if necessary, adjust the scope of your plan to fit the needs of your organization.

The Incident Response Plan outlined here is designed to address any potential cybersecurity incidents that may occur within our organization's networks, systems, and data. This plan is inclusive of all individuals who have access to our infrastructure, including employees, contractors, and third-party vendors. As a member of our Cyber Security Incident Response Team (CSIRT), you will be expected to lead or contribute to our organization's response efforts in the event of a cybersecurity incident. It is imperative that all CSIRT members familiarize themselves with this plan and be prepared to collaborate and work together towards the common goal of minimizing any adverse effects on our organization.

This document establishes a framework for managing and responding to cybersecurity incidents, including determining the appropriate response for common cybersecurity incidents. However, it is important to note that this document is not intended to provide an exhaustive list of all possible activities that may be required to effectively combat a cybersecurity incident. Instead, it serves as a general guide for CSIRT members to follow when responding to incidents.

In addition, this document is designed to establish incident handling and response capabilities that will enable us to effectively manage any cybersecurity incidents that may arise. Our response efforts will be driven by a thorough analysis of the incident, and we will take appropriate steps to contain and mitigate any potential damage. Our ultimate goal is to restore normal operations as quickly as possible while minimizing any negative impact on our organization.

Authority

Please identify and document the people or positions within your organization that will be responsible for managing an incident. This is important to ensure that your organization is prepared to handle any unforeseen events that may arise in the future. By having a clear understanding of who is responsible for what, you can minimize the impact of any incident and help your organization recover quickly.

In an organization, it is vital to ensure the security of confidential information related to the company and its customers. The primary responsibility for safeguarding this information lies with the President or Owner of the company. This includes developing and implementing policies, procedures, and controls that are designed to protect the integrity, confidentiality, and availability of the data.

However, during times of high or critical cyber security incidents, it may become necessary to entrust this responsibility to the General Manager. This is because such incidents can have severe implications for the company, and require swift action to prevent any further damage. The General Manager should have the necessary expertise and authority to coordinate the incident response team, analyze the situation, and take appropriate measures to mitigate the impact of the incident.

To ensure that the organization's information security policies and procedures are effective, it is essential to establish a culture of security awareness among all employees. This involves providing regular training and education programs to help employees understand the importance of information security, how to identify potential threats, and what actions to take to prevent or report security incidents.

In addition, it is important to conduct regular risk assessments to identify potential vulnerabilities in the company's information systems and infrastructure. This can help to proactively address any weaknesses and implement additional security measures to protect the organization's information assets.

Ultimately, safeguarding company and customer information requires a collaborative effort among all stakeholders, from the President and General Manager to every employee in the organization. By working together, establishing effective policies and procedures, and maintaining a culture of security awareness, companies can minimize the risk of cyber security incidents and protect their valuable assets.

Definitions

The task is to review the definitions given below and modify them as needed to align with your organization's specific Cyber Security Incident Response Plan. If required, you may add more definitions to the list to make it more comprehensive.

