

Internal and Confidential

Netradyne Cloud Software Development Life Cycle Process

v1.2

Table of Contents

[Netradyne Cloud Software Development Life Cycle Process 0](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001-Jul2024/ARCHIVE/CLOUD/Cloud2024/Cloud_Docs-Reviewed/Netradyne%20Software%20Development%20Life%20Cycle%20Process.docx#_Toc140175807)

[Document Control 2](#_Toc140175808)

[1 Purpose 3](#_Toc140175809)

[2 Scope 3](#_Toc140175810)

[3 Roles and Responsibilities 3](#_Toc140175811)

[4 Procedure 3](#_Toc140175812)

[4.1 Requirements Gathering: 3](#_Toc140175813)

[4.2 Planning, Design and Architecture: 3](#_Toc140175814)

[4.3 Continuous Integration and Development: 4](#_Toc140175815)

[4.3.1 Development Process 4](#_Toc140175816)

[4.4 Continuous Testing: 4](#_Toc140175817)

[4.4.1 Testing & Automation Process: 4](#_Toc140175818)

[4.5 Continuous Deployment: 4](#_Toc140175819)

[4.6 Continuous Monitoring and Management: 4](#_Toc140175820)

[4.7 Incident Response and Recovery: 5](#_Toc140175821)

[4.8 Security Automation and Orchestration: 5](#_Toc140175822)

[4.9 Collaboration and Knowledge Sharing: 5](#_Toc140175823)

[4.10 Maintenance and Updates: 5](#_Toc140175824)

[4.11 Continuous Improvement: 5](#_Toc140175825)

[5 Conduct 5](#_Toc140175826)

[6 Exception 5](#_Toc140175827)

[7 Terms/Acronyms 5](#_Toc140175828)

[8 References 6](#_Toc140175829)

[8.1 Templates 6](#_Toc140175830)

[8.2 Policies 6](#_Toc140175831)

[8.3 Process/Procedures 6](#_Toc140175832)

[8.4 Standards 6](#_Toc140175833)

[8.5 Miscellaneous 6](#_Toc140175834)

[9 Appendix A: Document RACI Matrix 6](#_Toc140175835)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDCLOUDSDLC2023001 |
| **Document Name** | Netradyne Software Development Life Cycle Process |
| **Document Status** | Released |
| **Document Released Date** | 14-APR-2023 |
| **Document Author** | Prasanna Babu |
| **Document Content Contributors** | Prasanna Babu, Saravanan Sankaran, Sudhansu Kumar, Gaurav Agarwal |
| **Document Signatory** | Ankit Srivastava |
| **Document Owner** | Ankit Srivastava |
| **Document Version** | v1.2 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 10-APR-2023 | Initial Release of SDLC Process Document | Prasanna Babu |
| v1.1 | 01-FEB-2024 | Refined to include more controls on data privacy/Data Protection | Melwin Prabu |
| V1.2 | 27-JAN-2025 | Review with no changes | Prasanna Babu |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 14-APR-2023 | Ankit Srivastava | Vice President |  |
| 02-FEB-2024 | Ankit Srivastava | Vice President |  |
| 29-JAN-2025 | Ankit Srivastava | Vice President |  |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| Netradyne Internal |  |
|  |  |
|  |  |

# Purpose

The SSDLC process is an extension of the DevOps methodology that integrates security practices throughout the software development lifecycle. It emphasizes the collaboration between development, operations, and security teams to ensure the delivery of secure and reliable software.

# Scope

Scope of this document includes Netradyne Product Development, Netradyne managed AWS infrastructure, GitHub repositories which include Netradyne Cloud, Netradyne Infra and other functions where coding, scripting are in place.

# 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

The Software Development Life Cycle (SDLC) process for Netradyne cloud environment involves several stages to ensure the efficient development, deployment, and maintenance of cloud-based applications.

Here's a high-level overview of the SDLC process at Netradyne:

Requirements Gathering:

This initial phase involves understanding the business requirements and objectives for the cloud-based application. It includes identifying key stakeholders, gathering functional and non-functional requirements, and defining the scope of the project.

Planning, Design and Architecture:

In this phase, the system architecture and design of the cloud environment are planned. Security considerations should be incorporated right from the planning phase. This includes identifying security requirements, threat modelling, and risk assessments. Security controls and measures are designed to address potential vulnerabilities and ensure compliance with relevant regulations and standards. It includes designing the application components, infrastructure, and data storage architecture to meet the scalability, availability, and security requirements of underlying sensitive data (including PII/PHI). Considerations may include selecting appropriate cloud services, designing APIs, and defining data flows.

Continuous Integration and Development:

Development teams follow coding best practices and security guidelines during the coding process. Code reviews, static code analysis, and vulnerability scanning tools are used to identify security flaws early in the development cycle. Security tests are integrated into the continuous integration (CI) process to ensure code quality and security standards.

