Netradyne Security Incident Response Plan

v1.3

Internal and Confidential

netradyne

TABLE OF CONTENTS

Document Control

Document ID	NDIRP2020001
Document Name	Netradyne Security Incident Response Plan
Document Status	Released
Document Released Date	29-NOV-2020
Document Author	Gautam Kumar
Document Content Contributors	Rajeev Ghosh, Sudhansu Kumar, Vijaykumar Dalal, Kavitha N Shetty
Document Signatory	Saravanan Sankaran
Document Owner	Saravanan Sankaran
Document Version	1.3
Information Classification	Internal

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised By
1.0	29/NOV/2020	Basic Version (High Level Coverage)	Infosec
1.1	20/OCT/2021	Revised Draft Version (Detailed Process Documentation)	Sudhansu Kumar
1.2	22/APR/2022	Revised Released Version (Formatted & aligned with Std. Template)	Gautam Kumar
1.3	17/APR/2023	Annual Review Performed	Gautam Kumar

Document Review/Approval

Date	Signatory Name	Organization/Signatory Title	Comments
29/NOV/2020	Vinay Rai	Vice President, Cloud	
20/OCT/2021	Saravanan Sankaran	Sr. Director – Infosec & IT	
22/APR/2022	Saravanan Sankaran	Sr. Director – Infosec & IT	
17/APR/2023	Saravanan Sankaran	Sr. Director – Infosec & IT	

Distribution of Final Document

Name	Organization/Title
Netradyne	

1 Purpose

This document outlines the plan for responding to information security incidents at Netradyne including defining the roles and responsibilities of participants, the overall characterization of incident response, relationships to other policies and procedures and guidelines for reporting requirements.

Due to the wide variety of incidents that could face and the rapid advancement of threats against the organization, its data and systems, this document is designed to provide guidance in reacting to data security incidents, determination of their scope and risk, and ensuring an appropriate response to information security incidents, including communication of incidents to the appropriate stakeholders, and reducing the incident from re-occurring.

Anyone suspecting an exposure of organization data or systems should immediately contact:

Information Security Team: Infosec@netradyne.com

IT Team: IT@netradyne.com

Privacy Team: DPO@netradyne.com

2 Scope

The scope of this process is to assist the Security Incident Response Team (SIRT)in mitigating the risk from the IT security incidents by establishing the guidelines on detecting, investigating and handling it effectively. The scope of this process provides a structured and planned approach to:

a. detect, report and assess information security incidents
b. responds to and manage information security incidents
c. resolve the information security event or issue in a timely manner
d. This process excludes:
e. the prevention of cyber security attacks, including detailed cyber security threat analytics
f. deep technical investigation tools and techniques, typically used by commercial cybersecurity incident response or forensics experts
g. cyber security insurance
h. in case of any PII / SPI / PHI /Sensitive incident gets reported, Data privacy office process would be followed as per the standards

3 Roles and Responsibilities

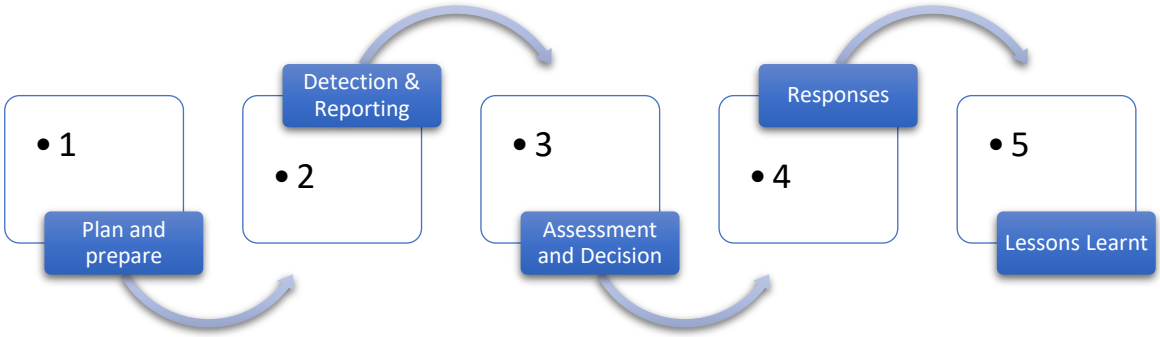
Roles and responsibilities specific to this document are included below:

Role	***Responsibilities***
Owner	• Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. • Is the point of contact for the document. • Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process.
Reviewers/Stakeholders	Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality)

Approvers	The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead.
Document Release	Document Owner/team to work with repository administrator to make release version available.

