netradyne

# Netradyne Information Security Policy & Procedure

v1.4

Internal and Confidential

## Document Control

| | |
|---|---|
| **Document ID** | NDISMS2020003 |
| **Document Name** | Netradyne Information Security Policy & Procedure |
| **Document Status** | Released |
| **Document Initial Release Date** | 30-NOV-2020 |
| **Document Author** | InfoSec |
| **Document Content Contributors** | Sudhansu Kumar, Kavitha S., Saravanan Sankaran, Vivian P. |
| **Document Signatory** | Saravanan Sankaran<saravanan.sankaran@Netradyne.com > |
| **Document Owner** | Saravanan Sankaran<saravanan.sankaran@Netradyne.com > |
| **Document Version** | v1.4 |
| **Information Classification** | Internal |

## Document Edit History

| Version | Date | Additions/Modifications | Prepared/Revised By |
|---|---|---|---|
| v1.0 | 27-NOV-2020 | Original issue | InfoSec |
| v1.1 | 28-JUL-2021 | 1.4.5 Security Committee (SC)<br>1.4.6.1 SIRT Members<br>Table updated | InfoSec |
| v1.2 | 05-AUG-2021 | Included DRP 3.8.8 section | Kavitha S. |
| v1.3 | 12-MAY-2023 | Aligned with standard template | Sudhansu Kumar |
| v1.4 | 09-JUN-2023 | Changes in PVM Deployment | Sudhansu Kumar |

## Document Review/Approval

| Date | Signatory Name | Organization/Signatory Title | Comments |
|---|---|---|---|
| 30-NOV-2020 | Vinay Rai | Vice President | |
| 29-JUL-2021 | Saravanan Sankaran | Senior Director InfoSec & IT | |
| 08-AUG-2022 | Saravanan Sankaran | Senior Director InfoSec & IT | |
| 13-MAY-2023 | Saravanan Sankaran | Senior Director InfoSec & IT | |
| 12-JUN-2023 | Saravanan Sankaran | Senior Director InfoSec & IT | |

## Distribution of Final Document

| Name | Organization/Title |
|---|---|
| All Employees | Netradyne |
| | |
| | |

## Table of Contents

# 1 Purpose

This document is a Netradyne Information Security Policies and Procedure document. This document establishes policy and procedures used by the NETRADYNE Information Security, Information Technology Operations and DevOps group and applicable to all Netradyne System. Due to the nature of our business, NETRADYNE enforces information security and computer usage policies covering all sensitive consumer, merchant/client, and NETRADYNE data. All employees are responsible to consider the sensitivity of information in every aspect of their work.

The objective of the NETRADYNE Information Technology Operations and Security Program is to achieve an effective and cost beneficial security posture for NETRADYNE Information Technology systems. Attainment of this objective requires a balanced combination of problem recognition, resources, and policy to implement an effective program.

# 2 Scope

This document applies to all NETRADYNE activities, departments, and divisions processing and/or utilizing Information Technology systems resources. The provisions of this document are intended to apply to all Information Security & Technology systems resources regardless of application, functional organization, or source of funding. Information Technology systems resources include all computer equipment, remote terminals, peripherals, data, software, associated documentation, contractual services, employees, supplies, and facilities.

# 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.<br>• Is the point of contact for the document.<br>• 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 Introduction

This document establishes policy and procedures used by the NETRADYNE Information Technology Operations and Security group. Due to the nature of our business, NETRADYNE enforces information security and computer usage policies covering all sensitive consumer, merchant/client, and NETRADYNE data. All employees are responsible to consider the sensitivity of information in every aspect of their work.

All elements of the NETRADYNE Information Technology Operations and Security Program are structured to minimize or prevent damage, which might result from accidental or intentional events, or actions that might breach the confidentiality of NETRADYNE records, result in fraud or abuse, or delay the accomplishment of NETRADYNE operations.

The objective of the NETRADYNE Information Technology Operations and Security Program is to achieve an effective and cost beneficial security posture for NETRADYNE Information Technology systems. Attainment of this objective requires a balanced combination of problem recognition, resources, and policy to implement an effective program.

To be responsive to the needs of NETRADYNE's growing organization, this policy is subject to change. Significant changes to the policy will be communicated as broadly as possible and will, at a minimum, include the use of email.

The information in this document:

- Describes the NETRADYNE Information Technology Operations and Security program
- Applies to all Information Technology systems and is from a total-system perspective
- Is considered as the minimum standard for all Information Technology Operations and Security systems and supporting activities
- Establishes Information Technology Operations and Security policies, assigns responsibilities and prescribes procedures for the development and maintenance of NETRADYNE wide Information Technology Operations and Security
- Complies with the intent of prevailing security and privacy legislation regarding safeguards and consumer protection

## 4.1 Scope

This document applies to all NETRADYNE activities, departments, and divisions processing and/or utilizing Information Technology systems resources. The provisions of this document are intended to apply to all Information Technology systems resources regardless of application, functional organization, or source of funding. Information Technology systems resources include all computer equipment, remote terminals, peripherals, data, software, associated documentation, contractual services, employees, supplies, and facilities.

The scope of this document is to:

- Provide uniform policy and centralized guidance for dealing with all known and recognized aspects of Information Technology Operations and Security affecting NETRADYNE and its operations
- Provide realistic guidance to ensure that all sensitive information handled by NETRADYNE automated systems is protected commensurate with the risk of inadvertent or deliberate disclosure, fraud, misappropriation, misuse, sabotage, or espionage

NOTE: Sensitive information includes but is not limited to information that is safeguarded to:

- Prevent damage to NETRADYNE business operations due to unauthorized disclosures
- Assure the individual privacy of NETRADYNE customers and employees
- Protect funds, supplies and materials from theft, fraud, misappropriation, or misuse
- Protect property and rights of contractors, vendors, and other organizations
- Provides for the documented and justified selection of physical, technical, and administrative security controls which are cost-effective, prudent, and operationally efficient
- Provides for the monitoring of the implementation of selected security controls and procedures
- Provides for the auditing and reviewing functions necessary to ensure compliance with stated security requirements
- Protect contract negotiations and other privileged considerations in dealings with contractors, vendors, correspondents, and other organizations
- Protect employees from unnecessary temptation to misuse NETRADYNE information or Information Technology systems resources while fulfilling their normal duties
- Protect employees from suspicion in the event of misuse or abuse by others
- Ensure the integrity and accuracy of all NETRADYNE information

- Protect NETRADYNE information processing operations from incidents of hardware, software or network failure resulting from human carelessness, intentional abuse, or accidental misuse of the system
- Ensure the ability of all NETRADYNE information processing operations to survive business interruptions and to function adequately after recovery
- Protect management from charges of imprudence in the event of compromise of any security system or disaster.

## 4.2 Objective

The objective of the NETRADYNE Information Technology Operations and Security Program is to create a NETRADYNE environment where, based upon an active and continuous risk analysis program, the following elements of Information Technology Operations and Security can be successfully integrated and implemented:

- Access to Information Technology systems resources based upon a defined access requirement
- A proven ability to audit all transactions and processes impacting NETRADYNE data bases and operational outputs
- Security awareness programs designed to educate employees in the NETRADYNE security requirements
- Traditional physical security controls and accountability with manual as well as automated processes
- Systems development review procedures and testing to ensure security in all
- Information Technology systems designs and procurements
- A program of management reviews and audits to ensure compliance with security controls
- A realistic and exercised contingency plan

## 4.3 Contacts

The contact for this policy is the CISO / MR.

## 4.4 Responsibilities

The NETRADYNE Information Technology Operations and Security Program has been established in recognition of the NETRADYNE dependence upon computer-based services and the special problems involved in securing them.

Because of this dependence and the embedding of Information Technology systems into virtually every NETRADYNE function and process, Information Technology Operations and Security cannot be viewed as a minor technical matter falling under the exclusive purview of the information processing community. To the contrary, the vital function of information systems and the potential impact of security shortcomings make Information Technology Operations and Security a serious concern for all NETRADYNE employees.

This section prescribes responsibilities for all levels of NETRADYNE management, support staffs, and committees in order to assure successful implementation of the NETRADYNE Information Technology Operations and Security Program. It also delineates the activities required of other organizational entities in support of the NETRADYNE Information Technology Operations and Security Program.

### 4.4.1 Production IT Manager

The Production IT Manager is responsible for the NETRADYNE Information Technology Operations and Security Program and for ensuring compliance with the security policy. In this capacity the manager will:

- Provide support for the development, implementation, and maintenance of policies, plans and procedures to manage the overall NETRADYNE Information Technology Operations and Security Program.

- Ensure identification of Information Technology Operations and Security related problems, requirements and needs for resolution to NETRADYNE executive management.
- Represent the interest of the NETRADYNE Information Technology Operations and Security Program to the Strategic Planning Committee.
- In cooperation with the Chief Security Officer, establish, document, and distribute security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- In cooperation with the Chief Security Officer, establish, document, and distribute security incident response and escalation procedures.
- Administer user account and authentication management.
- Monitoring and controlling all access to data.

### 4.4.2 Lead, Devops and IT

The Lead, Devops and Information Technology is responsible for overseeing the NETRADYNE Information Technology Security needs and requirements. In this capacity this role will:

- Act as the company Systems Security and Privacy Officer at NETRADYNE.
- Maintain current knowledge in Information Technology Operations and Security technology and the determination of its applicability to NETRADYNE.
- Ensure the integrity of the NETRADYNE Information Technology Operations and Security Program.
- Ensure accountability to all data protection regulations and requirements imposed by Privacy and Data Protection authorities, regulators, and NETRADYNE customers.
- Develop security policies, standards, guidelines, and procedures relative to the physical, personnel, data, communications, hardware, software, and operational aspects of Information Technology systems.
- Establish, document, and distribute security incident response and escalation procedures.
- Interface with all NETRADYNE managers, directly or through their security representatives, on matters of security that relate to or are unique to their areas.
- Review and approve the categorization of each new information processing area
- Verify that implemented administrative, physical, and technical safeguards are operationally adequate.
- Distributing security policies to all persons conducting work for NETRADYNE.
- Administer user account and authentication management.
- Monitoring and controlling all access to data.

### 4.4.3 All Netradyne management

All NETRADYNE managers are responsible for:

- Developing an understanding of the sensitivity/criticality of NETRADYNE information and information processing as well as formulating basic statements of security objectives, requirements, and specifications for their applications. This may be accomplished with support from the Information Technology Operations and Security group.
- Assisting the Information Technology Operations and Security group in the detection, documentation, and investigation of suspected or actual security incidents and/or violations
- Supporting, with technical assistance, any risk analysis project where specific functional expertise or advice is needed
- Evaluating employees on the nature of support rendered to the NETRADYNE Information Technology Operations and Security program through performance evaluations, comments and/or ratings
- Promulgating, as necessary, specific instruction for implementing the provisions of this document
- Enforcing Information Technology Operations and Security policies, standards, guidelines, and procedures

### 4.4.4 NETRADYNE employees

Employees are responsible for adhering to NETRADYNE Information Technology Operations and Security policies, standards, guidelines, and procedures. They will also assist in the identification of security vulnerabilities and violations that have, or would, decrease the NETRADYNE security posture.

### 4.4.5 Security Committee (SC)

The Security Committee is responsible for:

- Approving policy, standards, procedures, and guidelines on all matters relating to the security and privacy of the automated processing of customer, employee and NETRADYNE information
- Overseeing the formal NETRADYNE Information Technology Operations and Security program. This includes establishing, funding and staffing projects as necessary to identify potential threats to Information Technology systems, activities, facilities, and other resources, and recommending the implementation of reasonable protective measures
- Establishing appropriate working subcommittees to address security program issues which require continuing commitment of resources

| Name | Title | Location | Email |
|---|---|---|---|
| Sudhansu Kumar | Senior Staff-Risk & Compliance | Bangalore | Sudhansu.kumar@Netradyne.com |
| Vinay Rai | Senior Vice President, Engineering | Bangalore | vinay.rai@Netradyne.com |
| Saravanan Sankaran | Senior Director, InfoSec & IT | Bangalore | Saravanan.sankaran@Netradyne.com |
| Roshan Mathews | Senior Director, Engineering | Bangalore | roshan.mathews@Netradyne.com |

### 4.4.6 Security Incident Response Team (SIRT)

To best respond to and correct security issues that arise in the IT infrastructure, NETRADYNE formed a Security Incident Response Team (SIRT). While the NETRADYNE IT Operations and Security team hold a good deal of the responsibility to ensure a secure IT environment, a coordinated effort across functional groups is required to correct many security issues.

The primary goal of this team will be to investigate and resolve potential or confirmed security incidents through coordinated triage and the creation of a plan of action. In most cases, input from all team members will be of high value to quicken resolution. The SIRT team will be called together as soon as a security incident is identified through email or via conference call, depending on the severity.

The Security Incident Response Team (SIRT) is responsible for the investigation and resolution of potential or confirmed security incidents.

- Reactive – respond to incidents in a coordinated fashion by working with other NETRADYNE groups to develop the action plan and serving as the primary communication channel.
- Proactive – coordinate implementation of preventative measures. This includes communicating about threats, vulnerabilities, and best practices, along with directly implementing preventative measures, or in many cases, acting in a supporting role.
- Advisory – serves as the conduit of information and advisory for the company during an incident.

