Group 7

Incident Response Plan

Revision 1.0

01.06.2023

Table of Contents

[Revision History 3](#_Toc136849634)

[Purpose and Scope 4](#_Toc136849635)

[Purpose 4](#_Toc136849636)

[Scope 4](#_Toc136849637)

[Assumption 4](#_Toc136849638)

[Planning Scenarios: 5](#_Toc136849639)

[Unauthorized Access attack: 5](#_Toc136849640)

[Network Intrusion: 5](#_Toc136849641)

[Server Breach: 5](#_Toc136849642)

[Physical Security Breach: 5](#_Toc136849643)

[Definitions 7](#_Toc136849644)

[How to Recognize a Cyber Incident 8](#_Toc136849645)

[Cyber Security Incident Response Team (CSIRT) 10](#_Toc136849646)

[(CSIRT) Roles: 10](#_Toc136849647)

[(CSIRT) contacts: 11](#_Toc136849648)

[Incident Types: 12](#_Toc136849649)

[Incident Handling Process: 12](#_Toc136849650)

[Incident Specific handling processes 13](#_Toc136849651)

[Unauthorized Access Attack – Incidence response 13](#_Toc136849652)

[Network Intrusion – Incident Response 15](#_Toc136849653)

[Server breach – Incident Response 17](#_Toc136849654)

[Physical Security breach – Incident Response 19](#_Toc136849655)

[Approvals 21](#_Toc136849656)

[References 22](#_Toc136849657)

# Revision History

|  |  |  |
| --- | --- | --- |
| Revision Date | Items Revised | Author |
| 01.06.2023 | IRP created | Loveth Adeh |
|  |  |  |
|  |  |  |

# Purpose and Scope

## Purpose

This Incident Response Plan aims to ensure the organization is well-prepared to manage cyber security incidents effectively and efficiently. In today's evolving threat landscape, cyber incidents are increasingly frequent and sophisticated, and it is crucial for us to be ready to respond, prevent, and detect such incidents. By establishing a plan, assembling a dedicated response team, and conducting regular exercises, we aim to enhance our incident response capabilities, contain damage, and mitigate further risks to the organization. This document outlines the structure, roles, responsibilities, incident types, and the approach to preparing for, identifying, containing, mitigating, recovering from, and learning from cyber security incidents, ultimately minimizing their impact on the operations. The primary goal of this Incident Response Plan is to ensure our organization can respond to cyber security incidents in a coordinated and efficient manner.

## Scope

This plan covers our networks, systems, data, cloud technologies, and individuals associated with them. The members of our Computer Incident Response Team (CIRT) are responsible for taking a leading role or actively participating in addressing cybersecurity incidents. CIRT is expected to get acquainted with this plan as the Incident Prevention Team (IPT) will report to the CIRT with the aim of swiftly identifying, containing, and mitigating incidents.

## Assumption

The assumption is made that the CSIRT has knowledge of the NSIT incident response process, and they have conducted training sessions and drills based on different scenarios.

## Planning Scenarios:

This plan is designed to respond to scenarios such as the following:

· Unauthorized access and usage

· Physical Security Breach

· Network Intrusion

· Server Breach

## Unauthorized Access attack:

Individual gains physical or logical access to network, system, or data without permission. A scenario where an administrator had left their workstation unlocked and unattended for a few minutes, providing an opportunity for the unauthorized individual to potentially access sensitive information or perform malicious actions.

## Network Intrusion:

A scenario where an inbound connection originating from a watchlist IP address is detected, indicating a potential intrusion attempt. A scenario where the attacker is targeting the organization's VPN server, which could potentially compromise the network and gain unauthorized access to sensitive information.

## Server Breach:

A scenario where there is a there a presence of unfamiliar and unusual directory names, along with suspicious files, indicates that the server has been compromised. The attacker might have gained root access to the server, which gives complete control over the system and the ability to manipulate or access sensitive data.

## Physical Security Breach:

A scenario where an unknown person gained physical access to the organization's premises or access to the company's Enterprise Resource Planning software or system. A scenario where an administrator had left their workstation unlocked and unattended for a few minutes, providing an opportunity for the unauthorized individual to potentially access sensitive information or perform malicious actions.

