Information Technology Policy & Procedural Manual

V3.1

netradyne

Contents

Document Control

Document ID	ISMS-025
Document Name	Netradyne Information Technology Policy
Document Status	Published
Document Released Date	01-06-2023
Document Author	Chethan G
Document Content Contributors	Blaize Mathews; Sudhansu Kumar
Document Signatory	Saravanan Sankaran
Document Owner	Chethan G
Document Version	3.1
Information Classification	Internal

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised By
v1.0	13-Jan-2021	New IT Policy Document	Chethan G
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 G

Document Review/Approval

Date	Signatory Name	Organization/Signatory Title	Comments
13-Jan-2021	Saravanan Sankaran	IT Director	
07-Jan-2022	Kavitha Shetty	Sr. Program Manager	
22-Jun-2022	Kavitha Shetty	Sr. Program Manager	
20-May-2023	Saravanan Sankaran	IT Director	

Distribution of Final Document

Name	Organization/Title
All Employees	Netradyne

1 Purpose

The Netradyne IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the organization which must be followed by all staff. It also provides guidelines Netradyne will use to administer these policies, with the correct procedure to follow.

Netradyne will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

2 Scope

The scope of these policies and procedures are applicable to all the Netradyne employees. The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users.

3 Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

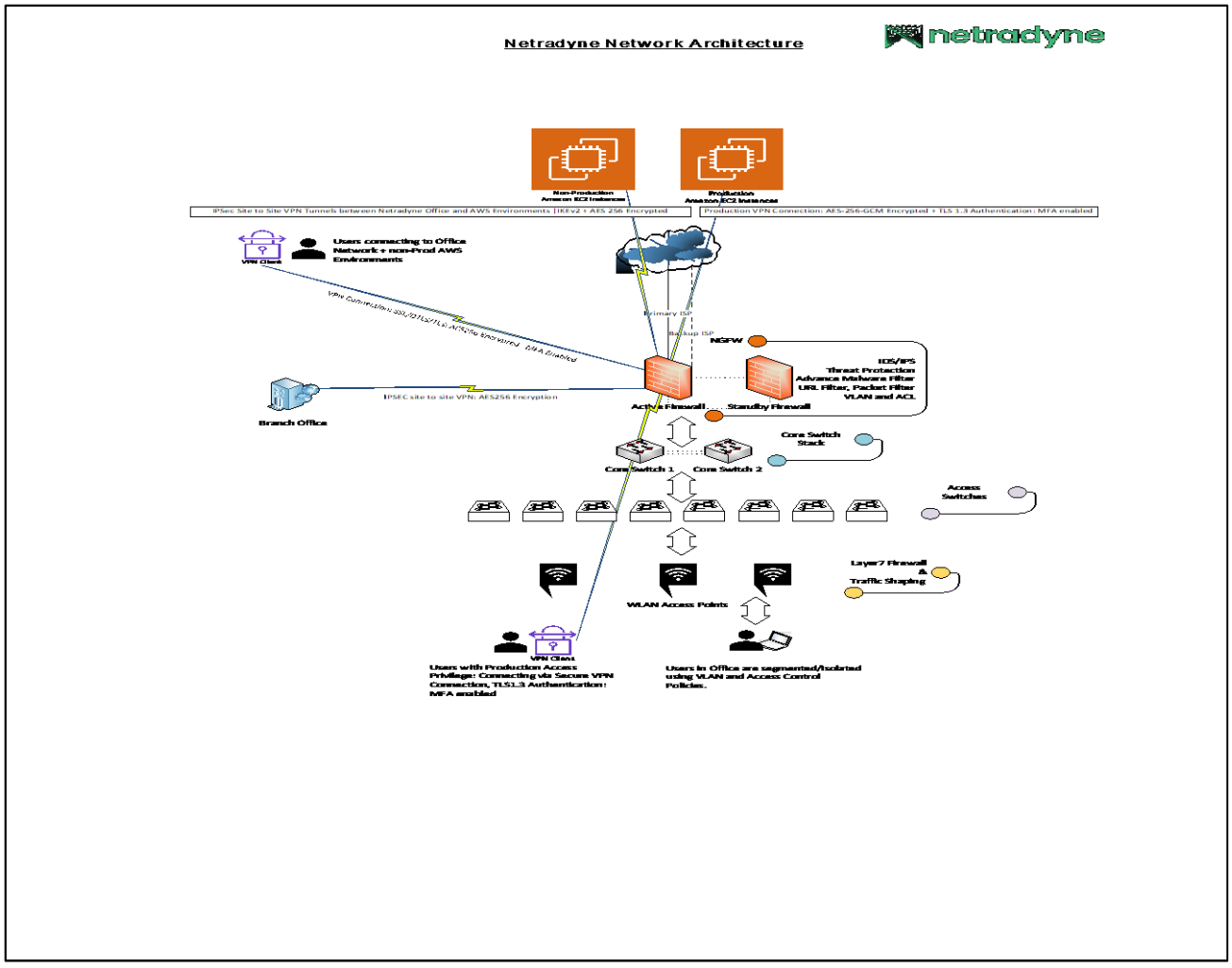
Role	***Responsibilities***
Owner	• Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. • Is the point of contact for the document. • Responsible for initiating and managing document review and the approval process from start 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.

