CYBER SECURITY
INCIDENT RESPONSE PLAN

STATIONX

Cyber Security Incident Response Plan	
Approved By (Approver name)	
Owner	Head of Cyber Security
Author (Your name)	
Audit	Information Security Team
Issue Date	
Document Name	Cyber Incident Response Process
Version	1.0
Document Class	Restricted
Distribution (Google Drive | OneDrive | Sharepoint)	

Document Revision History			
Version	Author (your name)	Notes	Date
1.0		Document Creation	

Table of Contents

1. Introduction

Cyber attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

This document provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential. Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. It is also vital to build relationships and establish suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement).

This document describes the process by which any cyber security incident is managed and includes the high-level procedure for each step. This process will be initiated as an action from the overall _____ (Company name) incident management process, either as an internal ticket or as an action identified by a third-party provider.

2. Purpose

The purpose of this Cyber Security Incident Response Plan is to establish that _____ is well-prepared to effectively and efficiently manage cyber incidents. Cyber security incidents are becoming more frequent and sophisticated, with no organization immune from the potential threats they pose. It is imperative that organizations are adequately prepared to detect, prevent, and respond to such incidents promptly.

This comprehensive plan ensures _____ is ready to address inevitable cyber incidents. It contains a structured approach that ensures the appropriate resources are allocated efficiently, roles and responsibilities are clearly defined, and a thorough methodology for the detection, containment, eradication, recovery, and post-incident analysis of incidents is followed.

The primary objective of the Cyber Security Incident Response Plan is to ensure that _____ is well-prepared and organized to respond to cyber security incidents. It will minimize the impact of incidents and reduce recovery time after an incident occurs.

3. Scope

This Cyber Security Incident Response Plan applies to all IT assets that fall under the jurisdiction of _____ This includes networks, computer systems, data, and personnel (e.g. employees, vendors, contractors).

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 combating cyber security incidents.

4. Definitions and Acronyms

The Cyber Security Incident Response Plan uses the following key terms to describe the incident response process. Ensure you are familiar with their definitions

Key Term	Definition
Cyber Incident	Any incident that occurs by accident or deliberately that impacts business processes or IT systems. An incident may be any event or set of circumstances that threaten the confidentiality, integrity, or availability of computer systems, networks, services, or data within [ ]. This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by [ ].
Cyber Incident	Malicious software is any software or code that is designed to harm, exploit, or compromise computer systems, networks, or user data
Ransomware	A type of malware that is designed to encrypt a victim's computer system to lock them out of their data. The attacker will then demand a ransom for the release of said data.
Denial of Service (DoS)	A cyber attack that aims to make a remote service unavailable to its intended users by flooding the service with illegitimate requests.
IT	Information Technology
IRT	Incident Response Team
DFIR	Digital Forensics and Incident Response
CISO	Chief Information Security Officer
EDR	Endpoint Detection Response (EDR) is a security tool that is installed on endpoint devices (e.g. laptops, desktops, mobile phones) to detect and block malicious activities.
WAF	Web Application Firewall (WAF) is a special type of firewall designed to protect web applications from cyber attacks.
IDS / IPS	Intrusion Detection System (IDS) is a security tool installed within a network to detect potentially malicious activity. An Intrusion Prevention System (IPS) is installed in a network to block potentially malicious activity.
AV	Anti-Virus (AV) is software designed to protect computer systems and networks from malicious activities.
Phishing	An attack technique where an attacker will pose as a trustworthy source to deceive a victim into divulging sensitive data, clicking on a link, or executing malware. Phishing can be done through email, text messages, phone calls, or social media messages.

Botnet	A network of Internet-connected devices that have been taken over by malware that connects to a central command and control (C2) server. A threat actor will use a botnet to perform various cybercriminal activities, such as a Distributed Denial of Service (DDoS) attack.
Confidentiality	Confidentiality refers to the protection of sensitive or private information from unauthorized access or disclosure, either maliciously or accidentally. It is part of the cyber security CIA triad and a fundamental pillar of [ ]'s business operations to defend against attacks.
Integrity	Integrity is the assurance that computer systems, networks, services, and data are accurate, reliable, and trustworthy. They have not been altered or tampered with by unauthorized individuals. It is part of the cyber security CIA triad and a fundamental pillar of [ ]'s business operations to defend against attacks.
Availability	Availability refers to ensuring that computer systems, networks, services, and data are readily accessible and useable when needed by authorized authorities. It is part of the cyber security CIA triad and a fundamental pillar of [ ]'s business operations to defend against attacks.
Exploit	A piece of software or code that can take advantage of a vulnerability or security weakness in a computer program, operating system, application, or network to carry out malicious actions.
Vulnerability	A weakness or flaw in a computer program, operating system, application, or network that can be exploited by a threat actor to compromise the confidentiality, integrity, or availability of the system.
Zero-day	A software vulnerability or security flaw in a computer program, operating system, or application that a vendor has not released a patch or security update to fix and can be exploited by a threat actor.
IOCs	Indicators of Compromise (IOCs) are artifacts or evidence that are left behind after an intrusion by a threat actor. They are used to identify or detect if a security breach has taken place, who is responsible, and help to mitigate threats.
SLA	A Service Level Agreement (SLA) describes the guaranteed measure of service availability provided by [ ] or a third-party contractor. Usually, financial repercussions occur if the service availability drops below the prescribed SLA.
War Room	A war room (a.k.a command center or situation room) is a dedicated meeting room where key decision makers and members of the IRT gather to collaboratively and rapidly respond to an incident.
Stakeholder	An individual, group, or organization with an interest, concern, or influence in a particular issue or project. Stakeholders can be internal or external, and it is important to identify and communicate critical decisions with them.