Terms	Definition
Acceptable interruption window	The "Acceptable interruption window" is the amount of time that a company considers acceptable for its critical systems to be non-functional or down during a disaster or disruption. It is a factor that is taken into account when developing a Business Continuity Plan and a Disaster Recovery Solution, as it helps to define the timeframe for how long the company can operate with limited or no functionality before it starts to experience significant negative impacts.
Confidentiality	Confidentiality refers to a security principle that aims to protect sensitive information from unauthorized access or disclosure. It involves keeping information secret and preventing it from falling into the wrong hands. Confidential information is typically classified as data that should only be seen or accessed by authorized individuals or groups. Examples of confidential information may include personally identifiable information (such as social insurance numbers or driver's license numbers), financial information, or trade secrets.
Cyber Security Event	A Cyber Security Event is an observable occurrence that happens within a computer system or network. Examples of such events can include a user connecting to a file share, a server receiving a request for a web page, or a user sending an email. Essentially, any activity that can be tracked or monitored within a computer system or network can be considered a Cyber Security Event. These events are important to track and analyze as they can provide insights into potential security threats or breaches.
Cyber Security Incident	A Cyber Security Incident is any event, whether accidental or deliberate, that affects the proper functioning of a company's communication or information processing systems. It can be any circumstance or situation that poses a risk to the confidentiality, integrity, or availability of the data, information, or services provided by the organization. This includes situations where data or services provided by the company are accessed, used, disclosed, modified, or destroyed without authorization.
Denial of Service (attack)	A Denial of Service (DoS) attack is when someone tries to make a website or other online service unavailable to the people who are supposed to be able to use it. They do this by sending so many requests to the service that it can't handle all of them, and it crashes or becomes too slow to use. This makes it impossible for legitimate users to access the service.
Exploit	An "Exploit" is a type of software, data, or command used in cyber security that takes advantage of a weakness or vulnerability in computer software, hardware, or electronic devices. It can cause unexpected or unintended behavior to occur, often allowing an attacker to gain unauthorized access or control over the affected system.
Indicators	Indicators, also known as "Indicators of Compromise" or IOCs, are signs or evidence that cyber attackers leave behind after they've infiltrated a company's computer network or systems. These clues can be found in different places, such as log entries, files, or databases, and can help investigators identify the source and nature of the attack or breach.

Integrity	The term "Integrity" refers to the process of maintaining accurate and consistent data that is accessible only to authorized users throughout its entire life cycle. This means that the data must be protected from unauthorized modifications, and that its accuracy and consistency must be ensured throughout its use. Integrity is an essential element of data management, as it helps to ensure that the information is reliable and trustworthy for the intended purposes.
Maximum tolerable downtime	"Maximum Tolerable Downtime (MTD)" is a term used in Business Continuity Planning to describe the longest period of time that a critical business process can be down before the organization's survival is at risk. In other words, it is the maximum amount of time that the company can tolerate without that process being operational before it starts to seriously impact the organization's ability to function. The MTD is an important consideration when developing a disaster recovery plan.
Response playbook	A Response Playbook is a set of guidelines that organizations use to improve their cybersecurity. The playbook provides a set of specific measures and best practices that can be implemented to enhance the organization's overall security profile. By following the playbook, companies can establish a set of standards for improving their existing systems and implementing new ones to better protect themselves against potential cyber attacks.
Service availability	"Service availability" refers to the state of a system being ready and responsive for users to access. This term is often used to describe how reliable a system or network resource is, based on the percentage of time it is available. For instance, if a system has a service availability of 99.97%, it means that it is accessible 99.97% of the time.
SLA	SLA stands for Service Level Agreement. It's a term used to describe a promise made by a service provider to their customers about how much time their service will be available. This is important because if the service is not available for the amount of time promised in the SLA, there may be financial consequences, such as a refund or credit.
Stakeholder relationship map	A Stakeholder Relationship Map is a visual diagram that shows how people are connected in an organization. When it comes to cyber security, these diagrams are used to assess the risks to a company's IT systems. By looking at these diagrams, companies can better understand the potential risks and take action to prevent or respond to cyber security incidents.
Vulnerability	A vulnerability is a problem in a computer system's code or programming that makes it do something unintended or unexpected. This can be exploited by hackers or cybercriminals to gain unauthorized access to the system or to cause harm. In other words, a vulnerability is a weakness that bad actors can use to attack a system.
War room	A War Room is a special room used to handle major incidents in an organization. It's important that the room has a door for privacy and is always available. Additionally, it must have good communication infrastructure such as network and phone connections.
Zero-day	Zero-day is a term used in cyber security to describe a type of software vulnerability that the software vendor is aware of but hasn't yet created a patch or fix for. This means that cybercriminals can potentially exploit the vulnerability to cause harm to a system, and it's called "Zero-day" because it's the first day the vulnerability has been discovered and there's no patch or solution to fix it yet.

How to Recognize a Cyber Incident

Instructions: Please review the indicators listed and only keep the ones that are relevant to your organization. You may also add more indicators to the list as necessary.

