

Netradyne Cryptographic Control Process

v2.2

Internal and Confidential

Table of Contents

[Document Control 2](#_Toc140173473)

[1 Purpose 3](#_Toc140173474)

[2 Scope 3](#_Toc140173475)

[3 Roles and Responsibilities 3](#_Toc140173476)

[4 Procedure 3](#_Toc140173477)

[4.1 Data-in-Transit security 3](#_Toc140173478)

[4.2 Data at Rest security 4](#_Toc140173479)

[4.3 Key Management 4](#_Toc140173480)

[4.4 Authentication 4](#_Toc140173481)

[ Users of application are strongly authenticated using password and MFA. 4](#_Toc140173482)

[ Devices are strongly authenticated through public key authentication. 4](#_Toc140173483)

[5 Conduct 4](#_Toc140173484)

[6 Exception 4](#_Toc140173485)

[7 Terms/Acronyms 4](#_Toc140173486)

[8 References 5](#_Toc140173487)

[9 Appendix A: Document RACI Matrix 5](#_Toc140173488)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDCLOUDCC2021001 |
| **Document Name** | Netradyne Cryptographic Control Process |
| **Document Status** | Released |
| **Document Released Date** | 23-MAR-2021 |
| **Document Author** | Gaurav Agarwal |
| **Document Content Contributors** | Gaurav Agarwal, Melwin Prabu |
| **Document Signatory** | Vinay Rai |
| **Document Owner** | Vinay Rai |
| **Document Version** | v2.2 |
| **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 newly implemented controls details. | 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 |
| V2.2 | 27-JAN-2025 | Annual review with no change | Gaurav Agarwal |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 23-MAR-2021 | Vinay Rai | Senior Vice President | Approved |
| 28-JUN-2022 | Vinay Rai | Senior Vice President | Approved |
| 20-MAR-2023 | Vinay Rai | Senior Vice President | Approved |
| 02-FEB-2024 | Vinay Rai | Senior Vice President | Approved |
| 31-JAN-2025 | Vinay Rai | Senior Vice President | Approved |

**Distribution of Final Document**

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

# Purpose

This **Netradyne** control document underscores the importance of cryptographic controls. These controls uphold the integrity, confidentiality, and authenticity of sensitive data, in compliance with **HIPAA's** patient data protection regulations and **GDPR's** stringent guidelines for the privacy of personal data. Using encryption, hashing, and digital signatures, these controls provide robust security against unauthorized access and data tampering.

# Scope

Cryptographic controls encompass the implementation and management of encryption algorithms, key management, and secure protocols to protect data at rest, in transit, and in use across systems and networks. Their scope extends to securing sensitive information and ensuring the integrity and confidentiality of communications and transactions of Netradyne’s data.

# 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

Following are the cryptographic controls used in IDMS product.

Data-in-Transit security

Devices connect to remote servers and AWS IOT service using TLS connection. HTTPS is enforced on external facing portals and APIs. We use AWS ELB for TLS negotiation which enforce TLS 1.2 and above TLS versions.

These measures align with **HIPAA and GDPR’s** stipulation for robust encryption standards to be applied to data in transit, safeguarding against unauthorized access or interception during data transfer.

Data at Rest security

* All the data stored on the device is encrypted using AES 256 algorithm.
* Data stored in AWS S3 cloud storage is encrypted using AES-256 SSE encryption.
* Sensitive and PII data stored in Database is encrypted using AES-256 algorithm.
* Passwords are salted and hashed using PBKDF2WithHmacSHA512 algorithm.
* Other Third-party API keys, tokens and database password are encrypted and stored in AWS SSM. Access to SSM is controlled using AWS IAM role and permissions.
* These measures, collectively, help ensure that data at rest is effectively secured, adhering to the **HIPAA**'s data protection and confidentiality requirements.

Key Management

* DB data fields are encrypted using Tenant specific encryption key (TEK) which itself is secured by environment specific Master Key.
* We utilize AWS KMS system for managing Master Keys. A separate master key is used for production environment. AWS KMS stores master keys in HSM and provides APIs for encryption and decryption without exposing actual key.
* Access to Master Keys for encryption and decryption is protected by AWS IAM roles and permissions.
* Automatic Master Key rotation is enabled in AWS KMS which rotates keys every year.
* Client Credentials which are used to generate access tokens to access API platform are stored in database in encrypted format.

Authentication

* Users of application are strongly authenticated using password and MFA.
* Devices are strongly authenticated through public key authentication.

# 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** | |
| AWS | Amazon Web Service | |
| TEK | Tenant specific encryption key | |
| IAM | Identity and Access Management | |
| TLS | Transport Layer Security | |
| KMS | Key Management Service | |
| IOT | Internet of Things | |
| HIPAA | Health Insurance Portability and Accountability | |
| GDPR | General Data Protection Regulation |

# References

<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/kms-security.html>

# 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 |