

Internal and Confidential

Netradyne Information Technology Policy & Procedure

v3.3

Table of Contents

[Netradyne Information Technology Policy & Procedure 0](#_Toc158726781)

[Document Control 3](#_Toc158726782)

[1 Purpose 4](#_Toc158726783)

[2 Scope 4](#_Toc158726784)

[3 Roles and Responsibilities 4](#_Toc158726785)

[4 Procedure 5](#_Toc158726786)

[4.1 IT Network Diagram 5](#_Toc158726787)

[4.2 IT Hardware & Software Policy 6](#_Toc158726788)

[4.2.1 IT Purchase Flow 7](#_Toc158726790)

[4.2.2 IT Hardware Policy 7](#_Toc158726791)

[4.2.3 IT Software Policy 7](#_Toc158726792)

[4.2.4 Obtaining Open-Source Software 8](#_Toc158726793)

[4.2.5 System Hardening and Baseline 8](#_Toc158726794)

[4.3 Inventory & Control of Assets 9](#_Toc158726795)

[4.3.1 Hardware Assets 9](#_Toc158726796)

[4.3.2 Software Assets 9](#_Toc158726797)

[4.4 Acceptable Use of IT Policy 10](#_Toc158726798)

[4.4.1 Computer Access Control 10](#_Toc158726799)

[4.4.2 Internet and Email Conditions of Use 10](#_Toc158726800)

[4.4.3 Actions upon Termination of Contract (IT Assets Return) 11](#_Toc158726801)

[4.4.4 Disposal of Media Policy and Procedures 11](#_Toc158726802)

[4.5 Vendor Management Policy 12](#_Toc158726803)

[4.5.1 Vendor Due Diligence 12](#_Toc158726804)

[4.5.2 Procurement of IT assets\accessories 12](#_Toc158726806)

[4.6 Employee Onboarding & Offboarding Policy 12](#_Toc158726807)

[4.6.1 Onboarding Policy 12](#_Toc158726808)

[4.6.2 Off-boarding Policy 13](#_Toc158726809)

[4.7 User Access Management 13](#_Toc158726811)

[4.8 Secure Login Policy 14](#_Toc158726812)

[4.9 Anti-Malware Policy 14](#_Toc158726813)

[4.10 Patch Management Policy 15](#_Toc158726815)

[5 Password Management Policy 16](#_Toc158726817)

[5.1 Mobile Device & Teleworker Policy 16](#_Toc158726818)

[5.1.1 Mobile device policy 16](#_Toc158726819)

[5.1.2 Teleworking 17](#_Toc158726820)

[5.2 Policy for IT Asset Offsite Use 17](#_Toc158726821)

[5.3 Clear Desk & Clear Screen Policy 17](#_Toc158726822)

[5.4 Printer Policy 17](#_Toc158726823)

[5.5 Logging and Monitoring 18](#_Toc158726824)

[5.6 Backups and Business continuity plan 18](#_Toc158726825)

[6 Conduct 18](#_Toc158726827)

[7 Exception 19](#_Toc158726828)

[8 Terms/Acronyms 19](#_Toc158726830)

[9 References 19](#_Toc158726831)

[9.1 Templates 19](#_Toc158726832)

[9.2 Policies 19](#_Toc158726834)

[9.3 Process/Procedures 19](#_Toc158726835)

[10 Appendix A: Document RACI Matrix 20](#_Toc158726842)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDITPP2021001 |
| **Document Name** | Netradyne Information Technology Policy and Procedure |
| **Document Status** | Released |
| **Document Released Date** | 13-JAN-2021 |
| **Document Author** | Chethan Gangaraju |
| **Document Content Contributors** | Blaize Mathews, Sudhansu Kumar, Vijaykumar Dalal |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Chethan Gangaraju |
| **Document Version** | v3.3 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 13-Jan-2021 | New IT Policy Document | Chethan Gangaraju |
| v2.0 | 07-Jan-2022 | Change in template format, Added Teleworking Policy, Patch Management Policy, Printer Policy. Content refinement for other sections | VijayKumar Dalal, Sudhansu Kumar |
| v3.0 | 21-Jun-2022 | Changes to UAM process, Asset Inventory, IT purchase policy | Vijaykumar Dalal |
| v3.1 | 15-May-2023 | Changes to Network Architecture diagram, changes to IT software policy, changes inventory and control of assets | Chethan Gangaraju |
| v.3.2 | 02-Feb-2024 | Refined to include more controls on data privacy/Data protection | Chethan Gangaraju |
| V3.3 | 29-Jan-2025 | Annual review with no change | Chethan Gangaraju |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 13-Jan-2021 | Saravanan Sankaran | Senior Director, Infosec & IT | Approved |
| 07-Jan-2022 | Kavitha Shetty | Sr. Program Manager | Approved |
| 22-Jun-2022 | Kavitha Shetty | Sr. Program Manager | Approved |
| 19-May-2023 | Saravanan Sankaran | Senior Director, Infosec & IT | Approved |
| 05-Feb-2024 | Saravanan Sankaran | Senior Director, Infosec & IT | Approved |
| 31-Jan-2025 | Saravanan Sankaran | Senior Director, Infosec & IT | Approved |

**Distribution of Final Document**

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

# Purpose

The Netradyne IT Policy and Procedure Manual contains policies and procedures related to the selection and use of IT within the organization, which must be followed by all the staff. This manual also includes guidelines for Netradyne to administer these policies and outlines the proper procedures to be followed.

Netradyne will safeguard all sensitive data which might include PII/PHI by keeping all IT policies up-to-date and relevant. Netradyne reserves the right to modify and amend certain sections of the policies and procedures or add new procedures as needed.

We encourage any suggestions, recommendations, or feedback on the policies and procedures specified in this manual to promote continuous improvement and ensure compliance with applicable privacy laws and regulations.

# Scope

The scope of these policies and procedures apply to all Netradyne employees and are designed to ensure appropriate access to and usage of IT resources, while preventing unauthorized access and misuse of such resources.

The objective of this policy is to establish a framework that governs the use of IT resources within Netradyne, ensuring compliance with applicable privacy laws and regulations, and protecting the security and confidentiality of sensitive data, including PII/PHI by adhering to these policies and procedures.

Netradyne employees can help maintain the integrity, availability, and confidentiality of the organization's IT resources.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Procedure

The Netradyne Information Technology (IT) Policy establishes guidelines, rules, and regulations for the proper usage and maintenance of IT assets, ensuring their ethical and acceptable use, and safeguarding the health, safety, and security of data, products, facilities, and employees.

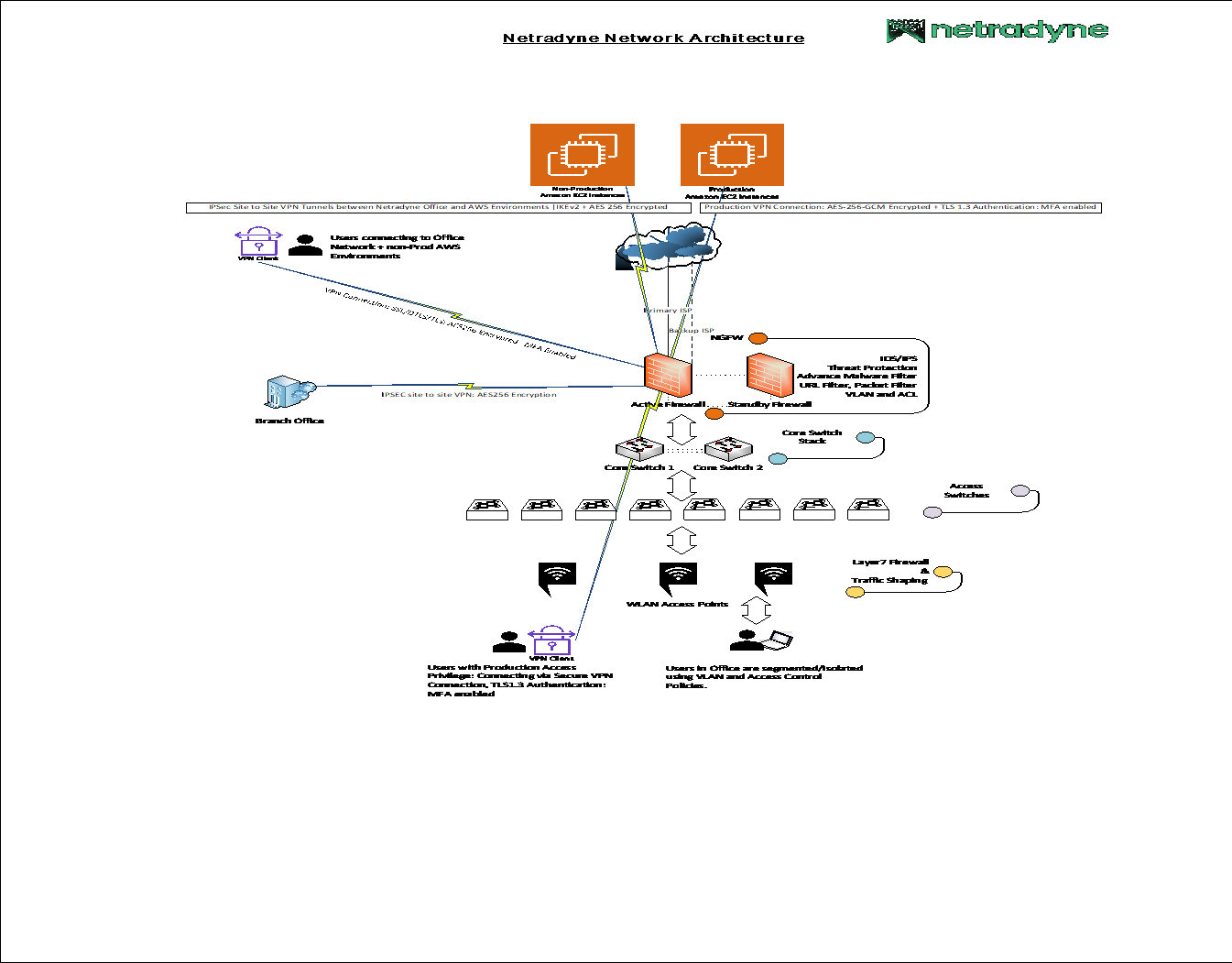
This policy also outlines guidelines for the purchase, compliance, IT support, and grievance redressal of employees, including the use of IT assets and services for daily business operations. Compliance with this policy is mandatory for all Netradyne employees, and it is crucial to ensuring the confidentiality, integrity, and availability of sensitive data, PII/PHI. Proper adherence to this policy will help mitigate risks associated with unauthorized access, use, or disclosure of IT assets, and help maintain the integrity and reputation of the organization.