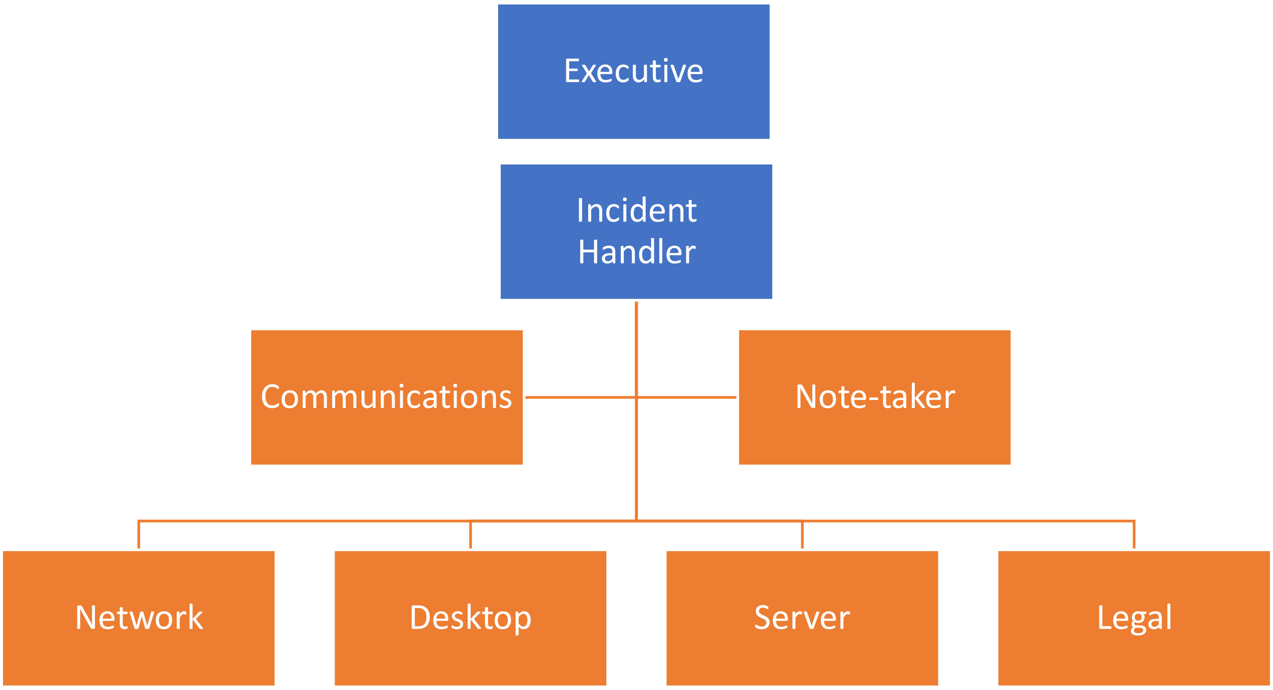
Cyber security incidents may not be obvious right away, but there are signs to look out for that could indicate a security breach, unauthorized activity, or misuse in your own system or those of your third-party service providers. Here are some signs to watch for:

1. If you see unusual log-ins or system activity, particularly from inactive user accounts, it could indicate a security incident.
2. If there is excessive or unusual remote access activity to your business, from either staff or third-party providers, it could also be a sign of a security incident.
3. If you notice any new wireless networks that are visible or accessible from your environment, it could be an indicator of a security incident.
4. If you see any new or suspicious files, malware, or unapproved executable files and programs on your networks or systems, including web-facing systems, it could be a sign of a security incident.
5. If you find hardware or software key-loggers connected to or installed on systems, it could indicate a security incident.
6. If you see any suspicious or unusual activity on your e-commerce websites or other web-facing systems, it could be an indicator of a security incident.
7. If you notice any tampering with Point-of-Sale payment devices, payment terminals, chip & PIN/signature devices, or dip/swipe card readers, it could be a sign of a security incident.
8. If you find any card-skimming devices in your business, it could indicate a security incident.
9. If you have lost, stolen, or misplaced merchant copy receipts or any other records that display a full payment card number or card security code, it could be a sign of a security incident.
10. If you have lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain payment card data or other sensitive data, it could also be an indicator of a security incident.

It's important to keep an eye out for any of these signs and to take action if you suspect a security incident may have occurred.

Cyber Security Incident Response Team (CSIRT)

Please provide the organizational structure of your CSIRT (Computer Security Incident Response Team) that includes, at a minimum, an Executive, an Incident Handler, and a communication spokesperson as per the common structure guidelines.



A CSIRT, or Cyber Security Incident Response Team, typically has a standardized organizational structure that includes specific roles and responsibilities for its members. This structure is designed to ensure that the team is able to effectively and efficiently respond to cyber security incidents.

Roles and Responsibilities

Instructions:

- First, you need to define the roles and responsibilities of each member of the Computer Security Incident Response Team (CSIRT) and provide their contact information in the space provided. You can use a table with best practices as an example.
- For each role, you should also identify a secondary and sometimes a tertiary alternative person who can take over the role if the primary person is unavailable.
- Some CSIRT roles may be fulfilled by third-party vendors or contracted individuals. This means that someone outside of the company may be responsible for a role, like responding to a security incident.
- Note that the Incident Handler, who is responsible for leading the response to a security incident, is usually not the company's President/CEO. Instead, it's typically the head of the IT team. However, if your organization doesn't have dedicated IT personnel, the President/CEO can take on this role.
- Finally, you should list the key external contacts and stakeholders that you may need to contact during a security incident. This might include a legal representative, financial institutions, key clients, staff, IT provider, and others who may be involved in the incident response process.

CSIRT Roles	Responsibility and Duties
Executive	The Executive role is accountable for safeguarding the organization against cyber security threats. They report to the board of directors and other executives, and are responsible for making important executive decisions within the CSIRT. As such, they oversee and manage key issues related to cyber security that require high-level decision-making.
Incident Handler	The Incident Handler is a key member of the CSIRT responsible for leading the team's response to cyber security incidents. Their main duty is to organize and initiate the Incident Response Plan to investigate and respond to security incidents. This involves analysing the incident, gathering information, and coordinating with other members of the CSIRT to develop a plan of action. The Incident Handler must also communicate with relevant stakeholders and external parties, such as IT providers or law enforcement, as needed. Their ultimate goal is to contain and resolve the incident as quickly and efficiently as possible while minimizing the impact on the organization.
Communications	As a key member of the team, the Communications Expert is responsible for overseeing all aspects of the company's public relations and internal communications efforts. They are tasked with ensuring that all stakeholders, customers, and the general public are kept informed in a timely and compliant manner. They accomplish this by creating and distributing messages, responding to inquiries, and monitoring public perception of the company. The Communications Expert plays a critical role in maintaining positive relationships with both internal and external parties, and serves as an important liaison between the company and the public.
Note-Taker(optional)	The Note-Taker is responsible for taking detailed and accurate notes during an incident response. They are responsible for documenting all aspects of the incident, including the timeline, actions taken, and the results of those actions. Their primary duty is to ensure that all information related to the incident is recorded and organized in a clear and concise manner. They may also be responsible for creating incident reports, which may be used for future reference or to share with stakeholders. The Note-Taker's responsibilities may include: • Taking detailed notes during an incident response • Documenting all aspects of the incident, including the timeline, actions taken, and results • Ensuring that all information related to the incident is recorded and organized in a clear and concise manner • Creating incident reports for future reference or to share with stakeholders • Communicating with other members of the CSIRT to ensure that all relevant information is captured • Maintaining the confidentiality of all incident-related information Overall, the Note-Taker plays a critical role in ensuring that all incident-related information is accurately documented and shared with other members of the CSIRT.

Network Technician(optional)	As a member of the CSIRT, the Network Technician is responsible for monitoring and maintaining the organization's network infrastructure. Their duties include identifying and responding to potential security threats, analysing network performance, and troubleshooting network issues. They work closely with other members of the CSIRT to develop and implement security measures that protect the network from unauthorized access, data breaches, and other cyber-attacks. Additionally, they are responsible for ensuring that network hardware and software is up-to-date and functioning properly, and may be required to perform regular security audits to identify potential vulnerabilities. Overall, the Network Technician plays a critical role in ensuring that the organization's network is secure, reliable, and functioning optimally.
Desktop Technician(optional)	The Desktop Technician is responsible for managing and maintaining the organization's computers and other devices. In the context of CSIRT, their main duties and responsibilities include: • Identifying and resolving technical issues related to hardware, software, and network connectivity • Installing and configuring operating systems, applications, and other software as required • Conducting regular security checks to identify and remediate any vulnerabilities • Responding to security incidents as directed by the CSIRT lead or Incident Handler, and providing technical support during incident response activities • Ensuring that all devices are up-to-date with the latest patches and updates • Providing training and support to end-users to ensure that they understand how to use the devices and follow security best practices And here's a professional paraphrase of the simplified definition: As a key member of the CSIRT, the Desktop Technician plays a critical role in managing and maintaining the organization's computers and devices. They are responsible for identifying and resolving technical issues related to hardware, software, and network connectivity, and ensuring that all devices are secure and up-to-date with the latest patches and updates. During security incidents, the Desktop Technician provides technical support to the CSIRT lead or Incident Handler, and helps to identify and remediate any vulnerabilities. Additionally, they provide training and support to end-users to ensure that they understand how to use the devices and follow security best practices. The Desktop Technician's contributions are essential to the overall success of the CSIRT and the organization's security posture.
Server Technician(optional)	The Server Technician in a CSIRT is responsible for maintaining and troubleshooting the company's servers. In the event of a security incident, they are responsible for working with other members of the CSIRT to investigate the incident and determine the extent of any damage. They may also be responsible for identifying and implementing security patches and updates to prevent future incidents. Other duties of a Server Technician in a CSIRT may include: • Monitoring server logs for suspicious activity and conducting regular security audits.

	• Ensuring that servers are configured and maintained in compliance with security policies and industry best practices. • Responding promptly to server-related issues or incidents that may impact the availability, confidentiality, or integrity of company data. • Collaborating with other CSIRT members to develop and test incident response plans, procedures, and training. • Keeping up-to-date with emerging threats and vulnerabilities, and recommending appropriate mitigations to management. • Maintaining accurate and up-to-date records of server configurations, maintenance activities, and incident response activities. Overall, the Server Technician in a CSIRT plays a critical role in ensuring that the company's servers are secure, available, and operating as intended. They work closely with other members of the CSIRT to prevent, detect, and respond to security incidents in a timely and effective manner.
Legal Technician(optional)	The Legal Technician in CSIRT is responsible for providing legal expertise and support during the incident response process. They review and analyse legal requirements, policies, and procedures related to the incident to ensure that the company is compliant. They also assist with the collection and preservation of evidence in accordance with legal requirements. In addition, they may liaise with external legal counsel or regulatory bodies to ensure that the company is meeting all legal obligations. The Legal Technician plays an important role in minimizing legal risks and ensuring that the incident response process is conducted in a legally sound manner.

CSIRT Responsibilities

It is possible to articulate the responsibilities of users in a detailed manner through effective writing. This would involve identifying the specific actions and behaviors that users are expected to exhibit when interacting with a particular system, product, or service. For instance, users may be required to adhere to certain rules or guidelines that govern their use of a platform, such as refraining from posting offensive content or respecting the privacy of other users.

To write about user responsibilities in detail, one must have a clear understanding of the context in which the users are operating, as well as the potential risks and consequences associated with non-compliance. It may also be necessary to provide examples or scenarios that illustrate how users can fulfill their responsibilities, as well as any potential pitfalls or challenges that they may encounter.

Overall, writing about user responsibilities in a detailed manner can help to promote responsible and ethical behavior among users, while also mitigating the risks and liabilities associated with the use of a particular system or product. It can also serve as a useful reference point for users who may be unsure of their obligations, and can help to ensure that everyone involved is on the same page when it comes to acceptable conduct.