Threat Actor	An individual, group, or organization that threatens the security, confidentiality, integrity, or availability of ’s systems, network, or data. They could be a criminal gang, nation-state, or political activist.
C2	Command and Control (C2) server is used by a threat actor to control systems they have infected with malware.
PUP	A Potentially Unwanted Program (PUP) is software that poses a risk to a system or network but is not strictly defined as being malicious.

5. Incident Response Policy

At , we recognize the importance of safeguarding our information assets, the privacy of our customers, and the integrity of our business operations. We the rise of sophisticated cyber threats, our commitment to cyber security is unwavering, and our dedicated to responding to cyber security incidents efficiently.

We are committed to the following:

1. Rapid Detection: Promptly detecting and identifying cyber security incidents so that they can be responded to in a timely manner
2. Prompt Response: Once detected, cyber incidents will be responded to with the utmost urgency, and the incident response team will take immediate action to contain, eradicate, and recover from an incident.
3. Effective Communication: We pledge to ensure effective and transparent communication with relevant stakeholders and third parties to keep them informed about an incident, its impact, and actions taken to address it.
4. Clear Roles and Responsibilities: Members of the IRT will have clearly defined roles and responsibilities to ensure a coordinated and efficient effort when responding to incidents.
5. Post-Incident Analysis: is committed to continuously improving its cyber security program. With this in mind, after each incident, a comprehensive post-incident analysis will be performed so that the organization can learn from the experience and strengthen its defenses against future threats.
6. Compliance and Reporting: We will diligently adhere to legal and regulatory requirements for incident reporting and response.
7. Training and Awareness: We are committed to raising the awareness of our employees about the risk cyber threats pose to the organization and providing the appropriate employees with training to tackle these threats.
8. Third-Party Collaboration: have established relationships and agreements with external service providers and partners to ensure that prompt incident response is upheld in our extended network.

This commitment to responding to cyber security incidents promptly is a fundamental element of our company’s cyber security strategy. It underlines our dedication to maintaining trust, protecting data, and minimizing the potential impact of security incidents on our organization and its stakeholders.

6. Incident Response Team (IRT)

The team that is assigned to perform the incident response process is defined in the following table, along with their roles and responsibilities.

Role	Responsibilities	Contact Details
Incident Response Manager	Distribution of work/priorities, coordinating response activities, and logging updates on the case management platform.	
Head of Security Operations	Identify risk and associated priorities and work with relevant stakeholders to provide internal comms and training.	
Lead Security Analyst	To analyze how the incident is taking place, categorize the incident, and collect all logs and information as evidence.	
IT Representative	Action shutting down any systems and accounts. Provide any logs for endpoints or networks owned by IT.	
Legal Advisor	Approve communications and approve the wording of reporting to governance organizations.	
PR/Communications Officer	Responsible for major incident communication to key stakeholders and press.	
Data Protection Officer	To advise the business about the identification and disclosure of a data breach to governance organizations.	
Digital Forensics Partner	To assist in the analysis, containment, eradication, and recovery from a cyber incident. Provide technical expertise in preserving forensic data which may need to be used for prosecution.	
CISO	Accountable executive for protecting cyber security within the organization. Responsible for reporting to board directors and other executives.	

It is important to keep the contact details of the IRT members up-to-date so they can be quickly reached whenever a cyber incident arises.

7. Incident Identification

Each cyber security incident needs to be accurately identified so that the incident response team can respond to the incident using the appropriate analysis, containment, eradication, and recovery procedures.