The SIRT has the following specific responsibilities:

- Rapid response and recovery to active security incidents to develop the response plan and assuring response and/or recovery efforts are coordinated across the NETRADYNE enterprise
- Conduct investigation of an issue, determination of a vulnerability, and/or the extent of an attack.
- Preserve evidence for possible legal follow-up
- Provide early alerts to new vulnerabilities and related attacks

#### 4.4.6.1 SIRT Members

| Name | Title | Location | Email |
|---|---|---|---|
| Rajeev Ghosh | Principal Enterprise Security Architect, InfoSec | Bangalore | Rajeev.ghosh@Netradyne.com |
| Vinay Rai | Vice President, Engineering | Bangalore | vinay.rai@Netradyne.com |
| Saravanan Sankaran | Infosec officer | Bangalore | Saravanan.sankaran@Netradyne.com |
| Roshan Mathews | Director, Engineering | Bangalore | roshan.mathews@Netradyne.com |

## 4.5 Review and Revision

At a minimum, this policy will be reviewed annually and revised as needed.

## 4.6 Technical Controls

### 4.6.1 Asset Management Policy

Netradyne’s Asset Management Policy outlines the principles, responsibilities, and procedures for effectively managing the organization's assets. Proper asset management is crucial to ensure the efficient use, safeguarding, and optimization of assets, including but not limited to financial assets, physical assets, and intellectual property. This policy applies to all employees, contractors, and stakeholders who have access to, use, or manage the organization's assets.

#### 4.6.1.1 The purpose of this policy is to:

- Define the Netradyne's approach to asset management.
- Ensure the accountability and responsibility for assets.
- Promote the efficient use and preservation of assets.
- Comply with legal and regulatory requirements.
- Safeguard sensitive and confidential information.
- Promote sustainability through responsible asset disposal and recycling

#### 4.6.1.2 Definitions

##### 4.6.1.2.1 Assets:

All resources, tangible or intangible, owned or controlled by the organization, with potential value or usefulness. All hardware, software, data, and related components that have value and contribute to the organization's information technology environment.

##### 4.6.1.2.2 Asset Manager/Custodian:

The individual or team responsible for overseeing the management of assets within Netradyne.

##### 4.6.1.2.3 Asset Lifecycle:

The stages assets go through, including acquisition, deployment, utilization, maintenance, and disposal.

### 4.6.1.3 Roles and Responsibilities

#### 4.6.1.3.1 Senior Management:

Senior management is responsible for setting the strategic direction for asset management, ensuring compliance with this policy, and allocating necessary resources.

#### 4.6.1.3.2 Asset Manager/Custodian:

The Asset Manager is responsible for:

- Identifying and classifying assets.
- Establishing and maintaining accurate records of assets.
- Assessing and mitigating risks associated with assets.
- Monitoring asset utilization and performance.
- Coordinating asset disposal and retirement.
- Ensuring compliance with relevant laws and regulations.
- Developing and implementing asset management procedures.
- Managing software licenses and ensuring compliance.
- Coordinating asset disposal and recycling.

#### 4.6.1.3.3 Employees:

All employees are responsible for:

- Safeguarding assets from damage, theft, or misuse.
- Reporting any asset-related issues or incidents promptly.
- Using assets responsibly and efficiently to fulfil their job responsibilities.

### 4.6.1.4 Asset Classification

Assets shall be classified into the following categories:

#### 4.6.1.4.1 Financial Assets:

Including cash, securities, investments, and accounts receivable.

#### 4.6.1.4.2 Physical Assets:

Including equipment, vehicles, infrastructure, and real estate.

#### 4.6.1.4.3 Information and Intellectual Property:

Including data, software, patents, trademarks, and copyrights.

- Hardware: Including computers, servers, networking equipment, and peripherals.
- Software: Including operating systems, applications, and licenses.

### 4.6.1.5 Asset Acquisition and Disposal

- All acquisitions of assets must be authorized by the relevant department and documented appropriately.
- Asset disposals must follow approved procedures, including assessment, valuation, and compliance with environmental and legal requirements.

### 4.6.1.6 Asset Records and Documentation

- Accurate records of all assets, including their location, value, and condition, must be maintained in asset inventory/register.
- Documentation related to asset acquisition, utilization, maintenance, and disposal shall be retained according to legal and regulatory requirements.

### 4.6.1.7 Asset Maintenance and Depreciation

- Regular maintenance schedules shall be established and followed to ensure the operational efficiency and longevity of physical assets.
- Depreciation methods will be applied to financial and physical assets, as required by accounting standards and regulations.

#### 4.6.1.8 Software License Compliance

- The Asset Manager is responsible for ensuring that software licenses are tracked, monitored, and kept in compliance with vendor agreements.
- Unlicensed software is strictly prohibited, and all employees must report any unlicensed software immediately.

#### 4.6.1.9 Compliance and Reporting

- Compliance with this policy shall be periodically reviewed and audited.
- Any breaches of this policy must be reported to senior management promptly.
- IT Assets must be secured to protect against unauthorized access, data breaches, and cyber threats.
- Sensitive data stored on IT assets must be encrypted and adequately protected according to data protection laws and internal security policies.

#### 4.6.1.10 Review and Revision

This Asset Management Policy will be reviewed annually or as needed to ensure its continued relevance and effectiveness.

#### 4.6.1.11 Conclusion

This policy serves as a guideline for the effective management of assets within Netradyne. All employees and stakeholders are expected to adhere to the principles and procedures outlined herein. Violations of this policy may result in disciplinary actions and legal consequences, as appropriate.

### 4.6.2 Application, Web, and Database server

The NETRADYNE server systems are configured for performance, stability, scalability, and security. All server systems, including web, application, and database servers, are built to configuration standards. These standards are applied when new systems are configured and verified as being in place before a system is installed on the network. All builds occur according to the change management and patch management policies defined in this document. They are monitored 24/7 for performance, security, and proper operation.

Access to these systems is role based and always based on the principle of least privilege.

### 4.6.3 Application and Web Servers:

Linux Ubuntu Server (n or n-1 version) is used for NETRADYNE's web and application servers and they are configured and hardened per industry best practices, considering the specific requirements. At a high level:

- All systems are hardened by disabling all services that are not used by the NETRADYNE application.
- All user and group accounts are reviewed periodically as part of internal audit/assessment.
- The number of accounts is minimized.
- All operating system and application-level passwords conform to NETRADYNE's strong password policy.
- All critical systems are protected using 2 Level Authentication and Authorization. First level for environment access and second is RSA encrypted user authorized keys of 512 bit minimum.

- Privileged account abilities are granted to a select few NETRADYNE personnel who need this level of access to perform their job function.
- All operating system and application logs are written to a secure centralized logging system built with Kibana, Logstash, and Elasticsearch software. These logs are archived for s defined time period.
- Only trusted keys and/or certificates are supported and permitted.
- Only secure protocol versions and configurations are supported and permitted.
- Only strong encryption strength is supported and permitted.

### 4.6.4 Database Servers:

PostgreSQL 11 is the database technology used by NETRADYNE. PostgreSQL Security Best Practices are utilized as the foundation for NETRADYNE's database security program.

At a high level:

- All SQL Server services are hardened by disabling all services that are not used by the NETRADYNE application.
- Database Service Accounts are all domain accounts whose passwords are known by folks who have a business need and require them to do their job.
- Database application password are maintained in a vault and is granted to the application via RBAC.
- NETRADYNE uses only TCP for database communication.
- All system stored procedures not required by the application are disabled.
- Database passwords conform to NETRADYNE's strong password policy.
- System Administrator privileges are granted to the select few NETRADYNE personnel who need this level of access to perform their job function.
- Cross database ownership is NOT used.
- Database auditing is enabled using the built-in tracing mechanism.
- All database logs and traces are written to a secure centralized logging server built with Kibana, Logstash, and Elasticsearch software, and archived for a period of 13 months.

### 4.6.5 System Build, Baseline and Hardening:

The hardening process includes the following objectives:

- Enabling only necessary services, protocols, daemons, etc. as required for the function of the system
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers

NETRADYNE leverages many inputs to ensure an appropriate configuration and security posture is maintained across policies, procedures, and assets. As industry best practices and security standards evolve, NETRADYNE adjusts and adapts its practices. Various sources are leveraged for this purpose including:

- Amazon Golden AMI continuous integration
- Centre for Internet Security (CIS)
- Security Technical Implementation Guide (*https://cyber.trackr.live/stig/U_CAN_Ubuntu_18-04_STIG/1/1*)

The compliance is measured via Amazon Inspector Tool.

Additionally, as part of the server build and hardening procedure, NETRADYNE systems are designed to serve only one primary function to prevent functions that require different security levels from co-existing on the same system. This level of function exclusivity applies across all system types, including web servers, application servers, and database servers, network components, as well as ancillary systems such as log management and file integrity monitoring.

### 4.6.6 Anti-Malware software/Endpoint Detection & Response (EDR)

Computer viruses and malware in general can cause significant damage resulting in loss of work and time to the individual, and possibly damaging the company as a whole.

The NETRADYNE IT Operations and Security team maintains EDR software on desktops and servers with the necessary centralized facilities to update virus signatures and to check for virus activity on the computing device.

Employees have been instructed not to tamper with, disable or otherwise interfere with the proper operation of anti-virus software. Employees have been further cautioned to use safe computing practices through ongoing security awareness program and to never open attachments in email from unknown or suspicious sources.

NETRADYNE uses CrowdStrike EDR for all endpoints. For more details refer below documents:

*Netradyne Antimalware Crowdstrike Procedure.pdf*
*Netradyne SOP Malware Analysis.pdf*

#### 4.6.7 Anti-spam

All company email originating from the NETRADYNE.com domain is filtered through a third-party email protection service in this case Office 365. Likewise, all email originating from outside is labelled for caution, NETRADYNE's domain is filtered for viruses and any offensive content before entering the company, there is also continuously updated blacklist of spammers. While no SPAM filtering system eliminates all form of SPAM, the current NETRADYNE system ensures that mail between NETRADYNE and its partners and customers is filtered to a level commensurate with industry standards.

NETRADYNE employees are prohibited from sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

For notification purposes of the product, we use Amazon SES and delivery guarantees. SES has a feedback mechanism; in case we get categorized as spam. We review them from time to time, ensuring we don't send bounces and rejections.

#### 4.6.8 Endpoints Configuration Baseline/Hardening

NETRADYNE has established a standard workstation configuration baseline in order to meet company objectives. These include:

- Reduced support complexity
- Consistent workstation build
- Reduced total cost of ownership
- Decrease time and simpler procurement
- Reduced mean time to detect and repair issues
- Manageable processes for exceptions

Standard build configuration is captured separately in an IT Policy Document.

#### 4.6.9 Laptop and Mobile Handheld security

Any desktop containing sensitive company or customer related information is encrypted to ensure data security. This functionality is provided through the use of disk encryption and is centrally managed at the provisioning time activity. The data on all MEP systems are encrypted using industry standard strong encryption levels, AES-256 and RC5-1024. However, at no time should any NETRADYNE employee have or use customer "Personal Identifiable Information" (PII) or "Personal Health Information" (PHI) on their workstation. Doing so is strictly prohibited and against company policy. Additionally, at no time should any workstation contain customer data in any form, to include raw data and customer databases.

- Employees log off all laptops at the end of the day.
- Personally owned computing or mobile devices and phones are never connected to the company network or to workstations unless authorized by the NETRADYNE IT Operations and Security team. This includes smart devices and other personal technology devices.
- Laptops are secured after hours by being in the possession of employees or secured in an office location to prevent theft.
- Employees immediately report the loss or theft of company owned computing assets to the NETRADYNE IT Operations and Security group. Repeated loss, abuse or damage to company owned assets may result in disciplinary action to the employee up to and including termination of employment.
- All company workstations have locking screensavers enabled after 15 minutes of inactivity. Authorized credentials are required to unlock.

### 4.6.10 Personal Laptop Firewalls

Personal Workstation firewalls are used at NETRADYNE to provide an additional layer of security against network-based attacks. These firewalls are integrated with the operating systems in use, either Windows or Mac, and each monitor and controls the incoming and outgoing network traffic for each individual host.

### 4.6.11 Remote security

#### 4.6.11.1 VPN Policy

In both the production and corporate environments, NETRADYNE uses strong security for its VPN system, including IPSEC, IKE, SHA, and Diffie Helman group 14. Active Directory based LDAP authentication is used for authentication and authorization. Employees are be given explicit access to the VPN system. An authenticated VPN connection is required before an employee working remotely can access the company network. All VPN connectivity to production is first be requested through NETRADYNE’s ticketing system and be approved by the VP, Devops and IT. All VPN connections are audited and logged to a central logging server for processing and alerting. Source IP, logged in account, connection duration, and other relevant details are collected. Idle connections are disconnected after 1 hour.

#### 4.6.11.2 Remote Administration and non-console access

The Windows Terminal Services offered with Windows Server operating systems have been deemed acceptable for use by computers operating within the NETRADYNE Windows Active Directory domain, and throughout the production datacentre. The Terminal Services or Remote Desktop service is configured to accept strong cryptography - a minimum of 256-bit encryption.

Similarly, the SSH protocol is authorized for use when connecting remotely to systems and network components. The AES-256 encryption standard is used. Systems are configured per industry best practice to ensure secure and encrypted connectivity. Sessions idle for more than 10 minutes require re-authentication to re-activate the terminal or session. All users that access the production environment will need an encryption key to access them. The key is created with RSA-512 strength as follows:

```
ssh-keygen -t rsa -b 512 -f ~/.ssh/id_rsa_512
```

#### 4.6.11.3 Wireless policy

##### 4.6.11.3.1 Employees wireless policy

The NETRADYNE corporate wireless system leverages a highly secure wireless infrastructure that includes WPA2, some of the strongest wireless protection protocols and standards available. However, at no time is customer confidential data allowed to reside or traverse the wireless network. Employees who connect to this system are segregated into a separate network for added access control.