4 Procedure

The incident response and management process consist of five distinct phases:



4.1 PLAN AND PREPARE

Plan and Prepare phase primarily consist of the following activities:

- Information security incident management policy and commitment of top management
- Information security policies, including those related to risk management, updated at organization, system, service and network levels
- Information security incident management plan
- SIRT establishment
- Relationships and connections with internal and external organizations
- Technical and other support (including organizational and operational support)
- Information security incident management awareness briefings and trainings
- Information security incident management plan testing
- Use Case and Data Model Management

4.2 DETECTION AND REPORTING

Information security incident management involves the detection and collection of information associated with and reporting on occurrences of information security events and the existence of information security vulnerabilities by manual or automatic means. In this phase, events and vulnerabilities might not yet be classified as information security incidents.

- Monitor & log System and Network Activity for the detection of any information security event
- Detect & report the event: Perform 24X7 monitoring & support to Detect and report the occurrence of an information security event or the existence of a threat, either manually through ITSM tool or by automated way through the monitoring systems
- Collect additional details on the event or threat: Collect additional information on an information security event or threat identified. Any observation involving PII data will be immediately bring to the notice of Data Privacy Office for further investigation from DPO along with SIRT
- Collect situational awareness information: Collect situational awareness information from internal and external data sources including local system and network traffic and activity

logs, external feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies
- Log all activities, results and related decisions for future analysis
- Secure storage of the evidence: Secure the digital evidence gathered as part of this investigation and store/preserve in a secure way to retain and maintain the integrity of the evidence
- Escalate, on an as-needed basis throughout the phase, for further review or decisions

4.2.1 Netradyne ServiceDesk

Employees who are not accessible to ITSM tool or any individual shall report the information security incident to SIRT through Netradyne ServiceDesk+ or writing an email to infosec@netradyne.com. ServiceDesk person would internally create an information security incident ticket on ITSM tool.

4.2.2 ITSM tool

All employees shall report the information security incident through ITSM portal itservicedesk.netradyne.com

4.2.3 Reporting to SIRT

Employees or any individual shall report any information security incidents to the info sec team by sending email to Infosec@Netradyne.com. This mailbox is being continuously monitored by the Security team and incidents would be recorded and investigated.

4.2.4 Security Information and Event Management

Incidents are detected by SIEM solution. SIEM primarily collects the logs from different device sources, aggregates and incidents are flagged based on the defined correlation rules (use cases). These incidents are further recorded and investigated

4.3 ASSESSMENT AND DECISION

Information security incident management involves the assessment of information associated with occurrences of information security events and the decision on whether to classify events as information security incidents.

Once an information security event has been detected and reported:

- Communicate the responsibility for information security incident management activities through an appropriate hierarchy of personnel with assessment and decision making
- Provide formal procedures for each notified person to follow, including reviewing and amending reports, assessing damage, and notifying relevant personnel
- Follow established guidelines for documentation of an information security event and the subsequent actions for the information security incident

4.3.1 IDENTIFICATION

In the identification phase, Incident responders or Security Analysts would classify whet her they are dealing with an event or an incident. This process involves, collection of all the available information, which shall be obtained from automated systems (SIEM etc.,) or Employee reported incidents or customer reported incidents. This process also involves checking out the areas of the affected system(s). It includes suspicious entries in system or network accounting, excessive login attempts, unexplained new user accounts, unexpected new files, password sharing, unauthorized access, malware, policy violation, potential threat, loss of company asset etc.

4.3.2 CONTAINMENT

In the containment phase, primary focus shall be on limiting the damage caused to the systems and prevent any further damage from occurring. This includes short and long-term containment activities.

Determination of what happened to the system(s), computer(s) or network shall be performed. A systematic review shall be carried out to identify the incident type(s):

- bit-stream copies of the drives
- real-time memory
- network devices log
- system logs
- application logs
- and other supporting data

The essential areas of coverage are.

- Protecting and keeping available critical computing resources where possible
- Determining the operational status of the infected computer, system or network

Determine the operational status of the infected system and or network, by any of the below listed three options:

- Disconnect system from the network and allow it to continue stand-alone operations
- Shut down everything immediately
- Continue to allow the system to run on the network and monitor the activities

4.3.3 Classification of severity, SLA & Escalations

Severity of the Information security incidents are classified as per the incident & Risk:

- Severity 1-CriticaI
- Severity 2-High
- Severity 3-Medium
- Severity 4-Low

Note: Severity of the incidents pertaining to Customer Sensitive Data will be classified based on the Customer input on the incident.