The process for identifying potential security incidents at _____ is to monitor for alerts on the following systems:

_____ (security solution 1 (e.g. EDR, AV, firewall, WAF, IDS/IPS, etc))

_____ (security solution 2 (e.g. EDR, AV, firewall, WAF, IDS/IPS, etc))

_____ (security solution 3 (e.g. EDR, AV, firewall, WAF, IDS/IPS, etc))

Once an incident is detected, it is managed using the case management platform

_____ (incident case management platform (e.g. ServiceNow))

8. Incident Classification

It is important to accurately classify all cyber security incidents based on their severity, their impact on the organization, and the urgency in which they need to be responded to. The following Incident Severity Matrix provides a matrix to classify an incident's severity based on its impact on the organization. Use it to assign a severity to each cyber incident.

Severity	SLA	Description	Impact
P1 Critical Incidents	Response time: 20 minutes Resolution time: 4 hours	A cyber incident that is disrupting _____ 's essential services or affects any internal/external business that leads to significant financial loss or life-threatening situation.	• _____ can no longer provide core services. • Classified data such as PII or business-sensitive information has been accessed, stolen, changed, or deleted. • Over 50% of the workforce cannot work, or critical systems cannot be accessed for an unknown period of time. • Recovery from an incident is impossible without external help. • Long-term reputation damage.

P2 Significant Incidents	Response time: 30 minutes Resolution time: 8 hours	A cyber incident that has a serious impact on business operation, affects internal business functions, and leads to financial loss or serious reputational damage	• [ ]'s internal business functions have been disrupted, and the ability to perform some services has been lost. • Sensitive data has been accessed or exfiltrated. • Recovery is unpredictable, and additional resources or help is needed. • Serious reputational damage.
P3 Moderate Incidents	Response time: 24 hours Resolution time: 5 business days	A cyber incident that has a substantial or moderate impact on internal business operations, but core services to external parties are still functioning as usual.	• [ ]'s internal business functions have been disrupted. • More than 10% of the workforce cannot work or access critical systems. • Time to recovery is predictable butmay need additional resources and help.
P4 Minor Incidents	Response time: 24 hours Resolution time: 5-10 business days	A cyber incident that has limited impact on certain individuals or systems and has no other impact on business operations or concerns to external parties.	• Minimal effect on internal business functions. • Less than 10% of the workforce is unable to work or access required systems for a short period of time. • Time to recover is predictable with existing resources.

Once an incident has been assigned a severity, it is classified using the following Incident Classification Matrix. This is so that incident responders can apply the appropriate analysis, containment, eradication, and recovery procedures to respond to the incident effectively.

Incident Classification	**Description**
Ransomware	Software that is designed to encrypt a system and hold it for ransom. Detected on endpoint systems or reported by an employee.
Denial of Service (DoS)	A flood of traffic designed to take down a website. Can also apply to phone lines, other Internet-facing systems, or internal systems. Identified through network traffic or reported by an employee.
Phishing	Emails, SMS messages, or phone calls that attempt to convince an employee to click on a link, download an attachment, or divulge sensitive information. Reported by an employee.
Unauthorized Access	Access to systems, accounts, or data by an unauthorized person (internal or external). Detected by endpoint systems or seen in network traffic.

Data Breach	Lost/stolen devices or hard copy documents; unauthorized access and exfiltration of data over the network. Detected by endpoint systems, seen in network traffic, or reported by an employee.
Potentially Unwanted Program (PUP)	Software that is considered suspicious and may contain hidden malware (e.g. games, crypto-tools, etc.). Detected on endpoint systems.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Detected on endpoint systems.
Suspicious Network Communication	Communication with a suspicious or malicious IP address or domain name (e.g. C2server, TOR node, botnet, etc.). Detected by endpoint systems or seen in network traffic.
Hacking Tool	Software that could be used to gain unauthorized access to computer systems, networks, or data. Detected by endpoint systems.
Scanning	Unauthorized, abnormal, or suspicious network traffic that is designed to scan a range of IP addresses for vulnerabilities, open ports, or services on target systems. Seen in network traffic.
Brute Force Attack	A flood of network traffic that systematically tries all combinations of passwords or encryption keys to gain unauthorized access to a computer system or account.
Test	Testing activity that is designed to emulate a cyber incident so that detections or mitigations can be implemented to protect against it.

9. Incident Response Process

adheres to the common cyber incident resolution structure which includes the following phases:

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

Each of these phases are detailed below.

9.1 Preparation

Preparation is the process of readying the organization for a cyber attack. It involves implementing preventative measures, regularly testing these measures, and training employees to respond effectively to cyber incidents.

To effectively prevent cyber incidents, _____ implements the following measures:

- _____ (preventative measure 1)
- _____ (preventative measure 2)
- _____ (preventative measure 3)

9.2 Detection and Analysis

Detection and analysis involves the identification and investigation of cyber incidents. This includes incident triage to determine the severity of an incident and root cause analysis to assess the incident's impact on the organization.