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

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

You can also add extra details here.

Incident Types

To complete your Plan, review the listed incidents and their descriptions, and decide which ones are relevant. You can expand the types of incidents if needed to ensure comprehensive coverage.

Type	Details
Unauthorized Access or Usage	Unauthorized access or usage refers to any instance where an individual or entity gains access to a system, network, or application without proper authorization or permission. This could include hacking into a system, exploiting a vulnerability, or using someone else's credentials to gain access to restricted areas. Unauthorized access or usage can result in the theft or exposure of sensitive data, the disruption of critical systems, and other security risks. It is important to have measures in place to prevent unauthorized access or usage, as well as procedures for detecting and responding to such incidents in a timely and effective manner.
Service Interruption or Denial of Service	Service interruption or denial of service refers to an incident where a system or service becomes unavailable or inaccessible to its intended users. This could occur due to a variety of reasons, such as network outages, system failures, malicious attacks, or overwhelming traffic. Service interruption or denial of service can have significant impacts on business operations, customer satisfaction, and revenue. To minimize the risks of service interruption or denial of service, organizations should have robust redundancy and failover mechanisms in place, as well as effective monitoring and response procedures to detect and mitigate incidents as quickly as possible.
Malicious Code	Malicious code refers to any code, script, or program that is designed to cause harm, steal information, or perform unauthorized actions on a system or network. Malicious code can be introduced to a system in a variety of ways, such as through email attachments, downloads from untrusted sources, or infected websites. Malicious code can include viruses, worms, Trojans, ransomware, and other types of malware. Malicious code can have serious consequences, such as data theft, system damage, and network intrusion. To prevent malicious code incidents, organizations should have robust anti-malware solutions in place, along with strict policies and procedures for managing software and system updates, and for educating users on safe computing practices.
Ransomware	Ransomware is a type of malicious code that is designed to encrypt or lock down a victim's computer or files, rendering them inaccessible until a ransom is paid. Ransomware typically spreads through malicious emails, attachments, or links, or by exploiting vulnerabilities in software or systems. Once the ransomware infects a system, it will typically display a message demanding payment in exchange for a decryption key that can unlock the victim's files or computer. Ransomware attacks can have severe consequences, such as data loss, business interruption, reputational damage, and

	financial losses. To prevent ransomware incidents, organizations should have robust data backup and recovery mechanisms in place, as well as strong cybersecurity defenses that include anti-malware software, firewalls, and intrusion detection systems. Additionally, employees should be educated on how to recognize and avoid ransomware attacks, such as by avoiding suspicious emails or downloads, and keeping software and systems up to date with the latest security patches.
Distributed Denial of Service (DDoS)	Distributed Denial of Service (DDoS) is a type of cyber-attack that aims to disrupt the availability of a network or website by overwhelming it with traffic from multiple sources. DDoS attacks typically involve a large number of compromised devices, such as botnets, that are coordinated to flood the target system or network with traffic, causing it to become inaccessible to legitimate users. DDoS attacks can be motivated by various reasons, such as hacktivism, extortion, or revenge. DDoS attacks can have severe consequences, such as downtime, lost revenue, and reputational damage. To prevent DDoS incidents, organizations should have robust network and application-layer defenses in place, such as firewalls, intrusion detection systems, and content delivery networks. Additionally, organizations should have incident response plans that outline the steps to be taken in the event of a DDoS attack, including communication protocols, technical mitigations, and post-incident analysis.
Network System Failures (widespread)	Network system failures refer to incidents where a critical network infrastructure, such as a router or switch, fails, causing widespread disruption to the network's operations. Network system failures can occur due to various reasons, such as hardware malfunctions, software bugs, or power outages. The consequences of network system failures can be severe, resulting in downtime, lost productivity, and revenue. To prevent network system failures, organizations should have redundancy mechanisms in place, such as backup equipment or alternative network paths, to ensure continuity of operations in the event of a failure. Additionally, organizations should have robust monitoring and alerting systems in place that can detect and notify personnel of potential system failures before they occur, allowing for timely intervention and resolution. In the event of a network system failure, organizations should have incident response plans that outline the steps to be taken to restore the system's operations as quickly as possible.
Application System Failures	Application system failures refer to incidents where an application, such as a software program or web application, fails to function properly, causing disruption or errors in its intended operation. Application system failures can occur due to various reasons, such as coding errors, database corruption, or incompatible software updates. The consequences of application system failures can be significant, resulting in lost productivity, revenue, and customer satisfaction. To prevent application system failures, organizations should have robust testing and quality assurance processes in place to identify and resolve issues before they impact users.