Any additional wireless local area networks are not permitted at corporate office locations, and employees are not permitted to install wireless devices without the proper written authorization from the Vice President, Devops and IT.

The use of wireless technologies for remote virtual private network (VPN) access (e.g. at home) to corporate networks is permitted due to company approved encryption being provided by the VPN software, not the home wireless devices.

The NETRADYNE headquarters is located within a high rise building in San Diego. As a result there are hundreds of wireless networks due to the close proximity of neighbouring floors and adjacent buildings. The IT organization has scanned for networks but this practice has not proven effective at reducing the risk of rogue wireless networks. Instead, the stringent security controls applied to NETRADYNE's wireless network help to maintain risk at acceptable levels.

###### 4.6.11.3.2 Corporate Guest wireless policy

NETRADYNE guests are allowed to connect to a separate wireless network that permits access solely to the internet.

###### 4.6.11.3.3 Production wireless policy

Wireless systems are not permitted in the NETRADYNE production network. It is hosted in the Amazon Web Services (AWS) environment.

### 4.6.12 Network policy

NETRADYNE's systems are based largely upon network communications. Since communication links pass within and outside of NETRADYNE protected areas, these communications represent one of the most critical and vulnerable elements of NETRADYNE's service. Therefore, proper configuration is instrumental to ensure high performing, stable and secure operation.

NETRADYNE establishes and maintains a current network diagram that identifies all connections between other networks.

#### 4.6.12.1 Network Components

Network components include routers, switches, firewalls, load balancers, and software defined networking systems.

#### 4.6.12.2 Network Ports

NETRADYNE has authorized the following network ports in the production environment as they serve a specific business purpose:

###### 4.6.12.2.1 Inbound rules for internet sourced networks (non-RFC 1918):

- HTTP is permitted and redirected HTTPS
- HTTPS is allowed to load balancing tier for SSL termination

###### 4.6.12.2.2 Outbound rules for internet destined networks (non-RFC 1918):

Production:

- SSL connectivity to ELD Providers, Sentry, Datadog, Openweather, Firebase, mixpanel, Managed IoT devices, Here-maps.
- Operational:
- SMTP (TCP 25) from Amazon SES mail servers is allowed for mail delivery.
- NTP servers are allowed outbound access on NTP port (TCP 123) to update their own time.

###### 4.6.12.2.3 Private network rules:

- All traffic allowed between the private subnets.

#### 4.6.12.3 Network Management:

VPN connectivity to NETRADYNE's production datacentre is restricted to specific IT Operations personnel. Two level authentication is used. Personnel can first access vpn hosts after authentication using a private key. Second level is to access host based on IPTables access rules configured on the VPN server (privileged access). All other ports are not authorized and blocked by default 'deny all' configuration.

#### 4.6.12.4 Network translation

Network address translation is used extensively on NETRADYNE's firewalls to mask internal IP addresses. RFC 1918 addresses are used exclusively within the NETRADYNE environment. As a result, host addresses and are never revealed or exposed to external parties. All internal routing is also not disclosed.

#### 4.6.12.5 Network roles and responsibilities

There are several groups responsible for managing and executing changes within the NETRADYNE compute environment. All changes are designed, proposed, and approved by NETRADYNE personnel as part of change management policy.

##### 4.6.12.5.1 Change approver

All network changes are approved by either the Lead of Devops and IT, or the NETRADYNE Production IT Manager. If approving, neither will implement or execute the actual change.

##### 4.6.12.5.2 Change implementers/executors

Those implementing the change will always be authorized full time employees who work in the NETRADYNE IT Operations and Security group. All changes are managed through NETRADYNE's ticketing system, JIRA, in adherence to NETRADYNE's change management policy. The requested actions are detailed and approved in the ticket. At no time are contractors, part time employees, or consultants granted access to production facilities or system to execute changes against production and customer facing systems.

##### 4.6.12.5.3 Change validation and testers

Depending on the type of change, the person who validates the result of a change could be the same person who executed the change, a peer, and possibly NETRADYNE's own QA team. The level of testing and those who are involved are ultimately determined by the team during the change proposal and ticket creation and documentation process.

### 4.6.13 Encryption & Cryptography

Netradyne has established guidelines and procedures for the secure and effective use of encryption to protect sensitive information and ensure the confidentiality and integrity of data in rest and transit.

The use of approved encryption algorithms and industry-standard encryption protocols shall be implemented based on criticality of data. Encryption algorithms and key lengths shall comply with current best practices and standards.

Robust key management practices shall be implemented to protect encryption keys and ensure their confidentiality, integrity, and availability. Keys shall be protected against unauthorized access, loss, theft, or destruction.

Detailed guideline and policy can be referred below:

Cryptography Standards Policy.pdf

### 4.6.14 Password policy

All the end users are responsible for safeguarding their system access login and password credentials. Password must comply with the password parameters and standards identified in this policy. Passwords must meet the complexity requirements outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. Individuals with Netradyne are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this policy to ensure passwords are kept confidential and are designed to be complex and difficult to breach.

The detailed password management policy of the organization is provided in the below document:

Netradyne Password Management Policy

### 4.6.1 Logging and Monitoring

#### 4.6.1.1 General system monitoring

All NETRADYNE systems are centrally managed and monitored through the use of various industry standard logging mechanisms, to include Datadog, Kibana, Logstash, Elasticsearch, PagerDuty, Pingdom, and more. Json, XML, SYSLOG, and HTTP are used to transmit events to the collection systems. Security events, key functionality events, system response, daemon/service status, resource state status (e.g. CPU, RAM, DISK), all generate alerts in real-time or via periodic reports and are responded to by the NETRADYNE IT Operations and Security team, 24x7. Additionally, daily reviews of key security and sensitive system events occur. All logged events are retained for 13 months.

#### 4.6.1.2 Database Security and Monitoring

PostgreSQL 11 is the database technology used by NETRADYNE. PostgreSQL Security Best Practices are utilized as the foundation for NETRADYNE's database security program. All SQL Server services are hardened by disabling all services that are not used by the NETRADYNE application. All Service Accounts are all domain accounts whose passwords are known by only those who require it to do their job. NETRADYNE uses only TCP for database communication. All system stored procedures not required by the application are disabled. Database passwords conform to NETRADYNE's strong password policy. System Administrator privileges are granted to a limited number of NETRADYNE personnel who need this level of access to perform their job function. Cross database ownership is NOT used. Database auditing is enabled using the built in tracing mechanism. All database traces are written to a secure system using File beat and ELK for a period of 13 months.

#### 4.6.1.3 Application Security and Monitoring'

NETRADYNE applications are configured to log details of the user sessions and the actions users perform. It also records administration events such as operations with user accounts. User actions are stored and used for monthly usage reports. Administration events, such as creation or deactivation of a user account, lockout or expiration of an account, password changes, assigning or removing a user role, adding, or removing a user from a group, are also logged. All such activities are sent to a centralized log management server built using a combination of auditD, logstash, winlogbeat, kibana, CloudTrail, and Elasticsearch. Logs are generally retained infinitely depending on need, sensitivity, and other factors.

### 4.6.2 Firewall and Routing Systems Policy

The NETRADYNE firewall systems are high performance and highly available systems that create discrete network segments that form a traditional tiered network topology and AWS Virtual Private Cloud Networking guarantees.

These systems are configured for high availability (n+1) and are updated according to the change management and patch management policies defined in this document. They are monitored 24/7 for performance, security, and proper operation.

Firewall rules are created and based on the principle of least access and permit only the traffic necessary for proper operation. Firewall rules and justification are detailed in the IT Policy document and NACL configuration of AWS VPCs and security group configuration of AWS EC2, and all are reviewed at least every 6 months for validity.

The firewalls perform all primary routing and firewalling functions within the NETRADYNE service platform. Most of these systems also perform intrusion prevention system (IPS), anti-malware and URL filtering.

#### 4.6.2.1 Web Application Firewall

The deep packet inspection of the NETRADYNE firewall function enables blocking malicious traffic. They are monitored 24/7 for performance, security, and proper operation. We use a Cisco ASA appliance to get this functionality. We conduct regular maintenance on the appliance.

#### 4.6.2.2 Inline Packet inspection on corporate networks

The deep packet inspection of the NETRADYNE firewall function enables blocking malicious traffic. They are monitored 24/7 for performance, security, and proper operation. We use a Cisco ASA appliance to get this functionality. We conduct regular maintenance on the appliance.

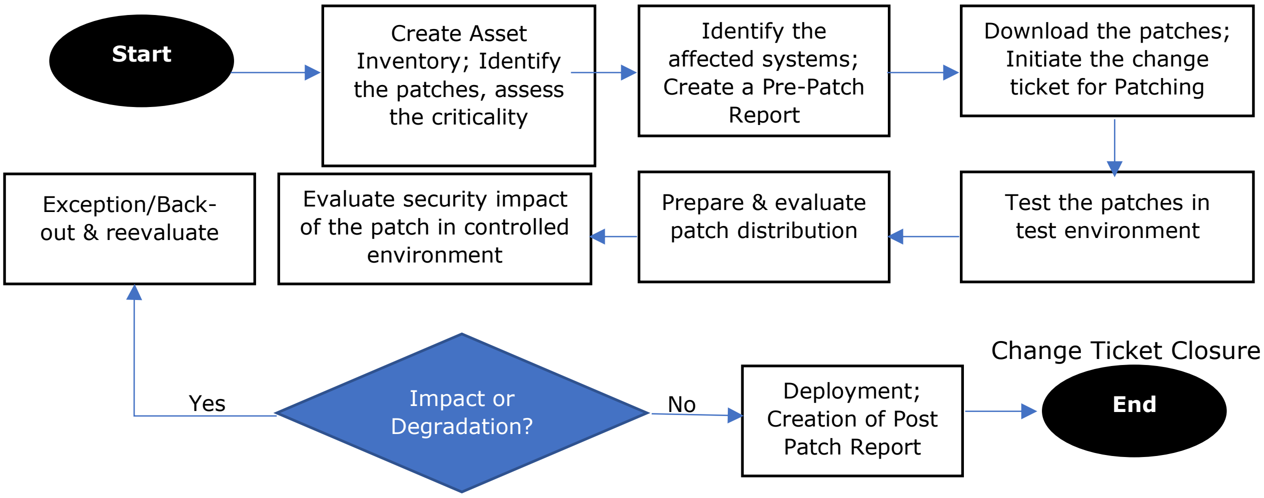
### 4.6.3 Vulnerability, System Update and Patch Management

There are a high number of systems and applications in use at NETRADYNE and ensuring they are fully patched and secure in a controlled manner is a priority. This includes all aspects of infrastructure, applications, and any other hardware and software.

In its corporate and development environments, NETRADYNE currently packaging and configuration management system to ensure all systems receive the latest security and functional software patches and fixes as ready. In the production environment, NETRADYNE works to ensure patches are applied in a controlled and non-disruptive manner using a group of tools. Critical Severity patches are scheduled to reviewed, evaluated, and deployed immediately or within 5 days; High severity patches are also reviewed and deployed immediately or within 30 days. Medium and Low severity patches are reviewed as part of the internal audit process and generally deployed within 3-12 months depending on relevance and severity.

All patches are also deployed in adherence to NETRADYNE's change management policy described in this document. This includes fully testing patches before deployment to production environments.

Process flow diagram is illustrated below for patch management:


Start
Create Asset Inventory; Identify the patches, assess the criticality
Identify the affected systems; Create a Pre-Patch Report
Download the patches; Initiate the change ticket for Patching
Test the patches in test environment
Prepare & evaluate patch distribution
Evaluate security impact of the patch in controlled environment
Exception/Back-out & reevaluate
Yes
Impact or Degradation?
No
Deployment; Creation of Post Patch Report
Change Ticket Closure
End

For more details, please refer to Netradyne Vulnerability & Patch Management Process.pdf

### 4.6.4 Network Time

NETRADYNE leverages the network time protocol (NTP) to ensure systems are time synchronized across corporate, development, and production systems. Having systems synchronized is critical to ensure timely issue resolution.

In the production environment, NETRADYNE leverages NTP services provided by canonical and amazon pool servers. All NETRADYNE systems are configured to use internal master NTP servers, and the masters contact NIST.

## 4.7 Administrative Controls

### 4.7.1 Personnel Status Change Policy

#### 4.7.1.1 Onboarding policy

The Information Technology Operations and Security group works closely with Human Resources and department heads to ensure new and departing employees, contractors, and consultants are processed efficiently and securely.

Hiring procedures provide the single most effective mechanism for screening applicants, which will assist in preventing theft, fraud, misuse of information, or sabotage at the hands of employees. For this reason, NETRADYNE sets forth the following pre-employment screening program for any personnel performing work for NETRADYNE.

##### 4.7.1.1.1.1 Full or Part Time Employees

Completed employment application forms and a job description are key documents to be used during applicant screening and the actual job interview.

A complete verification of the applicant's background and experience is required, consistent with the NETRADYNE Human Resources processes and privacy policy. This includes:

- Employment report
- Education report
- Personal reference checks
- Prohibited parties' verification, including:
- Once hired, they:
- Sign the NETRADYNE non-disclosure agreement (NDA)
- Sign the NETRADYNE Terms and conditions
- Sign the Employment Confidential Information and Invention Assignment Agreement.

#### 4.7.1.2 Contractors and Consultants

Depending on the role, consultants and contractors are subject to the same screening requirements as regular NETRADYNE employees and will undergo background screening by NETRADYNE upon hiring. Additional screening is at the discretion of the NETRADYNE IT Operations and Security team and Lead, Devops and IT. However, the contractor or consulting firm must also attest to some form of personnel screening and background checks before any work commences for NETRADYNE.