## IT Network Diagram

IT networks are a crucial component for modern businesses and organizations, providing a foundation for connecting computers, servers, and devices to facilitate communication, data sharing, and collaboration. At Netradyne, our IT networks are tailored to meet the specific requirements of our organization. Our offices are equipped with Wi-Fi and LAN, and to enhance uptime and availability, we utilize dual internet service providers (ISPs) to ensure redundancy and failover capabilities.

Our network design allows legitimate traffic to flow through the appropriate zones, segments, and resources, while unwanted traffic is detected and dropped. We implement firewalls, Virtual Local Area Networks (VLANs), and/or Access Control Lists (ACLs) to achieve this. We have network segregation in place to separate production and non-production networks, and firewall policies and ACLs are enabled to ensure that only authorized users have access.  
  
Netradyne users access non-production environments through Cisco AnyConnect VPN and production environments through OpenVPN, both of which are enabled with multi-factor authentication (MFA). Access to network devices and services is restricted to authorized IT engineers in line with our Access Control Policy.

We enable logging on all networking devices, including log configuration changes, and store the logs in a centralized location such as a syslog server or centralized log management platform. All administrator access to the network and network security products is authorized, logged, and monitored. Our IT team monitors all network services and their use, firewall traffic, and resource utilization to ensure the required system performance. We also make projections for future capacity requirements to ensure that our network can meet the demands of our growing organization. The below diagrams provide an overview of Netradyne network architecture across the office locations.



Access to websites containing illegal information or known to contain viruses or phishing material is restricted. Network services and devices are managed in line with the Malware and Antivirus Policy and specifically all sections of the policy. Host intrusion and network intrusion is deployed based on risk, business need and where practical to do so.

Access to the following types of websites where practicable is blocked:

* Known or suspected malicious websites.
* Websites sharing illegal content.

Network devices shall be patched and updated on a documented, regular, and timely schedule. Software or firmware of network devices, such as routers, switches, firewalls, and other infrastructure components, which address security vulnerabilities and other issues must be installed at regular intervals. Patching is an essential part of maintaining the security and reliability of a network.

The network device configuration is backed up on a weekly basis (recurring scheduled backup), typically on Saturdays, or whenever configuration changes are made, and the backup is stored in a central location that is secure.

## IT Hardware & Software Policy

This policy provides guidelines for the purchase of hardware and software that may contain PII/PHI for the organization. It ensures that all hardware and software assets purchased for organizational purposes are suitable, cost-effective, and integrate with other technologies as needed.

### IT Purchase Flow

The purchase of all hardware & software’s must follow the established IT Purchase Process. Click the below link to view the detailed IT Purchase Process.

[IT Purchase Process Flow](https://netorg726775.sharepoint.com/:b:/r/sites/netradynenet/IT%20Policies/Policy%20%26%20Procedures/IT%20Purchase%20Process%20Flow.pdf?csf=1&web=1&e=a30Exl)

* Requester will submit SD+ request to IT Team for any new IT purchase (hardware & software) which will follow the approval from concerned stakeholders.
* The IT team is authorized to purchase any software that is necessary for day-to-day operations in the organization.
* Software’s are procured directly from the manufacturer or its resellers. However, all new software being procured must undergo a review by the InfoSec and Legal teams for vendor risk assessment and data privacy, respectively, especially if they contain PII or PHI. Once the InfoSec team approves the software, it can be procured.
* If any internal stakeholder wishes to purchase an authorized application, the following procedures must be adhered to:
  + A copy of the software license must be provided to IT Team for completion of registration and inventory requirements.
  + Licenses must be registered in the name of Netradyne and not in the name of an individual end-user.
  + You must drop mail for software request with IT Team along with your functional owner approval.
  + Software being procured must undergo a review by the InfoSec and Legal teams for vendor risk assessment and data privacy, respectively, especially if they contain PII or PHI. Once the InfoSec team approves the software, it can be procured.

### IT Hardware Policy

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mouse, printers, and scanners.

The purchase should be made either directly with the manufacturers like Dell, Lenovo, etc. or from the genuine external vendors.

* Desktops, Laptops (Dell, Lenovo, MacBook)
* Servers
* Other Peripheral Devices

For all the Netradyne Laptop Assets we have a standard warranty from manufacturers

* 3Y ProSupport Plus and Accidental Damage Service
* Battery Carries 1 Year Warranty from Invoice Date
* Peripheral Devices like keyboard and Mouse carries 1 Year Warranty from Invoice Date

### IT Software Policy

This policy outlines guidelines for the purchase and use of software within the organization, which may capture any sensitive data which might include PII/PHI, to ensure that all software used is suitable, cost-effective, and integrates with other technologies as needed. This policy applies to software obtained as part of hardware bundles or pre-loaded software.

All software which is licensed needs to be purchased through IT team and prior to the purchase relevant heads of the department or teams must approve it. All other types of non-commercial software such as open source, freeware, etc. can be installed if it is needed for the day-to-day activity or they can reach out to the IT team for the installation of the same.

All purchases of software must be compatible with the organization's server and/or hardware system. The purchase of all software must adhere to this policy.

Use of any unauthorized software in the organization is prohibited. During the orientation sessions, employees are trained on the policies and procedures related to the use of software in the organization, including the restrictions on using unauthorized software which can pose a significant security risk to the organization.

Users (except exception users) must not have administrative access to their computer to allow them to install software onto it. Only approved software will be allowed, and this must be installed either by the IT department upon authorized request, or from internal self-service portal.