All Incidents are classified into low, medium, high and critical depending on the severity. The criteria to determine and classify Risks and Incidents are based on four broad categories namely financial impact, regulatory impact, reputation impact and technical impact. Other impacts include contract breach, service level assessment breach, non-availability of back-up, impact on employee for privacy related incidents.

While determining the risk category, each of the Risks and Incidents should be applied against each of the above-mentioned impact criteria and the most adverse consequence should be taken into consideration for the risk category determination. For example, if a given Risk and/or Incident may lead to a potential obligation to report to a regulatory authority but does not exceed USD 50 million, then such a Risk or Incident should be classified as Critical.

Determination of risk category can be a combined decision of CISO/DPO/Infosec/IT/HR

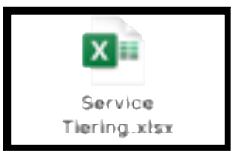
4.3.3.1 Incident Classification:

- The SIRT shall perform an assessment of the incident priority using the factors in the table below.

- Given the established priority, the incident will be allocated a Service Level which determines the timelines mentioned

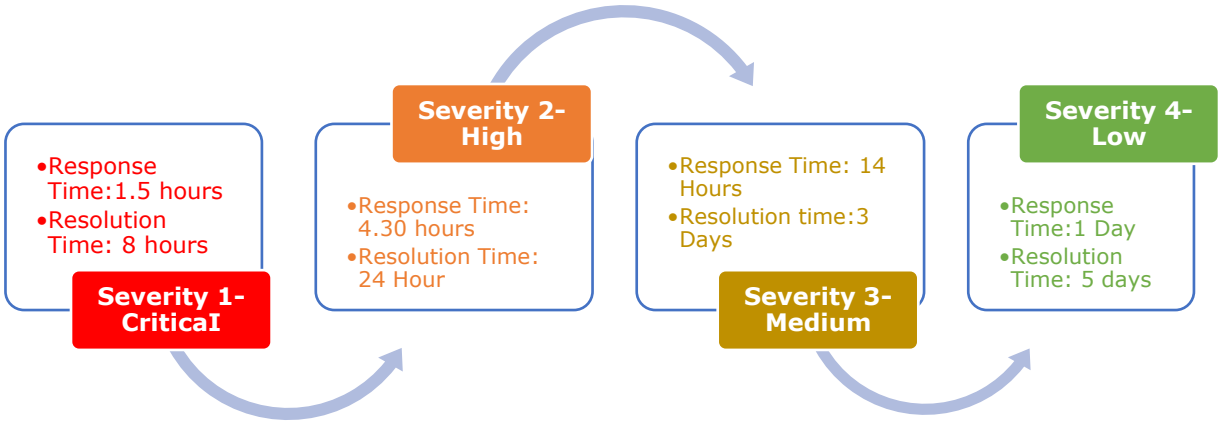
Priority	Factor	Examples of incident
Critical	An incident affecting the entire organization	Business disruptions resulting from malicious activity that results in > 50% degradation Any incident that impacts the availability of perimeter security infrastructure Exposure of unencrypted, unmasked, or insufficiently masked University confidential or sensitive information (Health Data/PII) into the public domain. This includes any data that could have a negative impact on the Organization's reputation. - Denial of service - Compromised Asset (critical) - Internal Hacking (active) - External Hacking (active) - Virus / Worm (outbreak) - Destruction of property (critical)
High	An incident affecting multiple facilities, User Groups or networks	Compromised privileged account credentials Incident involving Highly Critical assets >10% of Organization's users unable to use IT/any other resources Potential for involvement of law enforcement Active attack incidents by unknown attackers that impact the Organization's servers Exposure of unencrypted, unmasked, or insufficiently masked Organization's confidential or sensitive information (sensitive/Health Data/PII) into the public domain or to an unauthorised third party - Internal Hacking (not active) - External Hacking (not active) - Unauthorized access. - Policy violations - Unlawful activity. - Compromised information. - Compromised asset. (non-critical) - Destruction of property (non-critical)
Medium	An incident affecting small part of facility or network or a user	Malware incidents that don't fall in a higher severity Data loss incidents not involving sensitive information Confirmed phishing campaign that impacts only few users - Email - Forensics Request - Inappropriate use of property. - Policy violations which has minor impact
Low	Incident which does not fall into any of the above category with minor impact	Some localised inconvenience, but no impact to the Organization.

4.3.3.2 **Service Tiering:**



4.3.3.3 SLA & ESCALATION MATRIX

SLA for resolution of incidents is as below,



Note:

As there will be dependency with multiple stakeholders while handling incidents, the SLA defined above is applicable only for the period that the incident lies with SIRT.