For US based contractors or consultants, the following is conducted:

- Employment report
- Education report
- Personal reference checks
- Prohibited parties verification, including:
- Office of Foreign Assets Control (OFAC)
- Specially Designated Nationals / Terrorists / Narcotics Traffickers and
- Blocked Persons
- Debarred Parties, Denied Persons, Entity List, Unverified List and Palestinians Legislative Council 31 CFR Part 594

For consultants working from offshore locations, or, working for companies not based in the US, the following is conducted at a minimum:

- Employment report
- Education report

Before a contractor or consultant can perform work for NETRADYNE they:

- Sign the NETRADYNE non-disclosure agreement (NDA)
- Sign the NETRADYNE Terms and conditions (AUP)
- Sign the Employment Confidential Information and Invention Assignment Agreement.

Additionally, if the contractor or consultant is hired and involved in the processing or handling of NETRADYNE customer data, they:

- Undergo training about Data Protection Agreement with NETRADYNE.

All NETRADYNE positions are examined to determine whether they are consistent with these guidelines. All such determinations are documented and forwarded to the manager and Human Resources for inclusion in the official position description.

### 4.7.2 Hiring Procedures

Prior to commencing any level of work for NETRADYNE, the Human Resources and NETRADYNE IT Operations and Security teamwork with the hiring manager to document required system/network access, duration of requested access, and other details to ensure access entitlements are accurate. Any personnel to perform work for NETRADYNE undergo the same procedure upon arrival or role change. Upon exit from the company, or a role change, a similar process is conducted to ensure accurate access entitlement revocation is conducted and documented.

### 4.7.3 Access rights

Employees are granted access based on their role and job function in coordination with HR and hiring manager. This is approached from a functional, cost, and security perspective to ensure an appropriate level of access is provided. At no time are employees given access to sensitive systems, areas, and data without approval from HR, the hiring manager, and the security team.

Additional scrutiny is placed on granting access to NETRADYNE’s production datacentre wherein NETRADYNE’s service is delivered. This is currently located in an Amazon Web Services (AWS) facility known as US West N. California (us-west-1). AWS customers are not permitted physical access to this facility, and only the Lead, Devops and IT can approve logical and remote access to the environment that operates in this facility. Persistent remote access is limited to a small team of NETRADYNE IT Operations and Security personnel who own the responsibility of delivering and protecting NETRADYNE’s service to customers.

### 4.7.4 Termination Policy

#### 4.7.4.1 Voluntary Termination

This type of termination is the most agreeable for all parties involved and poses the least concern from a security point of view. However, voluntary terminations are analysed to determine motive.

#### 4.7.4.2 Job Abandonment

Job abandonment is always scrutinized until fully investigated and the matter resolved. If a person occupied a sensitive Information Technology Operations and Security position, all security actions required when an employee is involuntarily terminated also apply (see the paragraph entitled Involuntary Termination). If the employee is suspected of having knowledge of the computer system or the security features beyond that required of his position, additional security precautions may be required. A member of the NETRADYNE IT Operations and Security team will be assigned to carefully investigate and take any action necessary.

#### 4.7.4.3 Involuntary Termination

Involuntary termination of any Information Technology Operations and Security personnel, for whatever reason, will always be considered a serious matter. Terminations for unsatisfactory performance or dishonesty are a particularly serious threat to NETRADYNE.

#### 4.7.4.4 Termination Procedures

The IT organization follows a stringent procedure for ensuring that persons conducting work for NETRADYNE are accurately and fully removed from the information technology systems. The process begins upon notification from the Human Resources group indicating the following: exact time/date the person is to be removed from the company systems as well as any additional instructions in regard to organizational structure changes. Account disablement is then configured to occur at that time. The request is ticketed and tracked to completion. In addition, the Human Resource organization maintains its own termination policy and procedures to complete this process. This procedure includes the return of all keys, security key cards, hardware, software, data and documentation to the supervisor or Human Resources personnel as part of exit interview procedure.

### 4.7.5 Employee Security Awareness policy

#### 4.7.5.1 Employee IT Security Training

NETRADYNE employees receive an Information Technology Operations and Security briefing upon being hired, periodic security information throughout the year via email, and all participate in annual mandatory security awareness training. Topics includes password protection, workstation security, visitor policy, PHI/PII/NPPI, customer system and data protection in general, and more. At the conclusion of this training they review and digitally attest to the company Acceptable Use Policy.

#### 4.7.5.2 Information Technology Operations and Security personnel IT Security Training

Each new Information Technology Operations and Security systems employee receives a NETRADYNE Information Technology Operations and Security orientation. Such information provides a sound basis for an understanding of NETRADYNE policy regarding Information Technology Operations and Security and the reasons for it. Senior NETRADYNE management is actively involved and participates in motivating employees on this subject.

All new NETRADYNE employees are familiarized with specific security responsibilities of their position, and specific procedures established for reporting or responding to security violations or emergency situations.

All NETRADYNE Information Technology systems employees will receive an annual security review, which will reaffirm their security responsibilities and make them aware of areas of security emphasis. The review is completed each year and will cover current NETRADYNE Information Technology Operations and Security policy, procedures, and practices.

#### 4.7.5.3 Contractor and consultant IT security training

The provisions of the Employee Security Awareness Policy apply, in their entirety, to contractor or consultant personnel. All such personnel will abide by the restrictions placed upon NETRADYNE employees and are expected to support NETRADYNE Information Technology Security objectives. At the conclusion of this training they review and digitally attest to the company Acceptable Use Policy.

#### 4.7.5.4 Third Party Service Provider Security Training

The provisions of the Employee Security Awareness Policy apply, in their entirety, to third party service providers and vendors. All providers are evaluated to determine the level of their own security awareness training and equivalent programs may be found acceptable to meet NETRADYNE’s requirements.

## 4.8 Sensitive Data – Personal Identifiable Information (PII)

Netradyne defines Personal Identifiable Information (PII) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual ‘s identity.

Netradyne manages PII using a JIRA Epic https://Netradyne.atlassian.net/browse/IDMS-8259

## 4.9 Incident Response and Management Policy

### 4.9.1 General Incidents

The primary goal of the General Incident Response and Management policy is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations resulting from incidents. Essentially, this policy defines the process whereby an exception to normal service operation is investigated and appropriate action taken. This is to ensure the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within SLA limits.

#### 4.9.1.1 Objectives

The key objective is to provide a consistent process to ensure that:

- Monitoring and response for incidents occurs 24/7/365 by a team dedicated to target service delivery objectives and agreements.
- Specific incident response procedures are understood so that incidents are properly logged and routed
- Incident status is accurately reported
- Queue of unresolved incidents is visible and reported
- Incidents are properly prioritized and handled in the appropriate sequence
- Resolution provided meets the requirements of the SLA

#### 4.9.1.2 Scope

The scope of this policy includes all critical system components that could impact NETRADYNE's customers, as well as those that could impact services provided to company employees.

#### 4.9.1.3 Impact

Impact is determined by how many personnel or functions are affected, and it is used in determining the priority for resolution. There are three grades of impact:

#### 4.9.1.4 3 - Low

One or two personnel. Service is degraded but still operating within SLA specifications

#### 4.9.1.5 2 - Medium

Multiple personnel in one physical location. Service is degraded and still functional but not operating within SLA specifications. It appears the cause of the incident falls across multiple service provider groups

#### 4.9.1.6 1 - High

All users of a specific service. Personnel from multiple agencies are affected. Public facing service is unavailable

#### 4.9.1.7 Incident

An incident can manifest itself in several ways; as a disruption to an IT service; a degradation in the quality of an IT service; the failure of any hardware or software component; a discovered physical or security risk. Failure of any Item, software, or hardware, used in the support of a system that has not yet affected service is also an Incident. For example, the failure of one component of a redundant high availability configuration is an incident even though it does not interrupt or degrade service.

Additionally, the discovery of unauthorized wireless access points, or physically connected devices, is an incident requiring response per this policy.

A design flaw does not create an incident. If the product is working as designed, even though the design is not correct, the correction needs to take the form of a service request to modify the design. The service request may be expedited based upon the need, but it is still a modification, not a repair.

#### 4.9.1.8 Incident Repository

The Incident Repository is NETRADYNE's database containing relevant information about all Incidents whether they have been resolved or not. General status information along with notes related to activity are also be maintained in a format that supports standardized reporting. At NETRADYNE, the incident repository is contained within an Atlassian JIRA item tracking system.

#### 4.9.1.9 Priority

Priority is determined by utilizing a combination of the incident's impact and severity.

#### 4.9.1.10 Response

Time elapsed between the time the incident is reported and the time it is assigned to an individual for resolution.

#### 4.9.1.11 Resolution

Service is restored to a point where the customer can perform their job. In some cases, this may only be a work around solution until the root cause of the incident is identified and corrected.

#### 4.9.1.12 Service Level Agreement

The Service Level Agreement (SLA) is the agreement between NETRADYNE and its customers. It outlines the services to be provided and the operational support levels. These are defined in the master service agreement.

#### 4.9.1.13 Service Level Target

Service Level Target is a commitment that is documented as service level agreement. Service Level Targets are based on Service Level Requirements and are needed to ensure that services continue to meet the original Service Level Requirements.

#### 4.9.1.14 Severity

Severity is determined by how much the user is restricted from performing their work. In general, there are four grades of severity: minor, normal, critical and blocker. These are described in the master services agreement.

#### 4.9.1.15 Categorization

In order to adequately determine if SLA's are met, it is necessary to correctly categorize and prioritize incidents quickly. The goals of proper categorization are:

- Identify Service impacted and appropriate SLA and escalation timelines
- Indicate what support groups need to be involved
- Provide meaningful metrics on system reliability

#### 4.9.1.16 Priority Determination

The priority given to an incident that will determine how quickly it is scheduled for resolution will be set depending upon a combination of the incident severity and impact.

#### 4.9.1.17 Incident ownership and escalation

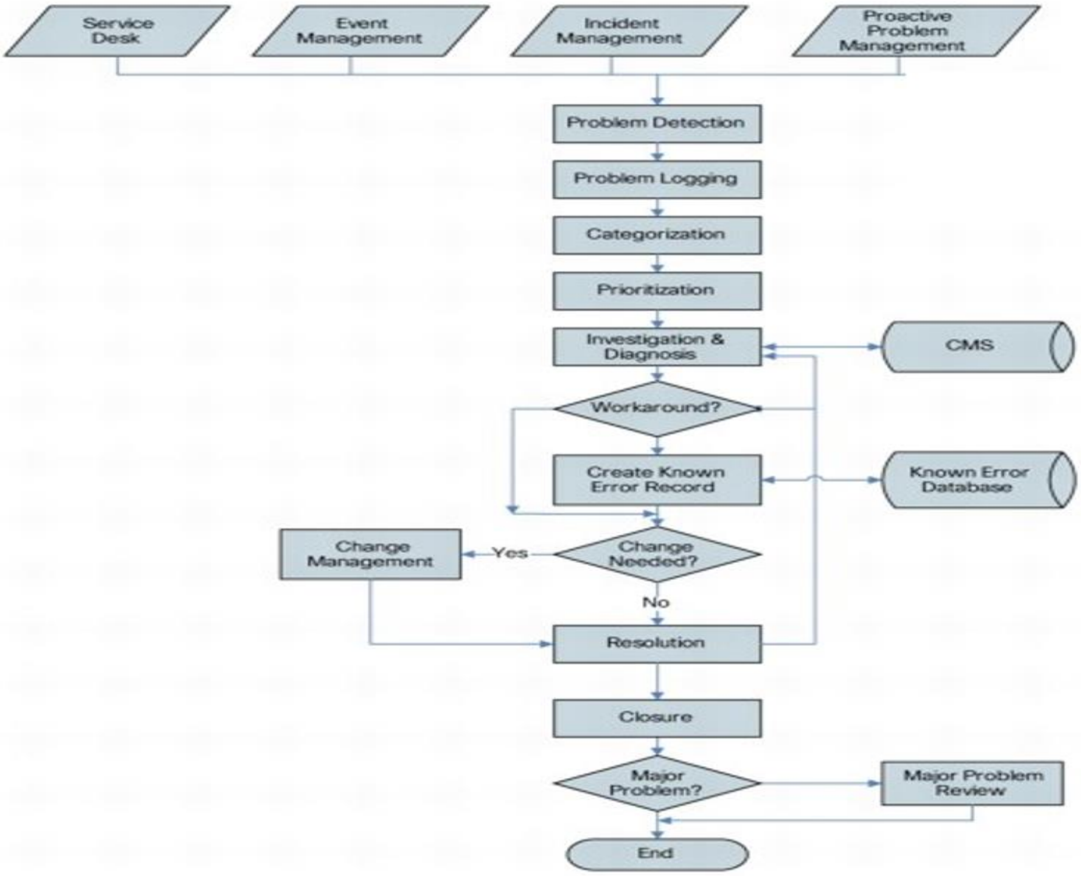
At all times during the life cycle of an incident, ownership remains with NETRADYNE support group. Regardless of where an incident is referred to during its life, the support organization is responsible for tracking progress, keeping users informed and ultimately for incident closure.

This remains true for issues requiring escalation.

#### 4.9.1.18 Policy reviews and update

This policy will be reviewed annually for appropriateness and alignment with industry best practices, compliance, and regulation. It will continuously evolve according to lessons learned. Additionally, when these changes occur, or as part of an annual tabletop exercise, personnel are trained to ensure they're aware of their security breach responsibility.