Any exception requests must be recorded/captured via IT Service Desk and approved by the inline manager and Infosec team.

### Obtaining Open-Source Software

Open-source software (OSS), freeware, and other software may be installed if needed for day-to-day activities, but it is important to note that some of these software may contain PII/PHI. Therefore, users must ensure that the software they install or download is safe and secure, and that it does not pose a risk to PII or PHI.

OSS (Open-Source SW) is available for download in online repositories. All of them are not of equal quality. Some of them may offer outdated versions of OSS or, in the worst cases, modified OSS which contains malicious components or parts that infringe third parties’ rights. For these reasons, you are asked to apply the following instructions: -

* Download OSS directly on its official author’s, editor’s, or project’s website if there is any.
* Download OSS from OSOR.EU if functionally relevant software is available.
* If not, choose repositories that are accepted and recognized through the OSS community.

[NetradyneOpen-SourceSecurityPolicy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NetradyneOpen-SourceSecurityPolicy.pdf?csf=1&web=1&e=w4ASdk)

### System Hardening and Baseline

System hardening and baseline is also referred to as configuration management. Configuration management is a process of maintaining systems, such as computer hardware and software in a desired state to establish security and minimize areas vulnerable to attack within an organization's systems. The hardened baseline configuration is the first step in this process and it is critical for protecting PII/PHI.

Some of the Hardened baseline configuration checklist could include:

* Enable encryption of all end user laptops to protect PII/PHI
* Install EDR (Crowdstrike) antivirus on all end user laptops.
* Enrol the device with JAMF/Desktop central for centralized management.
* Restrict local admin access for users on their laptops, except for exception users, to prevent unauthorized access to PII/PHI.
* Install standard software such as MS Office, Adobe Reader, etc. on all end-user laptops to ensure that PII/PHI is accessed and handled through secure software

.Any exception request must be recorded/captured via IT Service Desk and approved by the inline manager and Infosec team.

## Inventory & Control of Assets

Netradyne has a wide variety of assets (laptops, desktops, firewalls, switches, wireless access points, keyboard and mouse, adapters, etc...) under its control, all of which have specific value and requirements for protection, especially about PII/PHI. Therefore, it is essential to identify and allocate responsibility for their protection correctly.

These responsibilities include ensuring assets are managed and used appropriately, returned, or disposed of when no longer required, and that appropriate controls are placed upon them in line with their sensitivity and value to the organization.

An inventory of assets associated with Netradyne is maintained and tracked in ServiceDesk+ ITSM tool. Asset ownership refers to the responsibility for the protection and management of an organization's information assets. Asset ownership, which refers to the responsibility for the protection and management of an organization's information assets, including PII and PHI, will be assigned to specific individuals or departments within the organization.

### Hardware Assets

End Users Asset Inventory: Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process PII and PHI information. This inventory shall include all hardware assets issued to end users, whether connected to the organization’s network or not. We track and maintain all the IT asset inventory via ServiceDesk+ Asset Module.

Networking Asset Inventory: This inventory shall include all networking hardware assets that are hooked up, whether connected to the organization’s network or not. This inventory should be regularly updated to ensure that all assets are accounted for, and any missing or lost assets are reported immediately. By maintaining an accurate inventory of networking assets, Netradyne can ensure that all network devices are secured and managed appropriately.

Together, these inventories enable Netradyne to monitor and manage all of its technology assets effectively, minimizing the risk of data breaches or other security incidents.

### Software Assets

Inventory of Authorized Software: To protect the confidentiality and integrity of Netradyne's information assets, including those that contain personally identifiable information (PII) or protected health information (PHI), it is crucial to actively manage the software on the network. Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.

[IT - Netradyne IT Asset Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001%20-%20Aug2025/Policies/IT%20-%20Netradyne%20IT%20Asset%20Policy.pdf?csf=1&web=1&e=ispHpm)

This can help prevent security incidents and ensure that all software used within the organization is properly licensed and supported, further enhancing the security of PII/PHI.

## Acceptable Use of IT Policy

The purpose of this policy is to outline the acceptable use of Netradyne’s computing and network resources (IT resources) as well as other organizational assets to protect the confidentiality and integrity of personally identifiable information (PII) or protected health information (PHI).The Acceptable Usage Policy covers the security and use of all Netradyne information and IT equipment. It also includes the use of email, internet, voice, and mobile IT equipment. This policy applies to all Netradyne employees and contractors.

This policy applies to all information, in whatever form, relating to Netradyne business activities worldwide, and to all information managed by Netradyne relating to other organizations with whom it deals, including PII/PHI. It also covers all IT and information communications facilities operated by Netradyne or on its behalf.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, Netradyne will take disciplinary action, including the restriction and loss of network privileges.

Netradyne takes the security and integrity of its IT resources seriously and expects all the staffs to comply with this policy to protect the confidentiality and integrity of PII/PHI. By adhering to these guidelines, we can ensure the proper use of our technology assets, protect sensitive information, and minimize the risk of security incidents involving PII/PHI.

### Computer Access Control

Users of Netradyne’s IT resources are expected to abide by the following guidelines that are built around the underlying principles of acceptable use of organizational assets. These guidelines apply to all Netradyne staff who use the organization's IT resources.