# Definitions

**Unauthorized access or usage**: unauthorized disclosure or theft of sensitive information, disruption or compromise of services, damage to system integrity, financial loss, reputational damage.

**Denial of service**: incidents that result in the temporary unavailability or disruption of systems or networks, whether caused by technical failures, human error, or malicious attacks.

**Incident response plan**: A documented set of procedures and guidelines outlining the steps to be taken when responding to and managing a security incident.

**Incident prevention plan:** A comprehensive strategy that identifies potential threats and implements measures to minimize the occurrence and impact of security incidents.

**Computer Incident Response Team**: A team responsible for responding to and managing computer security incidents within an organization.

**Integrity:** Data or information remains unchanged, uncorrupted, and authentic

**Availability:** Accessible and available at all times

**Confidentiality:** Protection of sensitive information from unauthorized access, disclosure, or exposure.

**Cyber security incident**: Activity that threatens the security, integrity, or availability of computer systems, networks, or data.

**Exploit:** Vulnerability or weakness in a computer system or network to gain unauthorized access or control.

**SLA:** Agreement between a service provider and a customer that defines the level of service, performance targets, and responsibilities of both parties.

**IRT:** Incident Response Team

**CSIRT:** Computer Security Incident Response Team

# How to Recognize a Cyber Incident

In Group7 Limited, the incident prevention team must look for any signs or indicators of system compromise, breach, misuse, or unauthorized access even with third-party providers. These indicators for recognizing an incident in some areas of attacks are listed below:

1. **Server Breach**

i. Any unusual or excessive login attempts to the server.

ii. Log anomalies (event logs or system logs) in response to any suspicious activities to breaches.

iii. Unexpected patterns in network traffic to and from the server.

iv. Changed file permissions or server configuration detected.

v. Any reports of unauthorized access or data breach provided by the monitoring tools or server administrators.

vi. High volume of data is being transferred to any other device in the network or outside the network.

2. **Network Intrusions**

i. Any unusual network traffic to and from a single or group of network devices.

ii. Detecting any unfamiliar IP address or domains in the network.

iii. Unresponsiveness of network system or crashes.

iv. Frequent network performance issues or device slowdown.

v. Unexplained changes in network configurations or inbound/outbound rules.

vi. Unauthorized access to network systems detected by any monitoring tool or network administrator.

vii. Presence of any unidentified networks or Wi-Fi connections.

3.  **Physical Security Breach**

i. Unauthorized access to physical entries or forced entry attempts.

ii. Any stolen or manipulated physical entities including computers, network devices, security devices, or storage equipment.

iii. Changing or turning off any surveillance cameras, biometric devices, alarms, or any physical security entry devices.

iv. Any suspicious entry into the building premises is a form of physical breach.

4. **Unauthorized Access**

i. Access to a network, server, or any devices within an organization without proper authorization.

ii. User accounts with their privileges escalated and granted permissions on the accounts and data without authorization.

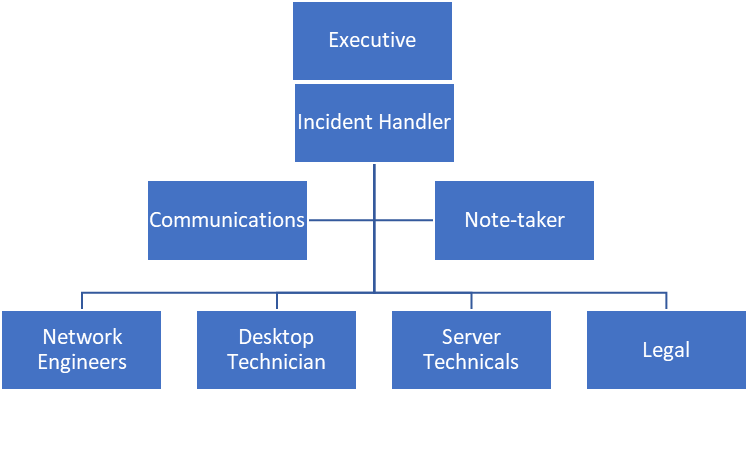
iii. Employees report any suspicious activities in their account or suspicious login.

iv. Changes in the log records for any unauthorized access into any of the devices.

v. Suspicious emails, pop-ups, or any activities reported by the users.

vi. Use of removable media like USBs, Hard Drives, or any I/O devices for unauthorized coping data from the devices.