Incident Workflow diagram:



### 4.9.2 Security Incidents

#### 4.9.2.1 Purpose & Scope

The purpose of this policy is to establish a method to manage and resolve security incidents. Additionally, it provides guidelines for the protection of any material or data that is impacted or put at risk as a result of an incident, vulnerability, or abnormality.

This procedure is to be used whenever a suspected or actual compromise of information system resources has occurred. NETRADYNE's data breach and notification policy is designed to disclose any breach of data to any customer whose unencrypted personal information was, or is reasonably believed to have been, obtained by an unauthorized person. Such information could include reports, documentation, digital data, computer hardware, software, and telecommunication and application systems. It includes adherence to legal requirements for reporting compromises and data breach.

#### 4.9.2.2 Definitions

Any event, actual or reasonably suspected to have occurred, which destroys or degrades the availability, integrity, or confidentiality of NETRADYNE information system resources, computer-based systems, computer-maintained data files, documents, or procedures.

#### 4.9.2.3 Responsibilities

NETRADYNE's employees are responsible for notifying supervisory employees whenever a suspected or actual compromise of NETRADYNE's systems occurs, or any abnormality that may have an impact on the integrity of NETRADYNE's security posture.

The Information Technology Operations and Security group is responsible for assigning a security representative to investigate the condition, assemble information, complete an Information Technology Security Incident Report and interface with the areas required to develop a solution.

All areas within NETRADYNE are responsible for supporting the investigation of a security incident that is conducted by the Information Technology Operations and Security group. They will also the investigation as necessary by applying their specific domain expertise.

#### 4.9.2.4 Procedure

Security incidents are generated by a system or machine alert, notification, audible alarm, or a report from NETRADYNE employees or non-employees. When a potential or actual security incident/violation occurs, the individual will inform his supervisor who will request the Information Technology Operations and Security group to investigate the situation. The importance of immediate notification and reporting of a security incident is a key factor in reducing vulnerability and/or exposure, as well as speeding recovery.

The reporting area will assemble all relevant information and material identified with the incident, if possible. Any material involved will be kept preserving and retain its authenticity for the investigation and evaluation process.

Upon notification, the Information Technology Operations and Security group will assign a security representative to investigate the reported situation. The security representative will obtain the facts from individuals regarding the incident to file an Information Technology Security Incident Report. The report will not include interjection of personal or preconceived opinions and views of the incident. Any interjection of personal views may bias the veracity and completeness of the investigation.

While compiling all relevant information on the incident, the security representative will include two major items required for the evaluation.

- A narrative description of events and actions associated with this incident. This is in chronological sequence. This should include time and location, beginning prior to and continuing through the incident. The description will include the initial impact on the information system and/or impact to NETRADYNE's service in the area of reliability or data integrity.
- The detailed steps or actions by individuals (by title or area) in chronological sequence that may have been implemented to correct, control, or resolve the effects or results of the incident.

Additionally, NETRADYNE will take the following actions during a security or data privacy incident:

- Identify to the customer what specific data, by customer and/or account number, has or may have been accessed. Customers are contacted through their assigned Customer Success Manager. Along with primary business points of contact, CSMs maintain security and data privacy contact information for this purpose. The Customer Success

Manager will provide regular status updates and investigation results to the customer until the incident is closed.

- Contact the payment brands with which NETRADYNE integrates and follow their specific incident response procedures.
- Take measures to contain and control the incident to prevent further unauthorized access.
- NETRADYNE will avoid making any public statements about any incident involving customer's data.

#### 4.9.2.5 Analysis/Evaluation

Analysis or evaluation of a security incident should not be attempted until all relevant facts and information have been assembled. Any premature analysis or evaluation of an incident may produce a biased and incomplete result.

The NETRADYNE IT Operations and Security group provides recommendations to eliminate the recurrence of a specific incident in the future.

In the case of an incident involving direct impact to NETRADYNE's customers, such as in the case of a service degrading denial of service (DOS) attack, NETRADYNE will work closely with its vendors and key infrastructure providers to investigate and provide technical assistance.

#### 4.9.2.6 Record Keeping and Notification

The Information Technology Security Incident Report is completed within five working days and is permanently recorded in NETRADYNE's document management system. All parties that could be impacted by a Security Incident are informed immediately. This includes internal departments, customers, and vendors.

#### 4.9.2.7 Continuous vulnerability awareness and identification

NETRADYNE maintains continuous awareness on its security posture. Various mechanisms are used for this purpose, including daily vulnerability scans, alerts from intrusion prevention systems, subscription to security periodicals, and email newsletters from reputable security sources, Additionally, at least annually, a tabletop exercise is held to validate this policy and provide a training session to the NETRADYNE IT Operations and Security team.

When new vulnerabilities are discovered through any of these channels, NETRADYNE reviews the issue and its risk rating, assigns its own risk rating relative to NETRADYNE's technology stack, and establishes a plan of action with any available input from vendors. This includes but is not limited to NETRADYNE's cloud hosting providers Amazon Web Services (AWS). Further, vulnerability scans directed at external and internal systems are conducted on a quarterly basis.

## 4.10 Vulnerability Assessment and Penetration policy

Ensuring the security of NETRADYNE's systems is a top priority for the NETRADYNE IT Operations and Security team. NETRADYNE conducts continuous security testing that includes internal and external vulnerability scans and penetration testing, as well as web application vulnerability assessments.

Vulnerability scans are executed in two ways: from an internally sourced host on a monthly basis, and from an externally sourced system on a periodic basis. They are performed using a recognized product in vulnerability assessment scans. Their primary purpose is to discover software vulnerabilities. These scans also occur when major product or infrastructure changes occur. They are also directed toward development systems on an ad-hoc basis as necessary.

Penetration scans are conducted at least once a year as part of NETRADYNE's annual audit. They also occur when new functionality or major product changes occur. The goal is to ensure security is maintained at all times.

Web application vulnerability assessments are conducted via third party organizations that specialize in application security. They are performed at least annually or after major product developments and changes.

The results of these three activities are shared with key staff to ensure all potential issues are addressed appropriately and in accordance with NETRADYNE's patch management policy. At a minimum, all the following OWASP Top vulnerability types are included in this activity:

- Injection flaws, particularly SQL injection, operating system command injection, LDAP, and XPath injection flaws as well as other injection flaws.
- Buffer overflows
- Insecure cryptographic storage
- Insecure communications
- Improper error handling
- Cross-site scripting (XSS)
- Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
- Cross-site request forgery (CSRF)
- Broken authentication and session management

A retest is conducted to validate that all issues are remediated after corrective actions are completed.

All scans and penetration tests are recorded and stored in the IT ticketing system both for audit purposes and sharing with prospects and customers. These are available to customers and prospects. System configuration standards are updated as new vulnerability issues are identified and addressed. Lastly, these scans, along with frequent and timely patching of all NETRADYNE systems, ensure a highly secure compute environment.

## 4.11 Acceptable use policy

NETRADYNE's acceptable use of assets is documented in the IT policy. It defines activities that are acceptable and authorized when using NETRADYNE's systems. It is shared with anyone working for NETRADYNE in any capacity, as well as with third party service providers (TPSP). Penalties for failure to comply are also described, and any deviations from it require prior explicit and written approval from the Lead, Devops and IT.

## 4.12 Change Management policy

### 4.12.1 Definition and Goals

NETRADYNE's Change Management policy incorporates planning, organizing, controlling, executing, and monitoring changes that affect the delivery of IT services. It encompasses all components and activities required to direct additions, modifications, and deletions to the IT environment; software, systems, network, processes, and environmental facilities.

This policy ensures that standardized methods and procedures are used for efficient and prompt handling of all changes in order to minimize the impact of incidents upon service quality and to improve the operations of the organization. The purpose of Change Management is to ensure that all elements are in place, all parties notified and trained, and the schedule for implementation is approved and coordinated with all other activities in the organization.

### 4.12.2 Purpose

- Better align IT services to business requirements
- Increase visibility and communication of Changes to both business and service-support staff
- Improve risk assessment

- Reduce adverse impact of Changes on the quality of services and on Service Level Agreements
- Better assess the cost of proposed Changes before they are incurred
- Make fewer changes that require rollback, along with an increased ability to do this more easily when necessary
- Improve Problem and Availability Management through the use of valuable management information relating to changes accumulated through the Change Management process
- Increase productivity of users - through less disruption and higher-quality services
- Increase productivity of key personnel through less need for diversion from planned duties to implement urgent Changes or back-out erroneous Changes
- Create a greater ability to accommodate a large volume of Changes
- Enhance the business perception of IT through an improved quality of service and a professional approach.
- Foster and facilitate a high level of communication amongst all IT departments
- Contribute to the successful implementation of configuration management within IT

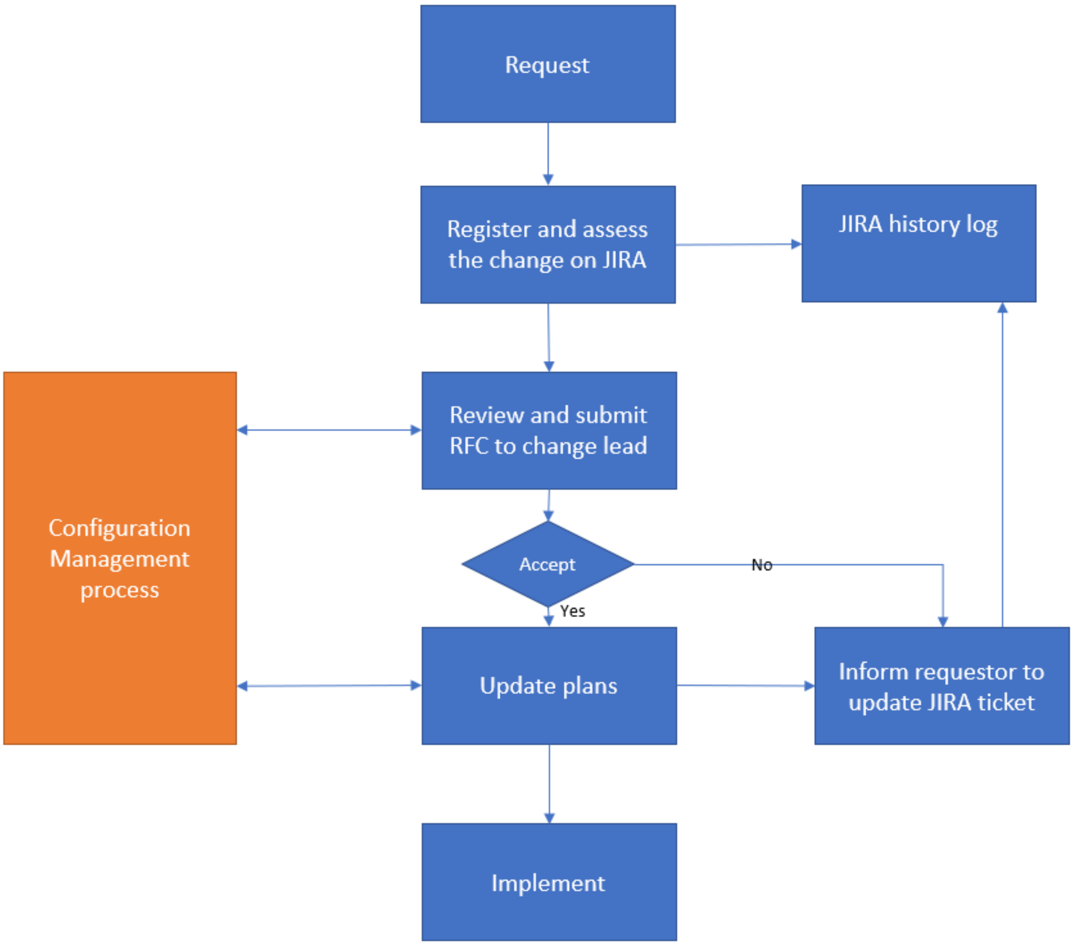
### 4.12.3 Change description

Information Technology changes involve changes to the NETRADYNE environment and include application, database, network, security, and server hardware and operating systems. These changes typically relate to application bugs and feature requests, system fixes and patches, security patches, network hardware software upgrades, and all other changes related to the NETRADYNE suite of applications and related databases.

### 4.12.4 Change Procedure

- All changes are communicated 48 hours in advance and communicated to all parties, to include IT department, business owners and other stakeholders involved or impacted by the change. The only exception is during emergency change requests, in which case this is indicated.
- Communication includes:
  - Description of the change
  - Testing plan to ensure desired change result
  - Implementation plan
  - Implementation date/time
  - Effort duration
  - Outage duration
  - Customer impact
  - Rollback plan
  - Approver
- Requests for changes are always peer reviewed and then approved by management.
- All ticket information is captured in the NETRADYNE ticketing system, JIRA.
- In the case of changes requiring vendor assistance, these would also be managed through NETRADYNE’s ticketing system, JIRA, in adherence to NETRADYNE’s change management.
- Emergency changes are also documented and approved by management. In this case, the team implementing the change conducts a change peer review involving all team members, assess customer impact, and establishes a rollback plan in accordance with the standard change management policy.
- Any unintended behaviour of a change is communicated immediately to establish plan of action to address.
- Completion of change is communicated to provide an “all clear” notification to all involved parties.

### 4.12.5 Change management process flow chart


Request
Register and assess the change on JIRA
JIRA history log
Configuration Management process
Review and submit RFC to change lead
Accept
No
Yes
Update plans
Inform requestor to update JIRA ticket
Implement

## 4.13 Data Policy

### 4.13.1 Overview

Customer and corporate data are a highly valuable part of NETRADYNE, and due to the high volume of credit card transactions and customer information processed by NETRADYNE, this data is protected at all stages of the data life cycle. The purpose of this policy is to establish effective controls to govern the use of this data.

### 4.13.2 Scope

The scope of this policy includes all NETRADYNE servers and systems that store customer and corporate data, especially relating to the NETRADYNE service at our third party hosted facilities.

### 4.13.3 Proprietary Information and Credit Card Data

Customer and corporate proprietary information, specifically customer credit card data, will be stored encrypted and accessible only to the authorized customers who created the data for 90 days and based on business need. Specifically, with regard to credit card information within the NETRADYNE application, all credit card information is masked for all users unless explicitly granted to someone holding the Administrator role.

After the 90-day period, the data will be removed from the database via automated tasks and only exist on tiered archival storage. This security policy explicitly prohibits permanent storing of any sensitive authorization data such as CVV or CVV2 codes which are only used once for the transaction.

### 4.13.4 Data Backups and Restores

Netradyne data backup and restore policy is established for ensuring data integrity, availability, and recoverability. The said implementation is customized to Netradyne's needs and compliance requirements, where majority of resources are hosted on Amazon Web Services (AWS)

A brief overview of implemented backup and restore controls are listed below:

#### 4.13.4.1 Data Classification:

Data are classified based on its criticality and sensitivity levels. This classification helps determine the appropriate backup frequency, retention periods, and security measures.

#### 4.13.4.2 Backup Frequency:

All business-critical data requires more frequent backups (daily basis) to minimize potential data loss.

#### 4.13.4.3 Retention Period:

Netradyne defines how long back up data need to be retained. This depends on regulatory requirements, business needs and follow the Netradyne Data Retention Policy (DRP). Netradyne Data Retention Policy is described in section 4.13.7. Netradyne's major Cloud Service Provide (AWS) offers different storage options (e.g., Amazon S3, Glacier) to accommodate short-term and long-term retention and the same are being leveraged.

#### 4.13.4.4 Incremental Backups:

Netradyne implements incremental backups to optimize storage and reduce backup durations. Incremental backups only store changes made since the last backup, reducing the amount of data transferred and stored.

#### 4.13.4.5 Redundancy:

Netradyne ensure backups are stored in separate AWS regions or Availability Zones (AZs) to protect against outages.

#### 4.13.4.6 Encryption:

Netradyne encrypt the backup data to protect sensitive information. AWS provides options for server-side encryption (SSE) using AWS Key Management Service (KMS).

#### 4.13.4.7 Testing and Validation:

Netradyne regularly tests the backup and restore processes to ensure they function as expected. Periodic restoration drills can help identify any issues, such as incomplete backups or errors in the restore workflow.

#### 4.13.4.8 Access Control:

Netradyne implement appropriate access controls and permissions for backup data. Only authorized personnel should have access to backups and the ability to perform restores.

#### 4.13.4.9 Documentation and Auditing:

Netradyne defines the backup and restore policies, including procedures, responsibilities, and contact information. Netradyne does regular review and update the policy to reflect any changes in its infrastructure or compliance requirements.

### 4.13.5 Data Classification Policy

All data handled by the company can be classified into one of four security levels, each of which requires different levels of protection.  Employees must be able to identify the security classification of the data they work with.  If there are questions as to the level of data classification, employees are required to obtain clarification from their management.

#### 4.13.5.1 Public

This classification applies to information that is available to the general public and intended for distribution outside the organization. This information may be freely disseminated without potential harm.   Examples include product and service brochures, advertisements, job opening announcements, and press releases.

#### 4.13.5.2 For internal use only

This classification applies to all other information that does not clearly fit into the other classifications.  The unauthorized disclosure, modification, or destruction of this information is not expected to impact the organization seriously or adversely, its customers, its employees, or its business partners. Examples include the company telephone directory, new employee training materials, and internal policy documents.

#### 4.13.5.3 CONFIDENTIAL

This classification applies to information that is intended for use within the organization.  Its unauthorized disclosure could adversely impact the organization, its customers, its employees, and its business partners.  Examples include medical information, appointment schedules, account records, department financial data, purchasing information, vendor contracts, merger and acquisition documents, corporate level strategic plans, and litigation strategy memos.

#### 4.13.5.4 RESTRICTED CONFIDENTIAL

This classification applies to the most sensitive medical, financial, and business information that is intended strictly for use within the organization or hosted on behalf of a NETRADYNE client or partner.  Its unauthorized disclosure could seriously and adversely impact the organization, its customers, its employees, and its business partners.  For example, customer data hosted in the NETRADYNE data centre, any code, data extracts, development samples, call recordings, design documents, and test data files that pertain to customers, as well as any data and documentation that contain Personally Identifiable Information (PII), or Non-Public Information (NPI).

### 4.13.6 Data protection policies

This section describes procedures that are used to protect confidential data in transit over networks and in storage.  Employees that have access to confidential information understand that the requirements below protect this information as it is transmitted or stored. For more information on Personal Data Protection Policy, please refer to Personal_Data_Protection_Policy.pdf.

All access to Company and Consumer Confidential data in electronic format are authenticated and authorized for a valid business purpose.  Security controls for authentication, authorization, and logging are approved by the Lead, Devops and IT.

### 4.13.7 Data Retention policy

The data retention period indicates the time for which data is accessible to the customer. It can be defined separately for each data category. Following are the default retention periods.

- Video Data Retention Period – 3 Months
  - i.e. Video data is accessible for the previous 3 months and the current running month.
- Non-Video Data Retention Period – 12 Months
  - i.e. Non-Video data is accessible for the previous 12 months and the current running month.

#### 4.13.7.1 Data Retention Policy Types

Data Retention Policy type indicates the data treatment post retention period. Following are the supported types.

##### 4.13.7.1.1 Type A:

Video Data is anonymized post retention period.

##### 4.13.7.1.2 Type B:

Video and Non-Video data is anonymized post retention period.

##### 4.13.7.1.3 Type C:

Video and Non-Video data is deleted post retention period.

##### 4.13.7.1.4 Type A-C:

Video Data is anonymized post retention period. Video data can be deleted on request at end of the contract.

## 4.14 Customer Support

All application components are monitored 24x7 and email alerts are sent when NETRADYNE service and system errors occur. All L2 and L3 support personnel are NETRADYNE employees trained specifically in the NETRADYNE application. Response times vary based on the issue severity. NETRADYNE Support is available via the following link, as is a breakdown of response times by severity level: https://www.NETRADYNE.com/support/

## 4.15 Contingency Planning & Business Continuity

The objective of contingency planning/Business continuity is to provide for the continuity of services necessary to effectively support overall NETRADYNE operations in a crisis situation. The contingency plan provides for both the emergency backup of critical applications as well as the orderly recovery and restoration of services. The contingency plan is discussed in detail in:

*NETRADYNE BUSINESS CONTINUITY PLAN.pdf*

At a high level, it accomplishes the following:

- Provides a level of service necessary to ensure continued NETRADYNE operations for critical applications
- Includes activities required to maintain the capability for effective emergency operations and recovery of lost services
- Documents the priority for recovery of critical operations based upon potential impact on overall NETRADYNE operations
- Contingency planning is in scope of all development projects tested to ensure the effectiveness of the plan

## 4.16 Netradyne Audit/Assessment Policy

### 4.16.1 Internal Audit/Assessment Policy

The NETRADYNE Infosec team regularly reviews its policies and systems for accuracy, as well as for new events and issues, as part of defined personnel roles and responsibilities. This effort is referred to as an internal audit and, along with other monitoring systems and processes, any deviation from documented and standard activities is immediately investigated and a plan of action is formulated and implemented. Internal audits are conducted atleast once in a year and are captured in the NETRADYNE ticketing system along with any findings.

- Identity and Access Control Management
- IT and Network security
- Information Security Governance
- Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Security Operations
- Business Continuity, Disaster Recovery and Pandemic Readiness planning and testing
- Compliance
- Physical Security

### 4.16.2 External Independent Audit/Assessment Policy

Netradyne will periodically indulge an Independent Security audit firm which outlines the procedures and guidelines for conducting audits of Netradyne's information security management system. The purpose of the policy is to ensure the objectivity, integrity, and effectiveness of the audit process in assessing the organization's compliance with relevant security standards, controls, and policies.

Here are some key elements that build an independent audit/assessment policy:

- **Scope:** Define the scope of the audit, specifying the systems, processes, and locations that will be assessed as part of the audit.
- **Audit Objectives:** Clearly state the objectives of the audit, which may include evaluating the effectiveness of Netradyne's system controls, identifying security vulnerabilities or gaps, assessing compliance with relevant standards or regulations, and providing recommendations for improvement.
- **Roles and Responsibilities:** Define the roles and responsibilities of all parties involved, including the organization being audited, the independent auditor, and any internal stakeholders who may participate in the audit process.
- **Audit Criteria:** Specify the criteria against which the audit will be conducted, such as industry standards (e.g., ISO 27001), legal and regulatory requirements, internal security policies, and best practices.
- **Audit Process:** Describe the steps and activities involved in the audit process, including the planning phase, data collection and analysis, on-site visits or interviews, documentation review, and the reporting process.
- **Audit Independence:** Emphasize the need for independence and impartiality in the audit process. Define the criteria that ensure the auditor's independence from Netradyne, including the avoidance of conflicts of interest and any restrictions on providing consulting or other services to Netradyne.
- **Reporting and Communication:** Outline the requirements for audit reports, including the format, content, and timelines for delivering the audit findings. Define how the audit results will be communicated to relevant stakeholders, such as management, internal teams, and regulatory authorities.
- **Follow-Up Actions:** Define the process for addressing audit findings, including the development of corrective action plans, timelines for implementation, and any required follow-up audits or reviews to verify the effectiveness of corrective measures.
- **Confidentiality and Security:** Specify the requirements for maintaining the confidentiality and security of audit information and data collected during the audit process.
- **Continuous Improvement:** Highlight Netradyne's commitment to continuous improvement by using audit findings to drive enhancements to the existing ISMS and security controls.

It's important to note that the specific content and requirements of an independent audit policy may vary depending on the Netradyne's industry, regulatory environment, and internal security objectives. This policy should be reviewed and aligned to address Netradyne's unique needs while adhering to recognized audit standards and best practices.

## 4.17 Access Privilege review policy

### 4.17.1 Separation of Duties

There are NETRADYNE functions that are separated physically and logically in order to reduce the possibility of an individual taking advantage of that function, or to inhibit collusion and conspiracy to defraud or misappropriate resources. Basic internal control principles require that the same person should not initiate, authorize, and enter a transaction.

### 4.17.2 Least Privilege

Individuals are given only a level of authority and granted only those privileges and accesses necessary to successfully accomplish their assigned duties. Individuals are not allowed either functional or physical access to controlled areas or operations unless required by their duties and requested by their supervisor.

### 4.17.3 Individual Accountability

The addition, deletion, and modification of user IDs, credentials, and other identifier objects is controlled by the NETRADYNE IT Operations and Security team such that each user's or service account’s identity is uniquely and positively established at all times. Individual access to, and activity in, a specific area or function is controlled and open to scrutiny. Individual access to controlled areas will not be allowed without establishing identity, authenticating that identity, and authorization based upon that identity. These activities are centrally logged for audit purposes.

### 4.17.4 Application Access

NETRADYNE’s security policies are defined around the principle of “least privilege” and “need-to know”. There are a limited set of NETRADYNE employees that will have physical and logical access to a given system, and this is true for both production customer systems, as well as QA and Engineering systems. This list of employees is defined and controlled throughout the customer relationship period. Access lists are reviewed quarterly to ensure that NETRADYNE employees have only the necessary access to do their job.

### 4.17.5 Corporate System Access

Providing access to corporate systems is similar to application access - based on the principle of “least privilege” and “need to know”. Additionally, employees are given access to systems based on managerial request and approval, NETRADYNE IT Operations and Security group approval, business/system owner approval, and in some cases, approval from HR. Access levels are reviewed on a quarterly basis to ensure accuracy and validity and these reviews are captured in the NETRADYNE IT Operations and Security group’s ticketing system.

### 4.17.6 Logical Access Control

Logical access controls are placed on sensitive systems, information and critical applications used by NETRADYNE to perform information processing considered critical to NETRADYNE. All NETRADYNE systems have the ability to accommodate and enforce logical access restrictions. Control is exercised according to the principle of least privilege. System capability restrictions are usually stated in terms of “No access”, “Read”, “Create”, “Modify”, “Delete”, and “Protected”.

Accounts with elevated privileges, such as domain administrator and super-user accounts, are scrutinized and closely controlled and monitored to ensure such authorization is absolutely required to conduct an employee’s role and responsibilities. All elevated accounts are reviewed on a quarterly basis.

## 4.18 Customer Data Protection

### 4.18.1 General Information Protection policy

Policies and procedures are required to protect the security of sensitive information accessed by employees. This sensitive information includes, but is not limited to, marketing; legal and accounting methods; software system design; computer programs; software; hardware; policies; plans; procedures; strategies and techniques; information concerning the company's earnings and methods for doing business; research and development projects; plans and results; trade secrets; technical specifications; custom programs and software; the Netradyne's and addresses of the company's employees, vendors, suppliers, clients, and customers; lists of clients and customers; all data and information associated with individuals who were or are our customers, including their identity; account information, pricing, credit and financial information; and any other data or information relating to the operations and business of the company which is not generally known by or readily accessible to the public.