SLA for HR has been defined as per their internal process, which is not covered under Incident Management's investigation timeframe.

4.3.3.4 **Escalation matrix within SIRT:**

Name	Title	Email	Contact
Vivian Preetham	TPM - Cloud	vivian.preetham@netradyne.com	Backup Contact
Sudhansu Kumar	Senior Staff Analyst -Risk and compliance	sudhansu.kumar@netradyne.com	Primary contact
Saravanan Sankaran	Senior Director - Infosec & IT	saravanan.sankaran@netradyne.com	Escalation
Roshan Mathews	Senior Director - Devops	roshan.mathews@netradyne.com	Escalation
Vinay Rai	Senior Vice President, Cloud	vinay.rai@netradyne.com	Escalation

4.3.4 HANDLING NOTICES FROM REGULATORY AUTHORITIES:

Netradyne is required to handle and act on the notices (e.g. Information Notice, Enforcement Notice, Correction Notice etc.,) received from the regulatory authorities of respective countries.

These notices can come either in the form of both soft or/and hard copy (via courier) to Netradyne registered office address of that country and needs to be responded immediately

4.3.5 ERADICATION

This stage emphasis to ensure a clean system ready to be restored. It could either be a complete reimage of a system, or a restore from a known good backup.

Eradication is the process of getting rid of the issue on the computer, system or network. Appropriate incident response procedure, appropriate to the incident, if the eradication is not feasible, all the affected systems would be isolated from the network and detailed investigation shall be carried out.

Primary aspects of eradication are:

- Clean-up usually consists of running the antivirus software, uninstalling the infected software, rebuilding the OS or replacing the entire hard drive and reconstructing the network.
- Notification always includes relevant personnel, both above and below the SIRT manager in the reporting chain.

Root Cause Analysis of the incident is carried out and immediate correction would be taken. Corrective measures are proposed to relevant stakeholders for avoiding the recurrence of the incident.

4.3.6 RECOVERY

At this point, determination whether to bring the system back into production and how long the affected system to be monitored for any signs of abnormal activity.

Two steps for recovery:

- Service restoration, which is based on implementing corporate contingency plans
- System and/or network validation, testing, and certifying the system as operational

If affected system(s) are not recoverable, it shall be forensically wiped-off and the system shall be rebuilt. Performing a scan for any known vulnerabilities or the infections that was observed.

4.3.7 FOLLOW-UP

The lessons learnt while the investigation is incorporated to the knowledge base repository and the process improvement (if any) will be updated back into the incident response process to produce better future outcomes and additional defences.

During the analysis/investigation on the incident, gaps on the current process been followed will be documented along with the Root Cause analysis and mitigation steps. Based on the incident and the gaps identified, if at all a change in the process is required, the same will be proposed to the respective process owner.

Upon the completion of incident investigation, the investigation summary/report will be shared with HRD for further course of action [disciplinary action]. The best practices and the lessons learnt during the investigation of an incident will be documented and a case study on the incident covering the details of the incident (in generic), root cause analysis and preventive & mitigation steps, will be published.

4.3.8 Classify the incident for closure

If the investigation is conclusive, complete and shall be considered for closure, update the status of the incident as Resolved. If it is not closed and require further detailed investigation, incident would be escalated.

4.3.8.1 Incident Closure

Incident is marked as Resolved and Root Cause is updated on the system.

4.3.8.2 Knowledge Base

Knowledgebase is updated with the lessons learnt during investigation, for future references.

4.4 RESPONSES

A dedicated SIRT person is designated to handle security incidents. That designated person will liaise with every stakeholder. Post the investigation closure, an incident Investigation Report would be prepared by the incident handler and would be shared with HR for further proceedings in terms of disciplinary action.

- When required, for any response to the external team, the responses would be given of routed through designated team.
- Investigate incidents as required and relative to the information security incident classification scale rating. The scale should be changed as necessary. Investigation can include different kinds of analyses to provide a more in-depth understanding of incidents.
- Review by the SIRT to determine whether the information security incident is under control, and if so, perform the required response. If the incident is not under control or it is going to have a severe impact on the organization's operations, follow escalation to the appropriate team.
- Assign internal resources and identify appropriate stakeholders to respond to an incident.
- Escalate as needed throughout the phase for further assessments or decisions.
- Log all activities, results and related decisions for later analysis
- Store the digital evidence gathered securely, and secure preservation is continually monitored, for legal prosecution or internal disciplinary action
- Communicate the existence of the information security incident and share any relevant details (e.g., threat, attack, and vulnerability information) with relevant internal stakeholders in accordance with SIRT communication plans and information disclosure policies
- After recovery from an incident, a Post Incident Activity will be initiated depending on the nature and of the incident. This activity includes
    - Investigation of the information pertaining to the incident,
    - Investigation of other relevant sources such as involved personnel, and summarized report of the investigation findings
- Once the incident has been resolved, it will be closed according to the requirements of the SIRT and all stakeholders would be notified

4.5 LESSONS LEARNT

This phase involves learning lessons from how incidents have been handled. Lessons learnt while handling incidents will be documented and used in the continuous improvement of Information Security Management Systems. During the incident investigation, the identified Information Security Weakness would be remediated/mitigated with appropriate measures.

SIRT will also be analysing the reported incidents on a quarterly basis and publish the Security Incidents & Breach Analysis report to the management. This report includes the dashboard of the incidents of the previous year and the trend of incidents compared with its previous years. Also, the Root Cause of every incident category will be analysed, and appropriate Corrective/Preventive measures will be documented.

- Identify the lessons learnt from information security incidents.
- Review, identify and make improvements to information security control implementation, if required the information security incident management policy. Lessons are based of one or many information security incidents Improvements that are supported by metrics.
- Review, identify and make improvements to the organizations existing information security risk assessment and management reviews.
- Review the effectiveness of the processes, procedures, reporting formats and organizational structure were in responding to, assessing and recovering from information security incidents. Based on the lessons learnt, identify and make improvements to the information security incident management plan and its documentation.
- Update the knowledgebase repository on the lessons learnt for the future references

5 Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

6 Exception

Exception to this procedure must be approved through the Netradyne Exception Process.

Exceptions may be granted in cases where security incidents are mitigated by alternative methods, or
in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate business needs. To request a security exception, contact the InfoSec team.

Below are the examples of exceptions:

- Patching on Production systems may require complex testing and installation procedures
- Inability to remediate a vulnerability due to lack of solution
- Incident Remediation are not feasible with application and business requirements

For any exception in Security Incident Management on valid reasons, approvals are needed from System Owner (First Level) and InfoSec Head (Second Level)

7 Terms/Acronyms

Term/Acronym	Definition
Information Security Incident Management	Exercise of a consistent and effective approach events that result in the loss of confidentiality, integrity, or availability of information, leading to adverse consequences like financial losses or harm to the to the handling of information security incidents
Data Breach / Privacy Breach	Breach of security leading to accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed
Incident Handling	Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents
Incident Response	Actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it
Information Security Event	Occurrence indicating a possible breach of information security or failure of controls
SIRT	Security Incident Response Team
DPO	Data Privacy Office, engaged for assessing impact due to breach on an individual and impact to the organization.
HRD	Human Resource Department, primarily be engaged to take disciplinary action.
Incident	any event that results in the (a) loss of confidentiality, integrity, or availability of information, leading to adverse consequences like financial losses or harm to the brand image and (b) breach of individual personal data.
Risk	any perceived damage of financial loss, disruption or damage to the reputation of Netradyne arising due to (a) failure of its information technology systems and (b) improper processes of handling of personal

	information, which if not addressed within an appropriate time shall lead to an Incident

8 References

8.1 Templates

Below Incident template must be filled in post investigation:

8.2 Policies

ISMS policies & Procedures

8.3 Process/Procedures

Vulnerability & Patch Management Procedure

8.4 Standards

NA

8.5 Miscellaneous

NA

9 Appendix A: Document RACI Matrix

Role/Activity	Document Owner/Functional Area Lead	Document Contributor	ND Leadership	Functional Area Team	InfoSec	All ND Member(s)
Ensure document is kept current	**A**	**R**	**I, C**	**R, C**	**C**	**I**
Ensure stakeholders are kept informed	**A**	**R**	**-**	**R**	**C**	**-**
Ensure document contains all relevant information	**A**	**R**	**I, C**	**R, C**	**C**	**I**
Ensure document adheres to document governance policy	**A, R**	**R**	**I**	**R, C**	**R, C**	**I**
Provide SME advice	**I, R**	**A, R**	**I**	**R, C**	**I, C**	**I**
Gathering and adding document contents	**I**	**A, R**	**I, C**	**R, C**	**C**	**I**
Document Approval	**A**	**R**	**I, R**	**I**	**I, R**	**I**

Key

R	**Responsible**
A	**Accountable**
C	**Consulted**
I	**Informed**