# Cyber Security Incident Response Team (CSIRT)



## (CSIRT) Roles:

|  |  |
| --- | --- |
| CSIRT Role | Description |
| Executive | The role of reporting to board directors and other executives, as well as making executive decisions within the CSIRT, falls under the responsibility of this position. They are accountable for addressing all matters that require executive-level attention within the CSIRT. |
| Incident Handler | The Incident Handler serves as the primary triage role within the CSIRT, responsible for coordinating the team and initiating the Incident Response Plan to effectively investigate and respond to cyber security incidents. |
| Communication | Responsible for managing both public relations and internal communications. |
| Note Taker | The note-taker is responsible for documenting the progress of the CSIRT |
| Network engineers | Responsible to provides technical expertise to the response. |
| Desktop Technician | Responsible to provides technical expertise to the response |
| Legal | Legal Counsel providing legal expertise to the CSIRT |
| Server Technical | Responsible to provides technical expertise to the response. |

## (CSIRT) contacts:

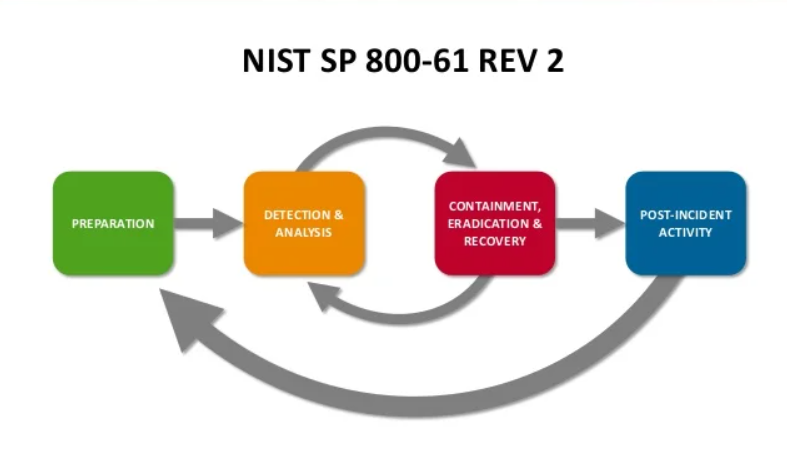
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Contact | Title | Email |
| Lead - Incident Handler | Loveth Adeh | 905 123 456 | Team Lead | l\_la@group7.ca |
| Backup - Incident Handler | Sajid Jazook | 548-888-5929 | Incident handler | a\_jazookahamed@group7.ca |
| Network | Nya Offiong | 122 090 567 | Manager | n\_offiong@group7.ca |
| Server | Anju Devassia | 909 567 1235 | Manager | adevassia@group7.ca |
| Legal | Ramiyah Nelda | 122 902 234 | Head of legal | rnelda@group7.ca |
| Note Taker | Dell Smart | 509 123 456 | Manager | dsmart@group7.ca |
| Communication | Jacks Deal | 509 456 789 | Manager | jdeal@group7.ca |
| Executive | Asdam Bills | 909657896 | President | abill@group7.ca |

## Incident Types:

|  |  |
| --- | --- |
| Type | Description |
| Unauthorized Access or Usage | Individual gains physical or logical access to network, system, or data without permission. |
| Physical Security Breach | Any event or incident which affects the physical assets including people or property impacting its security. |
| Network Intrusion | Unauthorized access to a network or system for malicious gains. |
| Server Breach | Unauthorized access to a server compromising its resources, data and commands by the malicious user. |

## Incident Handling Process:

The CSIRT team must follow the NIST incident response process starting from Preparation, Detection and Analysis, Eradication & Recovery and Post-Incident Activities.