Employees do not discuss or share any sensitive information regarding our company and/or its clients, customers, or employees with anyone who does not have a legitimate need to know such information. Employees do not discuss sensitive information in the public areas of our facilities (e.g. the elevators, reception area, and hallways) or in public conveyances, restaurants, or retail establishments where conversations may be overheard.

Employees do not attempt to gain access to sensitive information other than that which is required for their job functions.

## 4.19 Third Party Service Providers and Vendors

The provisions outlined in this document are applicable to the operations and activities on behalf of NETRADYNE of both service organizations and contract personnel, regardless of whether the service is provided on or off NETRADYNE premises.

Third party service providers (TPSP) offer a necessary adjunct to NETRADYNE's capabilities. By providing services or specialized support utilizing contract resources over short periods of time, NETRADYNE can achieve both operating and financial efficiencies that would otherwise require long term commitments or capital investments.

Relationships with outside service personnel and organizations, however, present unique legal and operational situations that are addressed cautiously in order to successfully fulfil NETRADYNE's objectives. Because of the sensitive nature of NETRADYNE operations and the data it processes, security is a foremost consideration in the establishment and maintenance of these relationships.

It is the intent of the policies in this section to ensure that outside Information Technology services provided to the NETRADYNE do not jeopardize the integrity of the NETRADYNE's security program.

### 4.19.1 Third Party Service Provider review

As part of this program, we ensure any third parties don't have access to the production environment but provide services that are required for information processing. This due diligence includes:

We review past public incidents and to ensure these activities are aligned to NETRADYNE's business objectives and commitments to its own customers.

We perform "reputational due diligence" to further mitigate risk by checking references, conducting internet searches to uncover reports of prior security incidents, and, to reveal and existing relationships with companies that are recognized industry leaders in information security.

We review due diligence items as well. This may occur sooner if a change merits an out of cycle review, such as an acquisition, relocation, or data breach. More details can be referred to below document (s)

Third Party Risk Management.pdf

*Netradyne TPRM Preliminary Assessment Accelerator_v1.1.xlsx*

## 4.20 Risk Management Policy

Netradyne Risk Management Policy outlines the principles, guidelines, and responsibilities for managing risks related to information security within our organization. It is aligned with the requirements of ISO 27001.

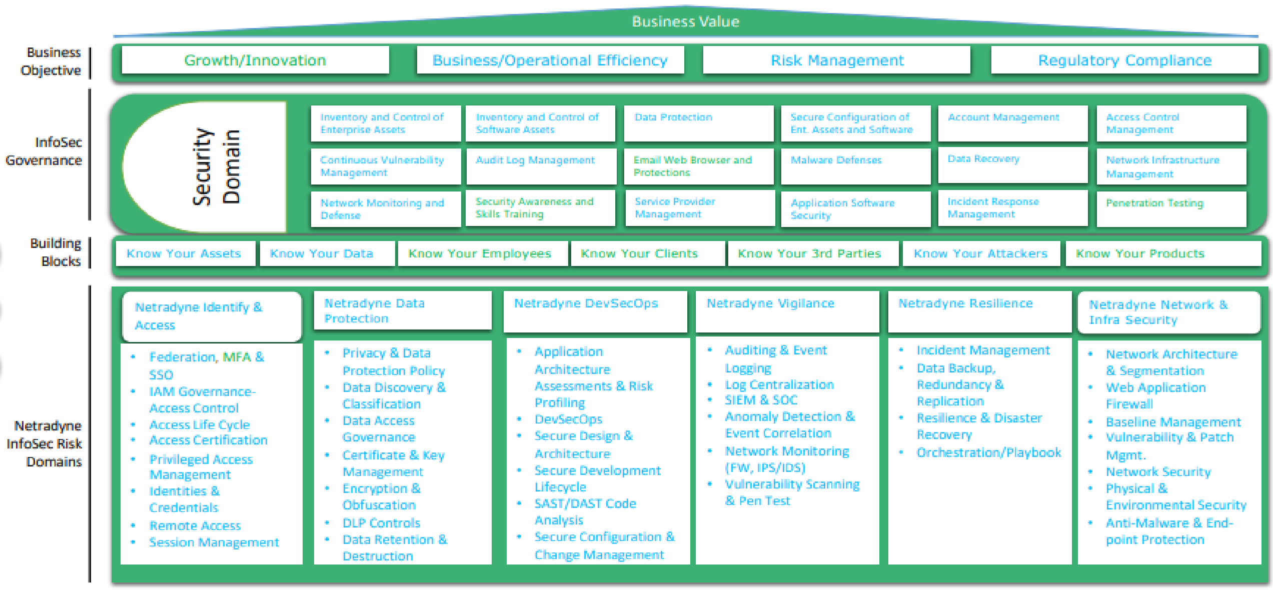
### 4.20.1 Objective

The objective of this policy is to define a Risk Governance Framework, establish a systematic and proactive approach to identify, assess, and manage enterprise-wide security risks to protect our organization's assets, including information, systems, and processes.

### 4.20.2 Scope

This policy applies to all employees, contractors, and third-party personnel who have access to the organization's information assets, regardless of the location or the form in which the information is stored or transmitted.

### 4.20.3 Risk Governance Framework



Business Value
Business Objective
Growth/Innovation
Business/Operational Efficiency
Risk Management
Regulatory Compliance
InfoSec Governance
Security Domain
Inventory and Control of Enterprise Assets
Inventory and Control of Software Assets
Data Protection
Secure Configuration of Ent. Assets and Software
Account Management
Access Control Management
Continuous Vulnerability Management
Audit Log Management
Email Web Browser and Protections
Malware Defenses
Data Recovery
Network Infrastructure Management
Network Monitoring and Defense
Security Awareness and Skills Training
Service Provider Management
Application Software Security
Incident Response Management
Penetration Testing
Building Blocks
Know Your Assets
Know Your Data
Know Your Employees
Know Your Clients
Know Your 3rd Parties
Know Your Attackers
Know Your Products
Netradyne InfoSec Risk Domains
Netradyne Identify & Access
Federation, MFA & SSO
IAM Governance-Access Control
Access Life Cycle
Access Certification
Privileged Access Management
Identities & Credentials
Remote Access
Session Management
Netradyne Data Protection
Privacy & Data Protection Policy
Data Discovery & Classification
Data Access Governance
Certificate & Key Management
Encryption & Obfuscation
DLP Controls
Data Retention & Destruction
Netradyne DevSecOps
Application Architecture Assessments & Risk Profiling
DevSecOps
Secure Design & Architecture
Secure Development Lifecycle
SAST/DAST Code Analysis
Secure Configuration & Change Management
Netradyne Vigilance
Auditing & Event Logging
Log Centralization
SIEM & SOC
Anomaly Detection & Event Correlation
Network Monitoring (FW, IPS/IDS)
Vulnerability Scanning & Pen Test
Netradyne Resilience
Incident Management
Data Backup, Redundancy & Replication
Resilience & Disaster Recovery
Orchestration/Playbook
Netradyne Network & Infra Security
Network Architecture & Segmentation
Web Application Firewall
Baseline Management
Vulnerability & Patch Mgmt.
Network Security
Physical & Environmental Security
Anti-Malware & End-point Protection

### 4.20.4 Risk Management Framework

#### 4.20.4.1 Risk Identification

- All assets within the organization, including information systems, processes, and data, shall be identified, and documented.
- Threats and vulnerabilities associated with each asset shall be identified and assessed.
- A risk register needs to be maintained which list our all the identified risk with its threat landscapes, risk owners, risk remediation strategies with provision for tracking and closure. You may refer the risk register for more details:
  - InfoSec_RiskRegisterOverview_Mar2023.pptx
  - ISMS_RiskRegister_MASTER.xlsx

#### 4.20.4.2 Risk Assessment

NETRADYNE uses an on-going security risk assessment process to discover, correct and prevent security problems. The risk assessment is an integral part of managing risk at NETRADYNE and is designed to provide appropriate levels of security for information systems.

The risk assessment helps NETRADYNE determine an acceptable level of risk and the resulting security requirements for each system. NETRADYNE then devises, implements, and monitors a set of security measures to address the level of identified risk.

- Risk assessments shall be conducted regularly or when significant changes occur.
- Risk assessments shall consider the likelihood and impact of potential risks to determine the level of risk exposure.

NETRADYNE's risk assessment occurs in three phases:

- System Documentation Phase
- Risk Determination Phase
- Safeguard Determination Phase

The risk assessment report:

- Summarizes the system architecture and components, and its overall level of security.
- Includes a list of threats and vulnerabilities, the system's current security controls, and its risk levels.
- Recommends safeguards and describes the expected level of risk that would remain if these safeguards were put in place.
- Shows where NETRADYNE needs to concentrate its remedial work.
- Provides input into NETRADYNE's disaster recovery and business continuity plan.

For a new system the risk assessment is typically conducted at the beginning of the System Development Life Cycle (SDLC). For an existing system, risk assessments may be conducted on a regular basis throughout the SDLC and/or on an ad-hoc basis in response to specific events such as when major modifications are made to the system's environment or in response to a security incident or audit. At a minimum, risk assessments shall be completed annually for administrative, physical, and technical security controls. In the case of the daily security vulnerability scans, the results are reviewed daily via email alert. Any new items are reviewed, and an immediate risk assessment occurs for any critical severity issues.

Risk rankings are based on industry best practices (OWASP Risk Rating Methodology, NIST SP 800-30 or ISO 27005, CVSS etc.) as well as potential impact. Vulnerabilities are considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise at enterprise-wide level if not addressed. Critical system includes security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit customer data or any sensitive data.

Risk Assessment team consists of the member(s) of the InfoSec Team.

#### 4.20.4.3 Risk Treatment

Risk should be prioritize based on asset values and likely impact

- Appropriate risk treatment options shall be selected based on the results of risk assessments.
- Risk treatment options may include risk avoidance, risk transfer, risk mitigation, or acceptance.

#### 4.20.4.4 Risk Acceptance

- Risks that are not treated or mitigated to an acceptable level shall be formally accepted by management.
- The acceptance of risks shall be based on a thorough understanding of the potential impacts and the organization's risk appetite.

#### 4.20.4.5 Risk Monitoring and Review

- The effectiveness of risk treatments shall be monitored and reviewed on a regular basis.
- Risk assessments shall be updated to reflect changes in the organization's risk profile through established risk register.

#### 4.20.5 Roles and Responsibilities in risk management

##### 4.20.5.1 Senior Management

- Senior management shall provide leadership and support for the risk management process.
- They shall ensure that appropriate resources are allocated for risk management activities.

##### 4.20.5.2 Risk Owner

- Each identified risk shall have a designated risk owner responsible for its management, accountability, and treatment.
- Risk owners shall develop and implement risk treatment plans or delegate it to risk custodian(s) and monitor the effectiveness of controls.

##### 4.20.5.3 InfoSec Personnel-Security Risk & Compliance

- The designated Information Security Personnel shall oversee the risk management process.
- They shall ensure that risk assessments are conducted, documented, and reviewed as required.

#### 4.20.6 Documentation and Reporting

- All risk assessments, treatment plans, and risk acceptance decisions shall be documented and captured in risk register.
- Regular reports on the organization's risk profile, risk treatment progress, and emerging risks shall be provided to senior management.

#### 4.20.7 Training and Awareness

Employees, contractors, and third-party personnel shall receive appropriate training and awareness programs on risk management and their roles in managing risks.

#### 4.20.8 Compliance

- Compliance with this policy and associated risk management procedures is mandatory for all personnel.
- Non-compliance may result in disciplinary action.

#### 4.20.9 Review and Update

This Risk Management Policy shall be reviewed and updated periodically to ensure its continued relevance and effectiveness.

### 4.21 Cardholder Data Environment Inventory and Access

NETRADYNE doesn’t have a card data environment.

### 4.22 Secure Software Development (SDLC) Policy/DevSecOps

NETRADYNE software development strategies focus on security industry best practices and aligning to SDLC best practises. The most basic goal of a comprehensive corporate security program is to prevent the unauthorized disclosure, modification, or use of information. This goal is addressed through the implementation of effective security controls at every interface point within an information management system

#### 4.22.1 Separation in development and production duties.

##### 4.22.1.1 Software Development:

The software development team develops software on in dedicated software development environments. They define technical architecture, and audits application security through secure code reviews. No access to production environments is defined or ever allowed.

#### 4.22.1.2 Quality Assurance:

The Quality Assurance group does not have production access outside of standard web user access for automated and regression testing.

#### 4.22.1.3 Product Management:

Product Management focuses on product business logic definition, custom features, user interface, technical design, and client usage analysis, and does not have access to production environments.

### 4.22.2 Change Management

Each software release goes through a formal software development lifecycle. A security code review is conducted prior to every release by architectural leads. This review includes a regression checklist to validate any potential impact and risk. Any modification to the core components requires lead architect validation and approval. All changes are promoted through the various environments via the change management policy defined in this document.

### 4.22.3 Risk Management in DevSecOps

Issues discovered as part of the secure development process are resolved prior to promotion to production. In some cases, the risk management policy defined in this document is used to rate, categorize, and prioritize remediation activities based on industry best practices and guidelines, such as those from OWASP, SCA.

### 4.22.4 Data Integrity

Attacks against "Integrity" are more widely referred to as "hacking." Criminal hacking consists of using weaknesses in a system to overcome security barriers or turning software features into vulnerabilities. Some hackers are content merely to signal their visit to the systems they violated, others vandalize web pages, and others will attempt to control all operations of a targeted system by gaining root access and executing arbitrary commands. Failure to protect the "integrity" of operating systems, services and data provided to an end user could be legally or financially disastrous. NETRADYNE leverages various frameworks and best practises, including OWASP, to ensure common vulnerabilities and attack surfaces are understood and guarded against.