* Comply with the customer’s contractual security obligations and requirements.
* Comply with all information security policies, regulations, procedures, and rules.
* Users are expected to protect the confidentiality and integrity of PII/PHI and other sensitive information by not sharing it with unauthorized individuals or using it for personal gain.
* Only access files or data belonging to you or where the owner of the data has permitted you to access them.
* Do not leave any passwords unprotected (Ex: Writing down).
* Do not perform any unauthorized changes to IT systems or information’s.

By following these guidelines, users can help ensure the proper use of Netradyne's IT resources and minimize the risk of security incidents involving PII/PHI.

### Internet and Email Conditions of Use

Use of internet and email is intended for business use and must be used in a manner that protects the confidentiality and integrity of personally identifiable information (PII) or protected health information (PHI).Personal use is permitted where such use does not affect the individual’s business performance, is not detrimental to in any way, not in breach of any term and condition of employment and does not place the individual or in breach of statutory or other legal obligations related PII/PHI.

All individuals are accountable for their actions on the internet and email system.

Individuals must not:

* Use the internet or email for the purposes of harassment or abuse.
* Use profanity, obscenities, or derogatory remarks in communications.
* Access, download, send or receive any data (including images), which is considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
* Use the internet or email to make personal gains or conduct a personal business.
* Use the internet or email to gamble.
* Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
* Place any information on the Internet that relates to the organization.

### Actions upon Termination of Contract (IT Assets Return)

All Netradyne organizations equipment and data, for example laptops and mobile devices including telephones, smartphones must be returned to Netradyne IT team at termination of contract. This is to ensure that no unauthorized access to personally identifiable information (PII) or protected health information (PHI) occurs. All organizational data or intellectual property developed or gained during the period of employment remains the property of Netradyne and must not be retained beyond termination or reused for any other purpose.

* It is user's responsibility to report suspected breaches of security policy without delay to your line management or to the IT department.
* All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with organizational disciplinary procedures.

When an employee leaves the organization under normal circumstances, their access to computer systems and data must be suspended at the close of business on the employee’s last working day. It is the responsibility of HR to request the suspension of the access rights via the [IT Service Desk].

### Disposal of Media Policy and Procedures

The purpose of this policy is to outline the proper handling of the media. This policy applies to employees, contractors, temporary staff, and other workers in the organization, including all personnel with access to sensitive and classified data and media. This policy applies to all equipment that processes classified and sensitive data (PII/PHI) that is owned by the organization.

When no longer usable, tape cartridges, hard copies, printouts, and other related items used to process, or store classified and/or sensitive data (PII/PHI) shall be properly disposed in a secure and appropriate manner. The assets are disposed through an authorized third-party vendor.

The following procedures are followed.

* When no longer usable, hard copies and printouts shall be placed in properly marked shredding bins.
* Tape cartridges shall be taken apart and placed in the properly marked shredding bins.
* Destruction is a method of destroying media/hard disks containing personally identifiable information (PII) or protected health information (PHI) unusable by physically dismantling them through methods such as crushing, disassembling, or any other means that renders the data unreadable and unrecoverable. This is a secure method of disposing of media and hard disks that contain sensitive PII/PHI, as it ensures that the data cannot be accessed or retrieved by unauthorized individuals.

Netradyne expects all individuals who handle media containing PII/PHI to comply with this policy to ensure that the organization's data is protected, and confidentiality is maintained.

## Vendor Management Policy

A vendor is a party in the supply chain that makes goods and services available to companies or consumers. It starts with due diligence and assessing whether a third-party vendor should have access to sensitive data.

### Vendor Due Diligence

Netradyne performs the Vendor Due Diligence (VDD) when a company seeks to buy, partner with, or enter a business relationship with another company. The customized due diligence checklist is used to assess another company. Due diligence is a process of evaluating and assessing whether a third-party vendor should have access to sensitive PII/PHI. This includes assessing the vendor's security controls and practices to ensure that they meet the organization's security standards and requirements. Proper due diligence is important to ensure that vendors are trustworthy and have a secure environment to manage and process PII/PHI.

[Infosec-Netradyne Third Party Risk Management Procedure](https://netorg726775.sharepoint.com/:b:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001%20-%20Aug2025/Policies/Infosec-Netradyne%20Third%20Party%20Risk%20Management%20Procedure.pdf?csf=1&web=1&e=jIhA09)

### Procurement of IT assets\accessories

* IT function has listed all the Vendors and maintaining the procurement list and vendors for Hardware’s and Network Management etc.

#### Preventive Maintenance

* Perform Periodic health check of the deployed products.
* Perform Upgrades and updates of the deployed products.
* Perform Log audits of the deployed products.

#### Emergency on-site support

* When the unexpected occurs, we can send an expert to help you bring your systems back online.
* Deliver skilled and focused resources when you need them.
* Our Emergency Support team can also assist your team during and directly following planned system changes.

#### Technical Account Manager (TAM)

* Dedicated Technical Account Manager
* Leverage personalized support to work remotely with a designated senior engineer during business hours.
* Get focused attention on critical issues. Training Services
* Our customized training services can provide the highest levels of practical training to deliver results for individuals and organizations.
* Certification level training available

## Employee Onboarding & Offboarding Policy

### Onboarding Policy

HR team will be sending an email & creating a ServiceDesk+ request to the IT team notifying them about the new joiner with the relevant details including personally identifiable information (PII) or protected health information (PHI) that may be required for the user's job role. 

An initial strong password must be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account to ensure the security of the account and protect any PII/PHI that may be stored. Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general, this will be role-based, This ensures that users are granted access only to the systems and data required for their specific job duties and that any PII/PHI is protected from unauthorized access.