The development phase involves coding the application logic and implementing the designed components. Development practices such as continuous integration and version control are often followed. Developers write code, perform unit testing, and ensure adherence to coding standards.

### Development Process

#### Developers follow the below procedure:

1. Get the requirements in the form or a JIRA ticket.
2. Analyse and create a design document for the proposed solution and design.
3. Estimate the work.
4. Develop the solution.
5. Write Unit tests.
6. Test the solution in development and lower hosted environments.

Continuous Testing:

This phase focuses on validating the application's functionality, performance, security, and scalability. Security testing is an integral part of the testing phase. It includes dynamic application security testing (DAST), penetration testing, and security scanning to identify vulnerabilities and weaknesses. It includes various testing types such as unit testing, integration testing, system testing, performance testing, and security testing. Automation tools and frameworks may be utilized to streamline the testing process and ensure comprehensive test coverage.

### Testing & Automation Process:

#### QA follows the below procedure:

1. Understand the requirement document.
2. Write Functional test cases.
3. Write Integration test cases.
4. On receiving approved changed, test in integration environment.
5. Notify stakeholders for any impact.
6. Perform regression tests.
   * Promote the release to production.
   * Monitor the changes postproduction.

Continuous Deployment:

Once the application has passed the testing phase, it is deployed to the cloud environment. Deployment practices may include infrastructure provisioning, containerization, and utilizing cloud-native deployment services. In the deployment phase, security controls are implemented to ensure secure deployment and configuration of the application. Continuous Deployment (CD) techniques enable automated deployments to ensure a smooth release process. Infrastructure as Code (IaC) and configuration management tools enable consistent and secure provisioning of resources. Security-focused deployment pipelines automate security checks, such as container image scanning, access controls, and security configurations.

Continuous Monitoring and Management:

Continuous monitoring is crucial for identifying and mitigating security threats and anomalies in real-time to ensure its performance, availability, and security. Security monitoring tools and services are employed to monitor application logs, network traffic, system performance, and security events. Intrusion detection and prevention systems, log analysis, and threat intelligence are used to detect and respond to security incidents promptly. Logging and analytics are employed to gain insights into application behaviour and performance.

Incident Response and Recovery:

A well-defined incident response plan is essential for addressing security incidents effectively. Security teams collaborate with development and operations teams to investigate and mitigate security breaches or vulnerabilities. Lessons learned from incidents are used to improve security controls and processes.

Security Automation and Orchestration:

Automation and orchestration play a vital role in the SDLC process. Security tasks, such as vulnerability scanning, patch management, and access controls, are automated to reduce human error and enhance efficiency. Security policies and configurations are enforced through code and configuration management tools.

Collaboration and Knowledge Sharing:

SDLC promotes collaboration and knowledge sharing among development, operations, and security teams. Regular communication, training, and workshops ensure that all teams have a shared understanding of security practices and are aligned with security objectives.

Maintenance and Updates:

Regular maintenance and updates are necessary to address bugs, security vulnerabilities, and incorporate new features or improvements. This phase includes ongoing support, bug fixes, and managing changes in the cloud environment. It may involve following DevOps practices to streamline the release process and ensure smooth updates.

Continuous Improvement:

The SDLC process in a cloud environment should be iterative, with a focus on continuous improvement. Feedback from users, monitoring data, and . This feedback loop helps prioritize future development efforts and ensures the application aligns with changing business needs.

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits All tests conducted adhere to the controls outlined in both HIPAA and GDPR regulations. Additionally, our workforce receives regular Security Awareness, compliance, and role-based training opportunities. New hires undergo security awareness training within 90 days of being hired. Furthermore, employees are required to complete mandatory training, including the protection of Personally Identifiable Information (PII), Protected Health Information (PHI), and other sensitive business data, which is monitored continuously. 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** |
| SDLC | Software Development Life Cycle |
| INFRA | Infrastructure |
|  |  |

# References

## Templates

[Design document template](https://netradyne.atlassian.net/wiki/spaces/IDMS/pages/385287638)

## 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

[Cryptography Standard Policy](https://netorg726775.sharepoint.com/:w:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISMS_ISO27001_2022/ISMS_Engineering/Cryptography%20Standards%20Policy.docx?d=we55ec70261d64f8794562ded04349c40&csf=1&web=1&e=1y3zF7)

[Test Data Selection](https://netorg726775.sharepoint.com/:w:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISMS_ISO27001_2022/ISMS_Engineering/Test%20data%20selection.docx?d=w621c6bcc77f649698663e395616c912d&csf=1&web=1&e=LkmmaE)

[Technical Vulnerabilities Management](https://netorg726775.sharepoint.com/:w:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISMS_ISO27001_2022/ISMS_Engineering/Managing%20Technical%20Vulnerabilities.docx?d=w48bfba583d254559859264c3fb4335af&csf=1&web=1&e=EXReBS)

## Miscellaneous

[Cloud Architecture Diagram](https://netradyne.atlassian.net/wiki/spaces/IDMS/pages/299958543)

# 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 |