### 4.22.5 Data Confidentiality

Maintaining data "Confidentiality" is an important element in all areas of information technology and application development. Confidentiality concerns may involve employee data, personal customer information, proprietary strategic information, credit card compliance, and more. The effective use of strong authentication and encryption are the basis for sound policies on the capture, gathering, analysis and storage of information with different levels of sensitivity. Vulnerabilities in this category can be mitigated through the installation of appropriate patches, or through the re-configuration of access control lists or firewall rule bases.

### 4.22.6 Data Storage

NETRADYNE conducts removal of all sensitive data from databases and storage using automation processes across production and development environments. These processes both detect and prevent the storage of this data. All BLOB data stored within the NETRADYNE system is encrypted in S3, Tenant PII Data is encrypted in database PostgreSQL using AWS KMS for key management.

### 4.22.7 Web Application Security Services

Secure software development practices focus on alignment with the Open Web Application Security Project (OWASP) to ensure an industry accepted baseline of security measures are instituted as part of the software development methodology.

#### 4.22.7.1 Authentication Services:

The NETRADYNE application is designed to prevent malicious activities by way of a hierarchical account management, extensive roles, and separation of client sensitive data. Additionally, at no time are test, custom, or default credentials used in production.

#### 4.22.7.2 Logging:

Extensive logging is enabled for both diagnostic and security functionality.

#### 4.22.7.3 Cookies:

The use of cookies prevents the storage of any sensitive information outside of session information.

#### 4.22.7.4 Server and transport security controls:

Industry controls are in place through server and transport layer authentication and transmission mechanisms, including certificates, HTTPS/TLS (SSL encryption), and advanced encryption security (AES). All communications to customers occur in a secure HTTPS encrypted request. Any non-secure HTTP request is redirected to HTTPS.

#### 4.22.7.5 Cross-Site Scripting Security:

Inputs and output data streams are wrapped through a XSS cleanse method to avoid scripting attacks.

#### 4.22.7.6 Cross-site forgery (CSRF):

We don’t use CSRF. This was also validated by the pentest results.

#### 4.22.7.7 Scope injection:

NETRADYNE utilizes named queries in java code which utilizes parameter binding to set the data. The JDBC driver will escape this data appropriately before the queries are executed ensuring data integrity.

#### 4.22.7.8 SQL Injection:

SQL injection validation routines are used to prevent malicious SQL from being run. This includes the following SQL reserved words: select, update, delete, insert, drop, alter table, and create. Examples of characters that can be used in attacks are > < ( ) [ ] ' " ; : - / \ NULL, etc. The NETRADYNE application sanitizes these characters via input validation. Input validation occurs before the user-supplied data is used by the application or stored in the database.

Non-alphanumeric characters are parsed (except @, dash, period, underscore, single quote, and space) to prevent them from being passed into SQL or from being displayed and thus "executed”.

#### 4.22.7.9 Buffer Overflows:

NETRADYNE software built on safe languages which don’t expose this vulnerability.

#### 4.22.7.10 Error Handling:

Detailed error messages, such as stack traces and debug information, are never presented to the user. Generic error messages are used instead including HTTP status response codes (i.e. 404 or 500 Internal Server error).

#### 4.22.7.11 Server Patches:

All production servers are patched every 6 months.

#### 4.22.7.12 Cryptography:

All cryptographic functions occur within the database environment using AWS KMS Encryption.

#### 4.22.7.13 Broken Authentication and Session Management:

We use access tokens which are stored in local storage. These tokens are issued by us. These tokens are refreshed every 3 hours. We can optionally expire them manually as well. We clear them out at log off. We do session tracking and logout users after 7 days.

### 4.22.8 Secure Software Development Training

Secure software development practices focus on alignment with the Open Web Application Security Project (OWASP) to ensure an industry accepted baseline of security practices and measures are met and instituted as part of the software development methodology. As part of regular secure code reviews, training opportunities arise in which the software development team reviews problematic code to ensure an acceptable level of security is maintained and to filter out insecure coding behaviours. These code reviews are required for all members of the software development team.

Additionally, as part of the company static application security testing, infer is used to review code as part of the software development lifecycle and prior to promotion of code to the production environment. Software developers are alerted to security issues in their code as a result.

## 4.23 Physical Controls

The objective of the physical controls implemented at NETRADYNE is to protect and preserve NETRADYNE resources including intellectual property, physical assets, human resources, and other sensitive company information.

Physical security measures are implemented with consideration for operational requirements and employed in conjunction with mutually supporting measures in the areas of employees, hardware, data, software, documentation, communications, and procedural security.

Physical security measures have been designed and implemented with consideration for the relative critical nature of the information processing resource to be protected. This is defined as the relative measure of impact on NETRADYNE by inadvertent or deliberate disclosure (i.e., loss of privacy and/or confidentiality), alteration, destruction, or non-availability of that resource.

Physical security measures are considered an integral part, but only a part, of the security environment for a resource. Inclusion of proper technical, administrative, and logical controls, as well as limitations on the privileges extended to gain access to specific devices, mitigate the need for physical security controls.

### 4.23.1 Production and Development Datacentres

The NETRADYNE production datacentre is physically located at an Amazon Web Services (AWS) facility known as US West, N. California (us-west-1).

Both are protected from environmental and security threats through the use of numerous technical, administrative, and physical security controls. For high availability, included are redundant uninterruptable power supplies and diesel power generators, fire and smoke detection and suppression systems, redundant ventilation, and air conditioning, and more. All systems undergo frequent and regular preventative maintenance.

From a security perspective, both locations are monitored by CCTV and a team of security guards are deployed at the entrance and throughout the facility 24x7, and regular patrols are conducted throughout the premises. Access to the building is controlled by security key cards, biometric scanners, and a man trap. This facility is ISO 27001 compliant.

### 4.23.2 Netradyne Office(s) - Corporate and Development

The corporate offices are protected through the use of numerous physical, administrative, and technical controls. Physical controls include uninterruptable power supplies, fire and smoke detection and suppression systems, and air conditioning. All facility systems undergo preventative maintenance biannually.

Security guards are deployed in the lobby of the building 24x7 and regular patrols are conducted throughout the premises and on all floors. The facility is located in a business hub and includes extensive security controls, including CCTV, motion sensing and alerting camera systems, and metal detectors are used at the entrance. Lobby doors are locked after hours and access is controlled through security key cards. Access to the elevators is also controlled by security key cards after regular hours. Guests are always required to be registered in advance of their visit, to check in at the front desk, and present photo ID.

### 4.23.3 Levels of Access Authority

Specific levels of access authority are established for each controlled area. There are two general levels of access authority.

#### 4.23.3.1 Permanent Access

Permanent employees who have responsibility for functions performed in a controlled area may be granted permanent access privileges to that area. Permanent access privileges will not be granted to employees who do not work in controlled areas or do not enter controlled areas on a frequent basis. Temporary employees who function in a position in a controlled area more than 30 days may be granted permanent access privileges if requested by the manager with administrative responsibility for that temporary employee.

#### 4.23.3.2 Temporary Access

Permanent employees who are not authorized to access a controlled area will only be granted temporary access privileges. Temporary employees who will function in a position in a controlled area for less than 30 days are granted temporary access privileges to that area. In addition, only temporary access privileges are granted to short-term non-employees, such as visitors, vendors, support-employees, and maintenance crews, and are accompanied by their company sponsor at all times. Any such requested are submitted through the NETRADYNE IT Operations and Security group’s ticketing system for authorization and audit purposes.

### 4.23.4 Physical Security Awareness

As part of annual security awareness training, persons conducting work for NETRADYNE are made aware of their role in observing and enforcing physical security policies and procedures and reinforcing them when interacting with others in the workplace.

### 4.23.5 General facilities and work area security

- Workstations are locked at the operating system level whenever unattended to prevent unauthorized access to workstations and the company network.
- Printers and fax machines are cleared of confidential information both during work hours and after hours. Printouts are picked up promptly.
- Doors with external access are never be propped open unless supervised maintenance work requiring unobstructed room access is underway.
- Doors marked for Emergency Use are not used for non-emergency purposes.
- Conference room white boards are cleared of any confidential information at the close of the meeting.
- In conference rooms with externally facing windows, care is taken when projecting confidential information on screens or walls. In these cases, blinds are pulled down to ensure that viewing from outside the building is not possible.
- All cabinets, drawers, credenzas, etc. containing confidential information are locked after hours of if left unattended over a period, such as during a meeting or lunch.

- Keys to file cabinets, credenzas, etc. that contain Confidential information are to be possessed and secured by authorized personnel and not "hidden" in the work area.
- All paper trash is to be properly disposed of or shredded. Shred bins are placed throughout office locations to facilitate secured disposal of confidential documents.
- Video cameras may be installed to record activity at office entry/exit points and doorways that permit access to interior secured rooms. Access to video recording data is restricted to authorized personnel and is used only for the purposes of security enforcement and monitoring.
- Lost security key cards are reported immediately to the NETRADYNE IT Operations and Security group for immediate deactivation. Security key cards are issued on an individual basis and are not to be shared or loaned.

### 4.23.6 General facilities and work area off-hours security

Department filing cabinets and rooms or offices containing confidential information are locked after hours. Desks are cleared of all confidential information, including, but not limited to, account or credit card information, internal diagrams, memos, database structures, financial information, and personnel information. Any persons conducting work for NETRADYNE do not leave sensitive or confidential information on their own or on other people's desks, or general work areas.

### 4.23.7 Security Key Cards

The NETRADYNE offices use security key/access cards issued to each employee by the Admin/building management. Security key cards are not loaned to or shared with anyone including other NETRADYNE employees. All lost, stolen, or misplaced security key cards are reported immediately to the NETRADYNE Administration Team. All security key cards or fobs that are found are to be immediately returned to the NETRADYNE Administration Helpdesk. For person exiting employment or contractual work for NETRADYNE, security key cards are returned to Human Resources during an exit interview.

### 4.23.8 Visitor policy

All visitors are escorted when arriving at and during their visit to a NETRADYNE office and are required to be registered prior to their arrival. They are required to present photo ID and sign into the guest book with the building management.

- Date and time of visit
- Visitor's full Netradyne
- Company, they represent.
- Whom they are visiting

While visiting a NETRADYNE office, visitors are escorted at all times by a NETRADYNE employee and wear an identification tag. These tags are provided by the building management security team.

### 4.23.9 Wiring closets

Access to wiring closets is restricted to authorized NETRADYNE employees and doors are locked when not occupied. Access is not possible from the exterior of the facilities.

# 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 Management Process. Any deviation in remediation/deployment timeline shall be approved as an exception with proper justifications and recorded in Netradyne Risk Register.

Exceptions may be granted in cases where security risks 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 or Mitigation is practically not possible within the prescribed duration To request a security exception, contact the InfoSec team. Below are the examples of exceptions:

- Patching on Production systems like GPU machines hosted in our data centre may require complex testing and installation procedures
- Deviations from normal patch schedules shall require authorization from IT & InfoSec Head
- Inability to remediate a vulnerability due to lack of solution
- Patch/Remediation are not feasible with application and business requirements
- Special access permission needed on valid reasons
- Business requirements are on conflict with Netradyne Information Security Policy and exception needed

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

# 7 Terms/Acronyms

| Term/Acronym | Definition |
|---|---|
| ***Resources*** | include computing, networking, communications, application, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services. |
| ***Production Environment*** | This is commonly used for any live environment in Netradyne e.g. SaaS Hosting, Netradyne Products used by our partners, SaaS products used by Netradyne, Netradyne Internal System Managed by IT Team etc. *(In future Patch & Vulnerability Management Procedure document will be more refined and dedicated procedures will be added to different type of production environment(s) as mentioned above.)* |
| ***Patch*** | is a software update comprised of code inserted (i.e., patched) into an executable program code. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited, to the following:<br>• Upgrading software<br>• Fixing a software bug<br>• Installing new drivers<br>• Addressing security vulnerabilities<br>• Addressing software stability issues |
| ***Remediation*** | is an effort that resolves or mitigates a discovered vulnerability. |
| ***Vulnerability*** | is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. |
| ***Vulnerability management*** | is the practice of identifying, classifying, remediating, and mitigating vulnerabilities. |
| ***DL*** | Distribution List |
| ***ND*** | Netradyne |

# 8 References

## 8.1 Templates

*NetradyneDocumentationTemplate_v1.0.dotx*
*Netradyne TPRM Preliminary Assessment Accelerator_v1.1.xlsx*
ISMS_RiskRegister_MASTER.xlsx

## 8.2 Policies

*Personal_Data_Protection_Policy.pdf*
*Acceptable Usage Policy.pdf*
*NetradyneOpen-SourceSecurityPolicy.pdf*
*Netradyne Information Technology Policy.pdf*
*Cryptography Standards Policy.pdf*

## 8.3 Process/Procedures

*Netradyne Vulnerability & Patch Management Process.pdf*
*NETRADYNE BUSINESS CONTINUITY PLAN.pdf*
*NETRADYNE DISASTER RECOVERY PROCESS.pdf*
*Netradyne Information Security Exception Process.pdf*
*Netradyne Antimalware Crowdstrike Procedure.pdf*
*Netradyne SOP Malware Analysis.pdf*
*NetradyneSecurityIncidentResponsePlan.pdf*
*Third Party Risk Management.pdf*

## 8.4 Standards

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

## 8.5 Miscellaneous

InfoSec_RiskRegisterOverview_Mar2023.pptx

# 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 |