

Internal and Confidential

Technical Vulnerabilities Management

v2.3

Table of Contents

[Document Control 2](#_Toc158804647)

[1 Purpose 3](#_Toc158804648)

[2 Scope 3](#_Toc158804649)

[3 Roles and Responsibilities 3](#_Toc158804650)

[4 Procedure 3](#_Toc158804651)

[4.1 Technical Vulnerabilities Management 3](#_Toc158804652)

[4.1.1 Internal Pen Testing 3](#_Toc158804653)

[4.1.2 Static Code Analysis 4](#_Toc158804654)

[4.1.3 Software Composition Analysis 4](#_Toc158804655)

[4.1.4 External Pen Testing 4](#_Toc158804656)

[4.1.5 Third Party tools for SAST, SCA and DAST 4](#_Toc158804657)

[5 Conduct 4](#_Toc158804658)

[6 Exception 4](#_Toc158804659)

[7 Terms/Acronyms 4](#_Toc158804660)

[8 References 4](#_Toc158804661)

[9 Appendix A: Document RACI Matrix 5](#_Toc158804662)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDTVM2021001 |
| **Document Name** | Netradyne Technical Vulnerability Management |
| **Document Status** | Released |
| **Document Released Date** | 23-MAR-2021 |
| **Document Author** | Gaurav Agarwal |
| **Document Content Contributors** | Gaurav Agarwal, Melwin Prabu |
| **Document Signatory** | Ankit Srivastava |
| **Document Owner** | Ankit Srivastava |
| **Document Version** | v2.3 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 23-MAR-2021 | Original document | Gaurav Agarwal |
| v2.0 | 23-JUN-2022 | Added latest information | Gaurav Agarwal |
| V2.1 | 16-MAR-2023 | Aligned with standard template | Melwin Prabu |
| v2.2 | 01-FEB-2024 | Refined to include more controls on data privacy/Data Protection | Melwin Prabu |
| V2.3 | 27-Jan-2025 | Annual Review | Gaurav Agarwal |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 23-MAR-2021 | Saravanan Sankaran | CISO |  |
| 23-JUN-2022 | Saravanan Sankaran | CISO |  |
| 20-MAR-2023 | Saravanan Sankaran | CISO |  |
| 02-FEB-2024 | Saravanan Sankaran | CISO |  |
| 29-JAN-2025 | Saravanan Sankaran | CISO |  |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
|  |  |
|  |  |
|  |  |

# Purpose

The purpose of the Technical Vulnerabilities Management document is to provide a comprehensive overview of the Netradyne’s vulnerability management processes, including vulnerability scanning, assessment, prioritization, and remediation, to ensure the security and resilience of the IT and cloud infrastructure, with a keen focus on data security/data protection and data privacy aspects (including PII, PHI and other sensitive data. The document outlining the steps and procedures for managing vulnerabilities effectively while upholding the privacy and security provisions of applicable statutory and regulatory requirements.

# Scope

The Technical Vulnerabilities Management document outlines the scope of vulnerability management activities, including the systems, networks, and applications covered, as well as the roles and responsibilities of individuals involved in the process. It defines the boundaries and extent of vulnerability management efforts within Netradyne.

# 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

Technical Vulnerabilities Management

Following controls are implemented to manage technical vulnerabilities.

### Internal Pen Testing

* OWASP Top Ten standard is used for internal pen testing.
* OWASP Zed Attack Proxy (ZAP) is used for internal pen testing.
* [Latest ZAP Scanning report](https://netorg726775.sharepoint.com/:u:/r/sites/ISMSForum/Shared%20Documents/ISMS%20Documents/Engineering/IDMS%20ZAP%20Active%20Scan%20Reviewed%20-%206th%20Oct%202020.html?csf=1&web=1&e=iBEJ5k)
* Next planned Internal Pen Test - <https://netradyne.atlassian.net/browse/IDMS-8675>
* Issue fixed - <https://netradyne.atlassian.net/browse/IDMS-6760>

### Static Code Analysis

* SonarQube tool is used to catch common bugs and vulnerabilities.
* SonarLint is integrated in developer IDE to catch issues at time of development.
* The following is the latest Scan report.
* <http://staging-sonarqube.netradyne.info:9000/dashboard?id=com.netradyne%3Acloud>

### Software Composition Analysis

* OWASP Dependency-Check tool is used to detect publicly disclosed vulnerabilities contained within a project’s dependencies.
* Dependencies are upgraded to a version which contains a fix for disclosed vulnerabilities.
* Zero-day vulnerabilities are identified and fixed with high priority.

### External Pen Testing

* External Pen-Testing is conducted Bi-annually.

### Third Party tools for SAST, SCA and DAST

* Evaluating third party tools to better manage technical vulnerabilities.

# 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** |
| OWASP | Open Web Application Security Project |
| HIPAA | Health Insurance Portability and Accountability |
| GDPR | General Data Protection Regulation |
| PHI | Protected Health Information |

# References

<https://owasp.org/www-project-top-ten/>

# 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 |