# Incident Specific handling processes

## Unauthorized Access Attack – Incidence response

* The event should be reported right away to the designated security contact or the incident response team (IRT).
* The affected system or account must be separated from the network to stop additional unauthorized access.
* The IRT must acknowledge the occurrence and launch an immediate reaction.
* The incident response team and the IT division should work together to determine the extent and consequences of the unauthorized access.
* To stop continued unauthorized access, the compromised system or account must be temporarily stopped or unplugged from the network.
* Access control measures must be reinforced, such as using extra authentication methods, resetting compromised accounts' passwords, or disabling compromised accounts.
* Any compromised or malicious activity should be looked for on any affected systems, including servers and databases.
* All pertinent evidence, including system logs, network traffic logs, and any other artifacts connected to the unauthorized access, should be gathered, and preserved by the incident response team.
* To examine the hacked system or device, gather volatile data, and determine the tactics and tools utilized by the attacker, digital forensics techniques should be applied.
* Logs, system configurations, and user activity should be examined to determine the extent of the unauthorized access and any data or system compromise.
* The IRT should cooperate with law enforcement agencies, as necessary, to share information and aid in the investigation.
* Weaknesses or vulnerabilities that permitted unauthorized access should be quickly recognized and fixed.
* To keep systems and software up to date and secure against known vulnerabilities, patches and upgrades should be deployed.
* Compromised accounts or systems should be recreated with secure configurations or restored from known good backups.
* Management, legal counsel, and any affected users should be informed of the occurrence involving illegal access.
* To keep affected users and stakeholders informed about the occurrence and any essential steps they should take, lines of communication should be developed.
* Post-incident study must be carried out to pinpoint the source of the unauthorized access as well as any security flaws or weaknesses.
* The incident's lessons should be recorded, and recommendations for better security controls and procedures should be made.
* To improve future incident response capabilities, the incident response strategy should be amended considering the findings.
* Employees must participate in security awareness training programs to inform them of the dangers of unauthorized access and the value of following security rules and procedures.
* To keep staff members up to date on emerging dangers and recommended procedures for avoiding unauthorized access, it is important that ongoing security training and awareness initiatives must be developed.

## Network Intrusion – Incident Response

• Immediately after network intrusion is discovered, the incident response team needs to be notified.

• After acknowledging the notification, the incident response team should designate a lead responder to start the incident response procedure.

• The lead responder should collaborate with the network intrusion detection analyst to acquire more details about the intrusion, such as the affected systems, the originating IP address, and timestamps.

• To stop further unwanted access, the team should disconnect the compromised VPN server from the network and isolate it from the affected network.

• The firewall rules should be modified to prevent traffic from the IP address on the watchlist

• Disable or isolate any impacted systems or accounts

• To determine the user ID and associated username used for the authenticated session, the incident response team should perform a thorough investigation by examining the intrusion detection, firewall, and VPN server logs.

• To identify the attack paths, methodologies, and compromised systems, logs from intrusion detection systems, firewalls, and other network devices must be examined.

• Any network traffic or packet captures that are accessible must be examined to gather more proof.

• The incident response team should communicate with the IT division and evaluate the amount of harm brought on by the network intrusion, including any compromised systems, stolen data, or unauthorized access.

• To restore affected systems to a known secure state, use system backups or clean copies.

• To guarantee a coordinated reaction, the incident response team and the preventive team should work in conjunction with other pertinent teams, such as IT, network administrators, and cybersecurity specialists.

• To promote effective information sharing and decision-making, communication channels and procedures should be established.

• The incident response team should draft a thorough incident report that includes a timeline, a list of the steps taken, conclusions, and suggestions.