	Additionally, organizations should have monitoring and alerting systems in place to detect and notify personnel of potential application system failures before they occur, allowing for timely intervention and resolution. In the event of an application system failure, organizations should have incident response plans that outline the steps to be taken to restore the application's functionality as quickly as possible, such as rolling back to a previous version or implementing a temporary workaround.
Unauthorized Disclosure or Loss of Information	Unauthorized disclosure or loss of information refers to incidents where sensitive or confidential information is disclosed or lost without proper authorization or safeguards in place.
Privacy Breach	A privacy breach refers to incidents where personal identifiable information (PII) is accessed, used, or disclosed without proper authorization or safeguards in place, potentially resulting in harm to individuals whose data has been compromised.
Information Security/Data Breach	An information security or data breach refers to incidents where an organization's computer systems, networks, or databases are compromised, potentially resulting in unauthorized access, theft, or destruction of sensitive information.
Account Data Compromise	An account data compromise refers to incidents where an unauthorized party gains access to login credentials, such as usernames and passwords, for an individual's account, potentially allowing the attacker to access sensitive information or conduct fraudulent activities.
Other	"Other" incidents refer to any other type of incident that may affect networks, systems, or data but are not included in the specific incident types mentioned earlier. These incidents could include events such as natural disasters, physical security breaches, insider threats, or other types of security incidents that compromise the confidentiality, integrity, or availability of an organization's networks, systems, or data. In such cases, organizations should have incident response plans in place that are tailored to the specific incident type to ensure a prompt and effective response.

Severity Matrix

The given instructions suggest that you should go through the provided best practice process and see if it is relevant and suitable for your organization. If it is applicable, you are advised to modify or tailor it to meet your organization's specific requirements and standards.

To elaborate further, reviewing the sample best practice process can help you gain an understanding of the different steps involved in achieving the desired outcome. By assessing its relevance to your organization, you can determine if it aligns with your business goals and objectives. If necessary, you can make changes to the process to ensure that it meets your organization's needs and standards.

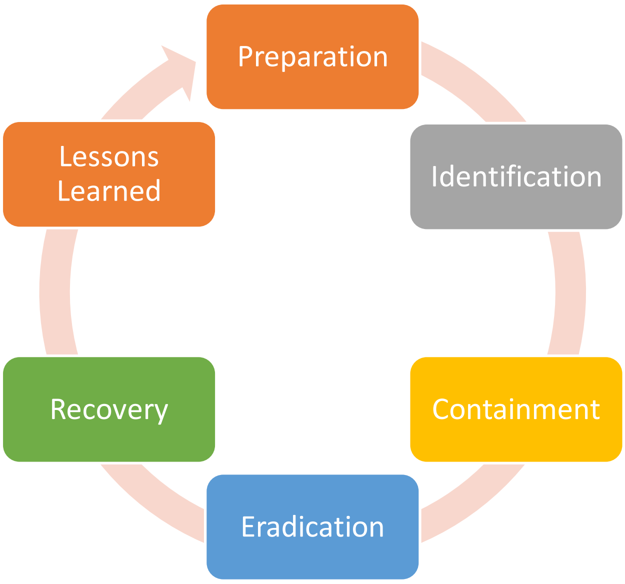
It's important to note that while the sample best practice process provides a framework for achieving success, it's not a one-size-fits-all solution. Each organization has its unique needs and requirements, and it's essential to customize the process accordingly to maximize its effectiveness. So, by revising and aligning the best practice process with your organization, you can enhance its suitability and ensure that it meets your specific needs.