[Employee Onboarding workflow](https://netorg726775.sharepoint.com/:b:/r/sites/netradynenet/IT%20Policies/Policy%20%26%20Procedures/Employee_Onboarding_workflow.pdf?csf=1&web=1&e=4WSuX3)

[Contractor Onboarding workflow](https://netorg726775.sharepoint.com/:b:/r/sites/netradynenet/IT%20Policies/Policy%20%26%20Procedures/Contractor_Onboarding_workflow.pdf?csf=1&web=1&e=piKaaB)

### Off-boarding Policy

HR team will be sending an email & create ServiceDesk+ request to IT team notifying about the exit employee with the relevant details providing all relevant details including any PII/PHI that may have been accessed by the employee during their tenure.  When an employee leaves the organization under normal circumstances, their access to computer systems and data containing PII/PHI must be suspended at the close of business on the employee’s last working day.

[Employee Offboarding workflow](https://netorg726775.sharepoint.com/:b:/r/sites/netradynenet/IT%20Policies/Policy%20%26%20Procedures/Employee_Offboarding_workflow.pdf?csf=1&web=1&e=ZmDNja)

[Contractor Offboarding workflow](https://netorg726775.sharepoint.com/:b:/r/sites/netradynenet/IT%20Policies/Policy%20%26%20Procedures/Contractor_Offboarding_workflow.pdf?csf=1&web=1&e=toKjfR)

## User Access Management

The purpose of this policy is to prevent unauthorized access to the Trust’s information systems including any personally identifiable information (PII) or protected health information (PHI) that may be stored. The policy describes the registration and de-registration process for all Trust information systems and services. These policies apply to new starters, leavers, and moving jobs, responsibilities, or portfolios. The aim of the User Access Management Procedure is to support the Information Security Policy and provide a framework for the management of access to users.

Access control is granted on the principle of least privilege. Users are only provided access to the information they require to perform their tasks and role. Access to systems is based on role. Access is granted by the business owner, system owner or data owner and formally approved.

The below diagram provides the overview of User Access Management process:

**Requester**

**Start**

User to submit the request as per the service catalogue template ensuring all the required information is updated

**Rejected**

Approved?

User Line Manager to review the request details in ServiceDesk+ portal and then approve or reject the request

**Approved**

Asset Owner to review the request details in ServiceDesk+ portal and then approve or reject the request. Should understand the purpose of requester

**Rejected** Approved? for seeking access to your applications

**Approved**

Request for High-Privileged Role?

If user has requested for high-privileged roles such as admin, the approval will be triggered to Infosec team

**Yes**

**No**

Infosec to review the request and then approve or reject as applicable

**Rejected** Approved?

**Approved**

Rejection of the request from approvers at any level will lead to cancelling of the request. User should get clarification with approver who rejected & then submit new request

**End**

IT team will review the request details & approval status and provision the access. Send mail confirmation & close the ticket in tool

`

User submits request via

ServiceDesk+ portal

**User Access Provisioning – Process Flow**

Review the request and provision the access

Send confirmation & close the ticket

Request gets cancelled

Where an adjustment of access rights or permissions is required, for example due to an individual changing role, this must be conducted as part of the role change. It must be ensured that access rights no longer required as part of the new role are removed from the user account. If a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role must be requested via IT Service Desk.

**IT Team**

**Infosec**

A review of user accounts with privileged access will be conducted by the Infosec team on a quarterly basis to ensure that this policy is being complied with.

[Infosec-Netradyne IAM Policy Document](https://netorg726775.sharepoint.com/:b:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001%20-%20Aug2025/Policies/Infosec-Netradyne%20IAM%20Policy%20Document.pdf?csf=1&web=1&e=wwEjLE)

## Secure Login Policy

We have secure login policies for accessing each system in ND. All 3rd party services that need to access the code, customer data or systems need 2-factor authentication. Rest systems are password-based.

Laptops will be provisioned by default with a strong password for security. For the rest of the third-party systems, we configure them to use strong passwords for all the members.

## Anti-Malware Policy

Computer viruses are data destructive programs written with the intent of copying and spreading the destruction to other computers and programs. Viruses are classified depending on how they infect the computer systems on a network, and they are of the following types such as Boot Virus, File Viruses, Macro Virus, etc.

The following are common symptoms of a computer infected with a virus:

* The computer fails to start.
* Programs will not launch, or they fail when simple commands are performed.
* Names of files are changing or become unreadable.
* File contents change or are no longer accessible.
* Unusual words or graphics appear on the screen.
* Hard or floppy disks are formatted.
* Variations occur in computer performance, such as slowing down in loading or operation.

Some viruses are deliberately designed to damage files or otherwise interfere with your computer's operation, while others do not do anything but try to spread themselves around. But even the ones that just spread themselves are harmful, since they (generate a lot of traffic and slow down the network leading to the denial of critical services) damage files and may cause other problems in the process of spreading. This may cause loss to individuals/organizations which may be massive. Hence the need for eradication of viruses.

Netradyne has an Antivirus policy defined for the use of Antivirus software in the organization. For Laptop and Standalone Machine, Desktop Antivirus with Latest Update should be installed. We use CrowdStrike EDR solution installed on all user machines.

[infosec-Netradyne\_SOP\_Crowdstrike](https://netorg726775.sharepoint.com/:b:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001%20-%20Aug2025/Policies/infosec-Netradyne_SOP_Crowdstrike.pdf?csf=1&web=1&e=TYCMcL)

## Patch Management Policy

Vendor issued regular security updates and patches are necessary to protect [ND] data and systems from malicious attacks and erroneous functions. Software updates/patches are very important to maintain a secure operational environment. This policy ensures and stresses regular security updates and patches to operating systems, firmware, utilities, and other software updates.

This policy applies to all the Netradyne end users and their machines. Netradyne IT staff will be responsible for creating, deploying, or supporting applications and system software.

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the [ND] network shall be regularly maintained by applying critical security patches within a month after the patches are released by the vendor.

Network devices shall be patched and updated on a documented, regular, and timely schedule. Software or firmware of network devices, such as routers, switches, firewalls, and other infrastructure components, which address security vulnerabilities and other issues must be installed at regular intervals. Patching is an essential part of maintaining the security and reliability of a network.

Patching is performed with the help of Endpoint Central Patch management & JAMF tool. The Central Patch Repository is a portal in the Zoho Corp. site, which hosts the latest vulnerability database that has been published after a thorough analysis. The customers of Endpoint Central & JAMF application are granted access to the Central Patch repository, to periodically download the vulnerability database. It scans the systems in the enterprise network, checks for missing and available patches against the comprehensive vulnerability database, downloads and deploys missing patches and service packs, generates reports to effectively manage the patch management process in the enterprise.

Kindly refer the below document for detailed process

[IT - Netradyne Patching SOP-Secpod.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001%20-%20Aug2025/Policies/IT%20-%20Netradyne%20Patching%20SOP-Secpod.pdf?csf=1&web=1&e=jAbD4Y)

# Password Management Policy

All the end users are responsible for safeguarding their system access login and password credentials which contains PII/PHI information. Password must comply with the password parameters and standards identified in this policy. Passwords must meet the complex 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.

[IT - Netradyne Password Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001%20-%20Aug2025/Policies/IT%20-%20Netradyne%20Password%20Policy.pdf?csf=1&web=1&e=1Sfxuh)

## Mobile Device & Teleworker Policy

### Mobile device policy

During travel (in cars, hotels, conference and meeting rooms, public places) an employee shall take reasonable precautions to protect his laptop as much as possible from damage, theft, and eavesdropping, especially when it contains PII/PHI.If left unguarded, the laptop should be concealed as far as possible (e.g., locked in the boot of the car). Normally an unattended laptop should be in shutdown mode; an unattended laptop should never be accessible without password protection.

* The loss of a laptop/mobile device should be reported to IT Team ([it@netradyne.com](mailto:it@netradyne.com)) immediately via ServiceDesk+ ticketing tool.
* All Netradyne employees must connect their laptops to the Netradyne internal network at least once a week so that the specified security patches and Antivirus definitions can be updated. If this is not feasible in a particular case, the employee should at any rate ensure that the virus definition files are updated at least once a week.
* An employee may not make any alterations which circumvent the Netradyne security mechanisms for his/her laptop. Apart from disciplinary measures, the employee may also be charged with the costs incurred by Netradyne if the laptop is damaged through unacceptable manipulation. Unacceptable manipulation includes, for example:
  + Autonomous set-up of unauthorized Internet connections
  + Switching off virus scanner, particularly with an open connection to the Internet
  + Misuse of privileges granted to enable certain business functions.
  + Retrieval of E-Mail’s from employee’s public mailboxes.
* Users are responsible for maintaining the confidentiality, integrity, and availability of the information(PII/PHI) on their mobile computing device.
* IT team will ensure that users do not have rights to install any software in the laptops given to them.
* In case of a business requirement, users shall take approvals from the department head and contact the IT Engineer.
* IT team shall ensure all Laptops/handheld devices have Antivirus installed on them.

### Teleworking

Netradyne users are currently working on a Hybrid model. A secure communication channel is established between the teleworkers and the networks of Netradyne. We use Cisco AnyConnect and OpenVPN application authentication mechanism for authenticating those using the teleworking solutions. Both applications are MFA enabled.

To ensure the security of Netradyne's information systems and PII/PHI, access rights are revoked, and equipment is returned when the teleworking activity ceases, or when an employee exits from Netradyne. This ensures that former employees or those who are no longer authorized to access PII/PHI cannot gain access through teleworking solutions.

Overall, Netradyne takes the security of its information systems and PII/PHI seriously and implementing secure teleworking solutions is one of the many ways in which the company ensures that its information systems and PII/PHI remain secure.

## Policy for IT Asset Offsite Use

* Breach of Confidentiality: Users are educated not to keep sensitive data\passwords containing PII/PHI information stored on the laptop.
* Theft of Equipment: User must log a case with police and inform IT team especially when it contains personally identifiable information (PII) or protected health information (PHI). IT team to remove\disable the user access.
* Loss of information: User must intimate IT team on any of the information especially when it contains personally identifiable information (PII) or protected health information (PHI) loss so that the further investigation can be taken care.
* Virus/Trojans: User must remove their laptop from network and bring surrender the laptop to IT team so that they Virus\Trojan's can be removed.

## Clear Desk & Clear Screen Policy

To reduce the risk of unauthorized access or loss of information, Netradyne enforces a clear desk and screen policy as follows:

* Personal or confidential business information containing PII/PHI must be protected using security features provided for example secure print on printers, encryption of laptops, etc.
* Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended to prevent unauthorised access to PII/PHI.
* Care must be taken to not leave confidential material on printers or photocopiers which may contain PII/PHI information.
* All business-related printed matter especially contacting PII/PHI must be disposed of using confidential waste bins or shredders.

By enforcing this policy, Netradyne ensures that PII/PHI is protected from unauthorized access or loss, and the confidentiality, integrity, and availability of PII/PHI is maintained.

## Printer Policy

Employees are required to use shared networked printers to print the documents form their workstation. The user must adhere to the organization printer policy as stated below:

* Printers are to be used for documents that are relevant to the day-to-day conduct of business at Netradyne These printers should not be used to print personal documents.
* Do not print multiple copies of the same document or any document that contains PII/PHI related information– the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.
* If you print something, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately (i.e., recycle).
* Make efforts to limit paper usage by taking advantage of duplex printing (i.e., double-sided printing) features offered by printers and other optimization features.
* Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer.
* If you encounter any physical problem with the printer (paper jam, out of toner, etc.) and are not “trained.” in how to fix the problem, please do not try. Instead, report the problem to IT Team.
* Report any malfunction of any printing device to IT Team as soon as possible.

## Logging and Monitoring

Logging should be enabled, including log configuration changes, preferably back to a central source like a syslog server or a centralized log management platform. All Netradyne networking devices are enabled with logging and the logs are stored or saved in syslog server.

All administrator access to the network and network security products should be authorized, logged, and monitored. Netradyne’s IT team shall monitor all network services and their use. All security system traffic should be monitored for misuse and intrusions.

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. Currently we are using Pingdom, site47/7 for alerting and monitoring of our critical devices.

## Backups and Business continuity plan

A business continuity plan (BCP) outlines procedures and instructions an organization must follow in the event of a disaster or other disruptive event. The goal of a BCP is to ensure that essential business functions can continue during and after a disaster or other interruption.

Netradyne has dual ISP connectivity and uses both connections simultaneously to provide failover and load balancing capabilities. If one ISP goes down, the other can take over, ensuring that the organization's internet connectivity remains uninterrupted. This redundancy is critical for businesses that require constant internet connectivity to conduct their operations.

Network device configuration is backed up regularly or whenever configuration changes are made to a central source. The central backup source shall be secured.

[Netradyne Business Continuity Plan.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001%20-%20Aug2025/Policies/infosec-Netradyne%20Business%20Continuity%20Plan.pdf?csf=1&web=1&e=G7IHnJ)

# Conduct

To ensure compliance with regulatory requirements and maintain the confidentiality, integrity, and availability of personally identifiable information (PII) or protected health information (PHI), Netradyne will conduct compliance checks using various methods. These methods include reports, internal/external audits, awareness training/assessments, and feedback to the process owner. These checks will ensure that employees are following the clear desk and screen policy correctly and prevent unauthorized access to PII/PHI.  
  
In case of non-compliance, the issue will be escalated to the Netradyne leadership team to take appropriate action. This will ensure that the policy is being followed consistently, regulatory requirements are met, and any non-compliance is addressed in a timely and efficient manner. By performing compliance checks, Netradyne can maintain the security of its information systems and PII/PHI, and ensure that its employees are following the company's policies and procedures..

# Exception

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

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. To request a security exception, contact the InfoSec team.

For any exception on valid reasons, approvals are needed from System Owner (First Level) and InfoSec Head (Second Level). By implementing this exception process, Netradyne has maintained the security of its information systems and PII/PHI while ensuring that legitimate business needs are met.

[Infosec-Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/netradynenet/Infosec%20Policies/Infosec-Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=CLRSlG)

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| ND | Netradyne |
| IT | Information Technology |
| PII | Protected Health Information |
| PHI | Personally Identifiable Information |

# References

## Templates

[NetradyneDocumentationTemplate\_v1.0.dotx](https://netorg726775.sharepoint.com/:w:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NetradyneDocumentationTemplate_v1.0.dotx?d=w15edb35bf0bd47b39b325132e1ab95fb&csf=1&web=1&e=IjO5cq)

[ISMS\_RiskRegister\_MASTER.xlsx](https://netorg726775.sharepoint.com/:x:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/General/RISK%20REGISTER%202022/ISMS_RiskRegister_MASTER.xlsx?d=w41fe8cc8e11b46488cafb429c940b19a&csf=1&web=1&e=bPA1LK)

## Policies

[Personal\_Data\_Protection\_Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Personal_Data_Protection_Policy.pdf?csf=1&web=1&e=J83cFd)

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=VhC3aG)

[NetradyneOpen-SourceSecurityPolicy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NetradyneOpen-SourceSecurityPolicy.pdf?csf=1&web=1&e=w4ASdk)

## Process/Procedures

[Netradyne Vulnerability & Patch Management Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20Vulnerability%20%26%20Patch%20Management%20Process.pdf?csf=1&web=1&e=J15BVF)

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

[NETRADYNE DISASTER RECOVERY PROCESS.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NETRADYNE%20DISASTER%20RECOVERY%20PROCESS.pdf?csf=1&web=1&e=Qluqs9)

[Netradyne Information Security Exception Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20Information%20Security%20Exception%20Process.pdf?csf=1&web=1&e=mKM5sw)

[Netradyne Antimalware Crowdstrike Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20Antimalware%20Crowdstrike%20Procedure.pdf?csf=1&web=1&e=YYHVxv)

[Third Party Risk Management.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Third%20Party%20Risk%20Management.pdf?csf=1&web=1&e=aakiV3)

# 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 |