_____ uses the following methods to detect and analyze cyber incidents:

- _____ (security tool | log source | user report)
- _____ (security tool | log source | user report)
- _____ (security tool | log source | user report)

9.3 Containment, Eradication, and Recovery

The containment phase involves stopping any further damage to the business and/or its IT systems and preventing the situation from becoming worse by removing the direct threat from the environment.

To contain incidents, _____ has the ability to isolate impacted endpoint machines and networks.

Once contained, the eradication phase can begin. This phase involves re-instating affected systems to their original operational status. Methods include rebuilding systems from a previous backup and resetting compromised accounts.

After eradication, the recovery phase begins. Systems are re-introduced back into the larger IT environment and brought back to a fully functioning status. An increased level of monitoring should be implemented during the recovery phase, and, if necessary, patches should be installed to prevent any further exploits.

9.4 Post-Incident Activity

After _____ has recovered from a cyber incident, the post-activity phase can begin. This phase involves a comprehensive assessment of how a cyber incident occurred. It includes holistically assessing the failures in the people, processes, and technology designed to protect the organization from cyber threats and learning from these failures.

All lessons learned from the incident should be documented, and processes started to implement mitigations to prevent the incident from happening again.

10. Communication Plan

The _____ Cyber Security Incident Response Communication Plan outlines the strategies, procedures, and roles for effective communication during cybersecurity incidents. The plan aims to maintain transparency, inform stakeholders promptly, and facilitate efficient collaboration among IRT members.

Key Objectives:

1. **Timely Notification:** Ensure prompt notification and information sharing during incidents.
2. **Clear Roles:** Define the roles and responsibilities of individuals and teams involved in communication.
3. **Consistent Messaging:** Provide consistent and accurate information to all stakeholders.
4. **External Relations:** Manage external communications with regulatory bodies, partners, vendors, and the public.

Communication Team:

	(Name)	(Title)
• CISO:		
• Incident Response Manager:		
• PR/Communications Officer:		
• Head of Security Operations:		
• Lead Security Analyst:		
• Legal Advisor:		
• Designate Spokesperson:		

Documentation and Record Keeping:

- All communication related to the incident will be documented in detail, including date, time, content, and recipients.
- These records will be maintained for legal and regulatory compliance.

Testing and Drills:

- Periodic testing and drills of the communication plan will be conducted to ensure the readiness of the IRT.

Plan Review:

- The communication plan will be reviewed and updated as necessary to address evolving threats and improve response effectiveness.

10.1 Internal Communication

1. **Incident Reporting:**
   - Employees will immediately report any potential incidents to the _____ IRT through _____ (contact information)
   - The incident will be documented using the incident reporting form.
2. **Incident Response Team Activation:**
   - The Incident Response Manager will activate the IRT.
   - Notification will be sent to relevant team members through _____ (notification method)
3. **Incident Updates:**
   - The Lead Security Analyst will provide regular updates to the IRT.
   - Updates will be communicated via _____ (communication channel)
4. **Escalation Procedures:**
   - The IRT will follow predefined escalation procedures for significant incidents.

10.2 External Communication

1. **Notification to Regulatory Bodies:**
    - The Legal Advisor will assess the necessity of notifying regulatory bodies in accordance with applicable laws and regulations.
    - If required, notification will be made through the appropriate channels.
2. **Partners and Vendors:**
    - The PR/Communications Officer will communicate with partners and vendors as necessary, providing updates on the situation.
3. **Public Announcement:**
    - _____ will issue a public announcement through the Designated Spokesperson in case of incidents that may affect customers or the public
    - The message will be clear and concise and will not disclose sensitive information.

11. Training and Awareness

To effectively prepare for cyber incidents, _____ is dedicated to ensuring employees are aware of the risks posed by cyber threats. The company is also dedicated to providing employees tasked with defending the organization from cyber threats with the appropriate resources and training required to perform this task.

To meet these objectives, _____ has the following programs in place to prepare employees for responding to incidents.

Employee Awareness Programs:

_____ (awareness program 1)
_____ (awareness program 2)
_____ (awareness program 3)

Employee Training Programs:

_____ (training program 1)
_____ (training program 2)
_____ (training program 3)

12. Maintenance and Review of the IRP

The Cyber Incident Response Plan will be reviewed and updated regularly.

Auditor	Information Security Team
Review Period	Annually or as required
Review Date	
Next Review Date	

13. Appendices

Appendix A: Incident Report Form

Provide a template for documenting incidents.

Appendix B: Contact Lists

Internal Contacts

Role	Name	Title	Phone	Email
Incident Response Manager				
Head of Security Operations				
Lead Security Analyst				
IT Representative				
PR/Communications Officer				
Data Protection Officer				
CISO				

External Contacts

Role	Name	Title	Phone	Email
Digital Forensics Partner				
Legal Advisor				

Appendix C: Checklist and Log Forms

Provide forms for documenting actions taken during an incident response.