4 Policy

The Netradyne Information Technology (IT) Policy defines rules, regulations and guidelines for proper usage and maintenance of the IT assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for purchase, compliance, IT support and grievance redressal of the employees pertaining to IT assets and services used for daily business operations.

4.1 IT Network Diagram

The below diagrams provide the overview of Netradyne network architecture across the office locations.



The detailed network architecture diagram for all the Netradyne offices is available in the below link:

Network Architecture Diagram

4.2 IT Hardware & Software Policy

This policy provides guidelines for the purchase of hardware & software for the organization to ensure that all hardware & software assets purchased for the organizational purpose is appropriate, value for money and where applicable integrates with other technology for the organization.

4.2.1 IT Purchase Flow

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

IT Purchase Process Flow v1.0.pdf

- Requester will submit SD+ request to IT Team for any new IT purchase (hardware & software) which will follow the approval from concerned stakeholders.
- IT team is authorized to purchase any software that is required for day-to-day operations in the organization.
- Most of the software's are procured directly from the manufacturer or its resellers.
- All the new software being procured should be reviewed with InfoSec & Legal team for the vendor risk assessment and data privacy respectively. Post review & approval from InfoSec the software 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.

- If internal stakeholder wishes to purchase an unauthorized application, the following procedures must be adhered to:
    - You must drop mail for software request with IT Team along with your functional owner approval
    - If approved by functional owner, the software will subsequently be placed on the "authorized" list

4.2.2 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 manufacturer like Dell, Lenovo, etc. or from the genuine external vendors.

- Desktop, Laptops (Dell, MacBook Pro)
- 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

4.2.3 IT Software Policy

This policy provides guidelines for the purchase of software for the organization to ensure that all software used by the organization is appropriate, value for money and where applicable integrates with other technology for the organization. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

All software's which are licensed, needs to be purchased through IT team and prior to the purchase it must be approved by relevant heads of the department or teams.

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 authorised request, or from internal self-service portal.

4.2.4 Obtaining Open-Source Software

Any other software's 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.

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.

4.2.5 System Hardening and Baseline

System hardening and baseline is also referred to as configuration management. Configuration management is a process of maintain systems, such as computer hardware and software in a desired state. Hardened baseline configuration is the first of several critical steps toward establishing security in our organization's systems and minimizing areas that could be vulnerable to attack.

Some of the Hardened baseline configuration checklist could include:

- Enable encryption of all end user laptops.
- EDR (Crowdstrike) antivirus installed on all end user laptops.
- Enroll the device with JAMF/Desktop central for centralized management.
- No local admin access for users on their laptops (except exception users).
- Standard software like MS office, adobe reader, etc... installed on all end user laptops.

4.3 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. To provide effective information security, it is important that assets are identified and responsibility for their protection is allocated correctly.

These responsibilities include ensuring assets are handled 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 are maintained and tracked in ServiceDesk+ ITSM tool. Asset ownership refers to the responsibility for the protection and management of an organization's information assets. Assign ownership of each information asset to a specific individual or department within the organization. This person or department will be responsible for the protection and management of the assets.

4.3.1 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 information. This inventory shall include all hardware assets that are issued to the end-users, whether connected to the organization’s network or not. We are tracking and maintaining 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.

4.3.2 Software Assets

Inventory of Authorized Software: Actively manage (inventory, track, and correct) all 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.

4.4 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. 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 handled by Netradyne relating to other organizations with whom it deals. 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.

4.4.1 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.

- Comply with the customer’s contractual security obligations and requirements.
- Comply with all information security policies, regulations, procedures, and rules
- Refrain from allowing anyone else to use their user ID/token and password on any IT system

- 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.

4.4.2 Internet and Email Conditions of Use

Use of internet and email is intended for business use. 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.

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

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

4.4.3 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. 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

4.4.4 Disposal of Media Policy and Procedures

The purpose of this policy is to outline the proper disposal of 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 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 shall be properly disposed. The assets are disposed through authorized third-party vendor.

The following procedures is 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. As the name implies, destruction of media/hard disk is to physically dismantle by methods of crushing, disassembling, etc.

4.5 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.

4.5.1 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.

Third Party Risk Management.pdf *Netradyne TPRM Preliminary Assessment Accelerator_v1.1.xlsx*

4.5.2 Procurement of IT assets\accessories

- Madhu infotech Pvt InfoTech Pvt
- Dell India Pvt Ltd
- Addit Technologies Pvt Ltd

4.5.3 Network Management

- Digital Track Solutions Pvt Ltd

Standard support provided by DT will coverup all the below list of deliverables

Sl. No	Description	Standard Support
1	Assisted Support	Phone, Mail & Onsite Support
2	Phone support	8*5 support
3	Mail Support	8*5 support
4	Response time (Priority)	4 hours
5	Patch & Version Upgrade	Whenever applicable
6	Preventive Maintenance	Quarterly
7	Training From DT	Basic Training
8	Installation	Yes
9	No of Visits per year	12
10	Case log Reports	Half Yearly

Below is the list of Support Deliverables

4.5.4 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.

4.5.4.1 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.

4.5.4.2 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

4.6 Employee Onboarding & Offboarding Policy

4.6.1 Onboarding Policy

HR team will be sending an email & create ServiceDesk+ request to IT team notifying about the new joiner with the relevant details. IT will be issuing Laptop\MacBook along with the relevant application access. The detailed procedure has been documented on GitHub Repository

4.6.2 Off-boarding Policy

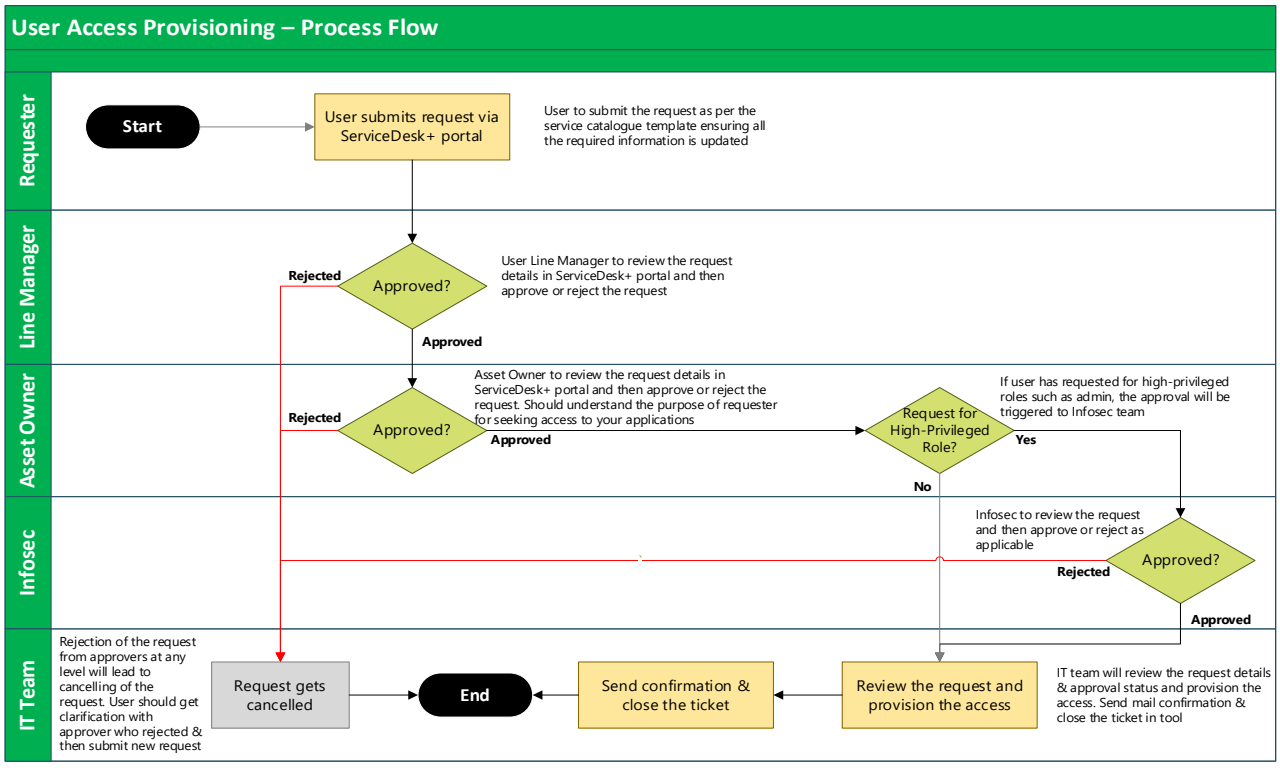
HR team will be sending an email & create ServiceDesk+ request to IT team notifying about the exit employee with the relevant details. IT team will be recovering the IT assets that were issues and revoke the application access. The detailed procedure has been documented on GitHub Repository

4.7 User Access Management

The purpose of this policy is to prevent unauthorized access to the Trust's information systems. 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 purpose of the User Access Management Procedure is to support the Information Security Policy and provide a framework for the management of user access. Netradyne User access matrix has been documented in the below SharePoint link

Netradyne_Access_Matrix

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



Note: If any employee has been promoted to different team or level trough the IJP (Internal Job posting) program, IT team will change the access level accordingly.

4.8 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.

For laptop we by default provision the laptop with a strong password. For the rest of the third-party systems, we configure them to use strong passwords for all the members

4.9 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:

1. The computer fails to start
2. Programs will not launch, or they fail when simple commands are performed
3. Names of files are changing or become unreadable
4. File contents change or are no longer accessible
5. Unusual words or graphics appear on the screen
6. Hard or floppy disks are formatted
7. 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.

4.10 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 much 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 to create, deploy, or support application 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.

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.

The detailed Patch Management Process is uploaded in the below link

Patch Management Procedure

4.11 Password Management 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

4.12 Mobile Device & Teleworker Policy

4.12.1 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. 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) 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.
- User should be responsible for maintaining the confidentiality, integrity, and availability of the information 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.

4.12.2 Teleworking

Netradyne users are currently working in Hybrid model. A secure communication channel is established between the teleworkers and the networks of Netradyne; Use of appropriate authentication mechanism for authenticating those using the teleworking solutions; and Revocation of authority, access rights and return of equipment when the Teleworking activity ceases or when the employee exits from Netradyne.

4.13 Policy for IT Asset Offsite Use

1. Breach of Confidentiality: Users are educated not to keep sensitive data\passwords stored on the laptop.
2. Theft of Equipment: User must log a case with police and inform IT team. IT team to remove\disable the user access.
3. Loss of information: User must intimate IT team on any of the information loss so that the further investigation can be taken care
4. 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

4.14 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:

1. Personal or confidential business information must be protected using security features provided for example secure print on printers, encryption of laptops, etc.
2. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
3. Care must be taken to not leave confidential material on printers or photocopiers.
4. All business-related printed matter must be disposed of using confidential waste bins or shredders.

4.15 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:

1. 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.
2. Do not print multiple copies of the same document – 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.

3. 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).
4. 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
5. Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer.
6. 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.
7. Report any malfunction of any printing device to IT Team as soon as possible.

5 Conduct

Compliance Checks to this policy document to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. This policy document shall be made available to relevant stakeholders and workforce, and they are expected to align with its requirements and acceptable uses. Non-compliance will be escalated to the Netradyne leadership team.

6 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)

7 Terms/Acronyms

Term/Acronym	Definition
ND	Stands for "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

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	Document Contributor	ND Leadership	Functional Area Team	InfoSec	Netradyne Employees
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