- The CSIRT will determine the severity of the incident based on several factors
- The CSIRT will consider whether a single system or multiple systems are affected
- The criticality of the system(s) affected will be evaluated
- The impact of the incident on a single person or multiple persons will be assessed
- The potential impact on a single team/department, multiple teams/departments, or the entire organization will be evaluated
- The Incident Handler must consider the relevant business context and other business factors to understand the urgency of remedial action
- The CSIRT will assess the known magnitude of impact and likelihood of effect spreading
- The potential impacts to the organization, including financial damage and reputational damage, will be evaluated
- The type of incident, whether sophisticated or unsophisticated, automated or manual, or nuisance/vandalism, will be assessed
- The CSIRT will determine whether there is evidence of vulnerability exploitation
- The existence of a known patch will be considered
- Whether the threat is new (zero day) or known will be assessed
- The estimated effort to contain the problem will be evaluated to determine the severity of the incident.

By considering these factors, the CSIRT can determine the severity of the incident and take appropriate action to mitigate its impact.

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



1. Preparation:

- Develop an incident response plan that includes roles and responsibilities, communication protocols, and procedures for detecting, reporting, and responding to incidents.
- Establish a CSIRT (Computer Security Incident Response Team) and provide them with the necessary training, tools, and resources to carry out their responsibilities.21
- Implement security measures such as access controls, intrusion detection, and data backup and recovery to prevent and mitigate incidents.

2. Detection and Reporting:

- Monitor systems and networks for suspicious activities or anomalies that may indicate an incident.
- Establish a reporting mechanism for employees, customers, and other stakeholders to report incidents.
- Notify the CSIRT immediately upon detection of an incident.

3. Triage and Analysis:

- Assess the incident to determine its scope and severity.
- Gather information about the incident, including the affected systems, data, and users.
- Analyze the incident to determine the cause, impact, and potential risks.
- Prioritize incidents based on their severity and potential impact on the organization.

4. Containment and Mitigation:

- Isolate affected systems to prevent the spread of the incident.
- Identify and apply appropriate mitigation measures to minimize the impact of the incident.
- Implement temporary fixes to restore normal operations while the CSIRT works on a permanent solution.
- Communicate with stakeholders about the incident, its impact, and mitigation measures.

5. Investigation and Resolution:

- Conduct a thorough investigation of the incident to determine the root cause and any related issues.
- Document all findings and actions taken during the incident handling process.
- Develop and implement a permanent solution to prevent similar incidents from occurring in the future.
- Test the solution to ensure it's effective and does not introduce new vulnerabilities.

6. Post-Incident Activities:

- Evaluate the incident response plan and update it as necessary based on lessons learned.
- Communicate with stakeholders about the incident, its resolution, and any changes to the incident response plan.
- Conduct a debriefing session with the CSIRT to review the incident handling process and identify areas for improvement.
- Provide training and awareness programs to employees and stakeholders to prevent incidents and improve incident reporting.

Approvals

As the responsible person for incident handling, [insert name], I have carefully reviewed and approved the detailed incident handling plan outlined above. This plan is critical for ensuring the security and resilience of our organization's systems and data, and I fully endorse its implementation. I understand that it is my responsibility to ensure that the incident handling process is effectively integrated into our organization's overall security strategy and that appropriate training and resources are provided to the CSIRT.

[Insert name], [insert title],

Signature

Version: [insert version number] Date: [insert date]

As the incident handler responsible for implementing the incident handling process, [insert name], I have carefully reviewed and approved the detailed incident handling plan outlined above. I understand that it is my responsibility to ensure that the CSIRT is appropriately trained and equipped to respond to incidents in a timely and effective manner. By following the incident handling procedures outlined in this plan, I am confident that we will be able to quickly detect, triage, contain, investigate, and resolve incidents.

[Insert name], Incident Handler

Signature

Version: [insert version number] Date: [insert 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/?
- CyberSecure Canada, https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools