

Internal and Confidential

Netradyne Vulnerability Response Playbook

V3.0

Table of Contents

[Netradyne Vulnerability Response Playbook 0](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISMS_ISO27001_2013/ISMS_Security%20Operations%20Center(SOC)/Netradyne%20Vulnerability%20Response%20Playbook.docx#_Toc158641203)

[Document Control 2](#_Toc158641204)

[1 Purpose 3](#_Toc158641205)

[2 Scope 3](#_Toc158641206)

[3 Roles and Responsibilities 3](#_Toc158641207)

[4 Procedure 3](#_Toc158641208)

[4.1 Preparation 4](#_Toc158641209)

[4.2 Vulnerability Response Process 4](#_Toc158641210)

[4.2.1 Identification 4](#_Toc158641211)

[4.2.2 Evaluation 5](#_Toc158641212)

[4.2.3 Remediation 6](#_Toc158641213)

[4.3 Incident Response Checklist 7](#_Toc158641214)

[4.4 Incident Response Preparation Checklist 11](#_Toc158641215)

[VULNERABILITY AND INCIDENT CATEGORIES 12](#_Toc158641216)

[5 Conduct 13](#_Toc158641217)

[6 Exception 13](#_Toc158641218)

[7 Terms/Acronyms 14](#_Toc158641219)

[8 References 14](#_Toc158641220)

[8.1 Templates 14](#_Toc158641221)

[8.2 Policies 14](#_Toc158641222)

[8.3 Process/Procedures 14](#_Toc158641223)

[8.4 Standards 14](#_Toc158641224)

[8.5 Miscellaneous 14](#_Toc158641225)

[9 Appendix A: Document RACI Matrix 14](#_Toc158641226)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDSDT2021001 |
| **Document Name** | Netradyne Vulnerability Response Playbook |
| **Document Status** | Released |
| **Document Released Date** | 28-04-2023 |
| **Document Author** | Rajeev Ghosh Rajeev.ghosh@netradyne.com |
| **Document Content Contributors** | Rajeev Ghosh Rajeev.ghosh@netradyne.com |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Rajeev Ghosh |
| **Document Version** | v3.0 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 21-APR-2023 | Initial Version | Rajeev Ghosh |
| v2.0 | 09-FEB-2024 | Refined to include more controls on data privacy/Data Protection | Hemchand |
| V3.0 | 03-FEB-2025 | Added Escalation Matrix ,SAL & Annual Review Performed | Girithar N |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 25-APR-2023 | Saravanan Sankaran | Senior Director - Info Security & IT | Approved |
| 12-FEB-2024 | Saravanan Sankaran | Senior Director - Info Security & IT | Approved |
| 05-FEB-2025 | Saravanan Sankaran | Vice-President– Infosec & IT | Approved |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| All Stakeholders | Netradyne Inc |
|  |  |
|  |  |

# Purpose

This document is a Netradyne Policy/Process/Procedure document for managing vulnerability management.

# Scope

This SOP applies to all NETRADYNE technology assets, facilities, employees, contractors (as provided by law or contract), partners, and visitors, in achieving NETRADYNE missions, programs, projects, and institutional requirements.

Vulnerability Management Process is defined and established and identified vulnerabilities are remediated as per the prescribed timeline. Periodic cadence shall be established by InfoSec team with relevant stakeholders to review, track and close the pending vulnerabilities.

# 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. |

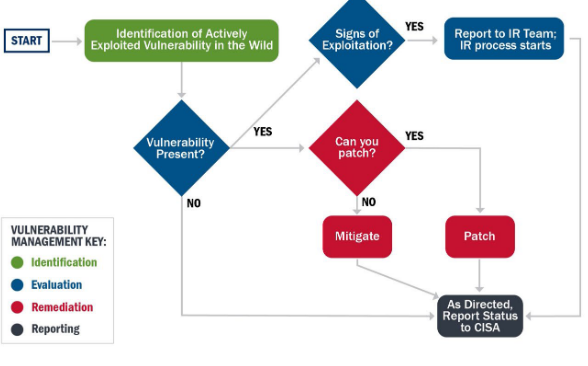
# Procedure

One of the most straightforward and effective means for an organization to prioritize vulnerability response and protect themselves from being compromised is by focusing on vulnerabilities that are already being actively exploited in the wild. This playbook standardizes the high-level process that agencies should follow when responding to these urgent and high-priority vulnerabilities. It is not a replacement for existing vulnerability management programs in place at an agency but instead builds on existing vulnerability management practices. Most vulnerabilities will have common vulnerabilities and exposures (CVE) descriptors. In other cases, agencies might encounter new vulnerabilities that do  
not yet have a CVE (e.g., zero-days) or vulnerabilities resulting from misconfigurations. Appendix D  
provides a companion checklist to track response activities to completion.

## **Preparation**

Effective vulnerability response builds on strong vulnerability management. Ensure that effective  
vulnerability management practices are being followed.29 Such practices include building and  
maintaining robust asset management that includes inventorying:  
• Agency-operated systems and networks,  
• Systems and networks that involve partnerships with other organizations, and  
• Systems and networks operated by others, including cloud, contractor, and  
service provider systems.  
Have a process in place to understand the relevance of vulnerabilities to the environment by tracking  
operating systems and other applications for all systems. Understand all systems might have  
vulnerabilities and the implication of potential vulnerabilities on operations.

## Vulnerability Response Process

Standard vulnerability management programs include phases for identifying, analysing, remediating,  
and reporting vulnerabilities. Figure below describes the vulnerability response process in terms of standard  
vulnerability management program phases.

### Identification

Proactively identify reports of vulnerabilities that are actively exploited in the wild by monitoring threat feeds and information sources, including but not limited to:  
• CISA resources; for example:

CISA/US-CERT National Cyber Awareness System (NCAS) products,  
which include the weekly bulletins containing vulnerability summaries.  
Note: all agencies should subscribe to NCAS products.30

CISA Binding Operational Directive (BOD) 22-01, Managing  
Unacceptable Risk of Known Vulnerabilities, which is continually updated  
with vulnerabilities being exploited in the wild.  
Note: subscribe to NCAS products for all BOD 22-01 vulnerability  
updates, which are announced via Current Activities.

• External threat or vulnerability feeds, such as NIST’s National Vulnerability  
Database,31 that can also show vulnerabilities being exploited in the wild outside  
FCEB agencies

• Internal SOC monitoring and incident response, which can detect vulnerabilities  
being exploited at an agency. Capture additional information about the vulnerability to help with the rest of the response process, including the severity of the vulnerability, susceptible software versions, and IOCs or other investigation steps that can be used to determine if it was exploited.

### Evaluation

First, determine whether the vulnerability exists in the environment and how critical the underlying software or hardware is, using methodologies such as Stakeholder-Specific Vulnerability Categorization (SSVC).32 Existing patch and asset management tools are critical and can be used to automate the detection process for most vulnerabilities. For actively exploited vulnerabilities, use the “rapid response” processes in these tools (e.g., CDM). In rare cases, such as one-off misconfigurations and zero-days, additional manual scans may need to be performed. Binding Operational Directives (BODs) or Emergency Directives (EDs) issued by CISA may also list specific technical steps to evaluate whether a vulnerability exists.

If the vulnerability exists in the environment, address the vulnerability itself—as described in the Remediation section below—and determine whether it has been exploited in the agency's environment. Use existing best practices to find signs of exploitation, including:

• A sweep for known IOCs associated with exploitation of the vulnerability.  
• Investigation of any abnormal activity associated with vulnerable systems or services, including anomalous access attempts and behavior.  
• Completion of any detection processes   
• If needed, collaboration with a third-party incident responder. If the vulnerability was exploited in the environment, immediately begin incident response activities as described in the Incident Response Playbook. At the end of the Evaluation phase, the goal is to understand the status of each system in the environment as:  
• Not Affected. The system is not vulnerable.  
• Susceptible. The system is vulnerable, but no signs of exploitation were found, and  
remediation has begun.  
• Compromised. The system was vulnerable, signs of exploitation were found, and incident  
response and vulnerability remediation has begun.

### **Remediation**

Remediate all actively exploited vulnerabilities that exist on or within the environment  
in a timely manner. In most cases, remediation should consist of patching. In other  
cases, the following mitigations may be appropriate:

• Limiting access;  
• Isolating vulnerable systems, applications, services, profiles, or other assets; or  
• Making permanent configuration changes.

Existing patch management tools and processes can be used to regularly patch all vulnerabilities. Use “rapid response” processes—as described in the Evaluation section above—in those tools for vulnerabilities that are being actively exploited in the wild. In cases where patches do not exist, have not been tested, or cannot be immediately applied promptly, take other courses of action to prevent exploitation, such as:

• Disabling services,  
• Reconfiguring firewalls to block access, or  
• Increasing monitoring to detect exploitation.

Once patches are available and can be safely applied, mitigations can be removed, and patches applied. As systems are remediated, keep track of their status for reporting purposes. Each system should be able to be described as one of these categories:

• Remediated. The patch or configuration change has been applied, and the  
system is no longer vulnerable.  
• Mitigated. Other compensating controls—such as detection or access  
restriction—are in place and the risk of the vulnerability is reduced.  
• Susceptible/Compromised. No action has been taken, and the system is still  
susceptible or compromised.

## Incident Response ChecklistTable Description automatically generated

Graphical user interface, application, table

Description automatically generatedTable

Description automatically generated

A white and black checklist with black text

Description automatically generatedGraphical user interface, application

Description automatically generated

Table

Description automatically generatedTable

Description automatically generated

Incident Response Preparation Checklist

Table

Description automatically generated

Application, table

Description automatically generated

Table

Description automatically generated

VULNERABILITY AND INCIDENT CATEGORIES

* Major Incident – Per the Office of Management and Budget (OMB) Memorandum M-20-04 or  
  subsequent memo, a major incident is either:  
  Any incident that is likely to result in demonstrable harm to the national security interests, foreign  
  relations, or the economy of the United States or to the public confidence, civil liberties, or public  
  health and safety of the American people.41 Agencies should determine the level of impact of the  
  incident by using the existing incident management process established in the National Institute  
  of Standards and Technology (NIST) Special Publication (SP) 900-61 Revision 2, Computer  
  Security Incident Handling Guide.
* A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted,  
  or otherwise compromised, is likely to result in demonstrable harm to the national security  
  interests, foreign relations, or the economy of the United States, or to the public confidence, civil  
  liberties, or public health and safety of the American people. Major incident determination is  
  required for breaches involving PII of 100,000 or more people.42  
  Breach – Per OMB Memorandum M-17-12 or subsequent memo: The loss of control, compromise,  
  unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other  
  than an authorized user accesses or potentially accesses personally identifiable information or (2) an  
  authorized user accesses or potentially accesses personally identifiable information for other than  
  authorized purpose.
* Event – Per NIST SP 900-61 Revision 2: An event is any observable occurrence in a system or network.  
  Vulnerabilities:  
  • Internal discovery of potential compromise leveraging a vulnerability  
  • Known exploitation of vulnerability (NVD tagged entries; wide-spread public reporting; viable  
  proof-of-concept exploit released, et

#### Escalation matrix and SLA:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Email** | **Contact** |
| Gautam Kumar | Staff Security Analyst | gautam.kumar@netradyne.com<mailto:sudhansu.kumar@netradyne.com> | Primary  Contact |
| Saravanan Sankaran | Vice President - IT & InfoSec | [saravanan.sankaran@netradyne.com](mailto:saravanan.sankaran@netradyne.com) | Escalation |
| Vinay Rai | Senior Vice President, Cloud | [vinay.rai@netradyne.com](mailto:vinay.rai@netradyne.com) | Escalation |

**Vulnerability Remediation SLA**

| **Risk Level** | **Remediation Timeline** | **IoT (Driveri Devices) Specific Timeline** |
| --- | --- | --- |
| **Critical** | Within **5 business days** | Within **3 months** |
| **High** | Within **30 business days** | Within **6 months** |
| **Medium** | Within **90 business days** | Within **9 months** |
| **Low** | Within **12 months** | Planned & prioritized within **12–18 months** |

# 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.

# Exception

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

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| HIPAA | Health Insurance Portability and Accountability Act |
| GDPR | General Data Protection Regulation |
| ePHI | Electronic Protected Health Information |
|  |  |
|  |  |
|  |  |
|  |  |

# References

## Templates

<List of (or Links to) associated templates>

## Policies

[Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=mRSIq4)

[Netradyne Information Security Exception Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Exception%20Process.pdf?csf=1&web=1&e=RbfEhO)

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=2jMnrk)

## Process/Procedures

[NETRADYNE DISASTER RECOVERY PROCESS.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20DISASTER%20RECOVERY%20PROCESS.pdf?csf=1&web=1&e=xTyHtp)

[NETRADYNE BUSINESS CONTINUITY PLAN.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20BUSINESS%20CONTINUITY%20PLAN.pdf?csf=1&web=1&e=eCZUy6)

[Netradyne Vulnerability & Patch Management Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Vulnerability%20%26%20Patch%20Management%20Process.pdf?csf=1&web=1&e=N697w0)

[NetradyneSecurityIncidentResponsePlan.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NetradyneSecurityIncidentResponsePlan.pdf?csf=1&web=1&e=Nzo34K)

## Standards

<List of (or Links to) related Netradyne Standards>

## Miscellaneous

<List of (or Links to) any relevant documentation not covered in the list above>

# 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 |