## Server breach – Incident Response

* The database administrator should be able to identify unusual and unexpected directory names.
* The administrator must immediately report the occurrence to the computer incident response team (CIRT).
* The CIRT should assemble a team with the necessary expertise and name a lead incident responder.
* The team should evaluate the seriousness and potential impacts of the breach.
* The CIRT should disconnect the compromised server from the network to prevent further unauthorized access.
* The team should search for and remove any malicious files or directories.
* The CIRT should look through the system logs to identify the attacker's entry point.
* The proper fixes, updates, or settings must be implemented in order to eliminate vulnerabilities.
* The CIRT must collect and preserve breach-related evidence, and forensic techniques must be utilized to collect and analyze relevant data including log files, timestamps, and system artifacts.
* The CIRT should conduct a thorough impact analysis to determine the breach's extent.
* The team should identify any possible losses or harm, compromised data, and impacted systems.
* It is necessary to tell key parties, such as management, legal, and the relevant departments.
* The CIRT must develop a communication plan to inform relevant stakeholders, including executive management, legal counsel, affected users, and regulatory agencies.
* Keep the lines of communication open and prompt throughout the incident response procedure.
* To bring the affected server and associated systems back online, the CIRT must develop a recovery plan.
* Use clean backups to restore the system to a known secure state.
* Patches and security updates must be installed in order to fix vulnerabilities.
* The CIRT should conduct a post-incident review to identify the response procedure's advantages and disadvantages.
* To improve incident response procedures in the future, lessons learned should be documented.
* A revision of the incident response plan is necessary in light of the findings and recommendations.
* The CIRT should implement better monitoring techniques in order to find and prevent similar intrusions in the future.
* To verify the effectiveness of security precautions, ongoing audits and assessments of security must be conducted.
* Staff members should get frequent training and awareness campaigns to strengthen security processes.

## Physical Security breach – Incident Response

* The system administrator must notify the physical security team that an unidentified person left her office and that there was suspicious activity.
* The event must be reported right away to the computer incident response team (CIRT).
* The physical security team needs to protect the area and impose access restrictions in order to stop further unwanted entry.
* The CIRT needs to acknowledge the incident and launch an immediate response.
* Law enforcement or the proper authorities must be informed, if necessary.
* The incident response team has to gather and save all available evidence, including as video surveillance, witness accounts, and any physical traces the intruder may have left behind.
* In order to guarantee the admissibility and integrity of the evidence, the chain of custody must be upheld.
* The CIRT should evaluate the consequences of the breach, taking into account any possible loss, compromise of sensitive data, or harm.
* To learn more about the occurrence, the team should examine security logs, access records, and system activities.
* If necessary, the incident response team should alert the necessary parties, including as executive management, HR, legal counsel, and law enforcement agencies.
* Internal lines of communication should notify staff members about the occurrence while preserving privacy and reducing anxiety.
* Digital forensics should be used to examine any hacked systems or devices and find potential data breaches.
* The CIRT should undertake a comprehensive investigation to find out what the intruder did.
* To learn more, it is advisable to speak with witnesses and other relevant parties.
* The physical security team should implement the required steps to fix vulnerabilities and stop upcoming breaches, such as tightening workstation security standards and increasing access control mechanisms.
* Check the afflicted workstation carefully for signs of tampering or compromise.
* The incident response team should help the payroll administrator change their login information and maintain the payroll system's security.
* To determine the underlying reasons, frailties, and holes in the physical security measures, the CIRT should perform a post-incident analysis.
* Lessons learned must be recorded, and suggestions for enhancements ought to be provided.
* To improve future incident response capabilities, the incident response strategy should be amended considering the findings.
* Employees should get security awareness training from the company, with a focus on the value of physical security measures and procedures.
* It is important to perform regular drills and exercises to evaluate the efficiency of security measures and response capabilities.

# Approvals

After reviewing the Security Incident Response Plan, the Incident Handler acknowledges that they are responsible for managing high or critical cybersecurity incidents or can delegate the responsibility to another qualified individual. The Incident Handler or their delegate is expected to handle the incident in a manner that minimizes additional risk to the organization. The incident will be addressed following a predefined process, which involves identifying, containing, eradicating, recovering from, and learning lessons from the incident

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible Name | Signature | Version | Date |
|  |  | 1.0 | 01.06.2023 |

## 

# 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](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-electronic-documents-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/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/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/](https://sansorg.egnyte.com/dl/6Btqoa63at/)?
* Rosencrance, L. (2023, February 7). *10 types of security incidents and how to handle them: TechTarget*. Security. https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them
* Kaspersky. (2023, April 19). *What is a security breach?.* www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach