

Netradyne IT Asset Policy

v2.3

Internal and Confidential

***Table of Contents***

[Document Control 2](#_bookmark0)

1. [PURPOSE 3](#_bookmark1)
2. [SCOPE 3](#_bookmark2)
3. [ROLES AND RESPONSIBILITIES 3](#_bookmark3)
4. [PROCEDURE 3](#_bookmark4)
5. [IT ASSET RETURN POLICY 5](#_bookmark5)
6. [IT ASSET LOST/STOLEN PROCEDURE 6](#_bookmark6)
7. [IT ASSET MAINTENANCE AND REPAIR 6](#_bookmark7)
8. [IT ASSET DISPOSAL & SCRAPPING POLICY 7](#_bookmark8)
   1. [Ground of condemnation 7](#_bookmark9)
   2. [Disposal Methods 8](#_bookmark10)
9. [PHYSICAL SECURITY & THEFT PREVENTION 8](#_bookmark11)
10. [MEDIA SANITIZATION 9](#_bookmark12)
11. [CONSEQUENCES OF BREACHES 9](#_bookmark13)
12. [CONDUCT 9](#_bookmark14)
13. [EXCEPTION 9](#_bookmark15)
14. [TERMS/ACRONYMS 9](#_bookmark16)
15. [REFERENCES 9](#_bookmark17)
16. [APPENDIX A: DOCUMENT RACI MATRIX 10](#_bookmark18)

## Document Control

|  |  |
| --- | --- |
| **Document ID** | NDITAM2021001 |
| **Document Name** | Netradyne IT Asset Policy |
| **Document Status** | Released |
| **Document Released Date** | 6-Jun-2024 |
| **Document Author** | Chethan Gangaraju |
| **Document Content Contributors** | Kothai Rajkumar, Priyesh Parashar |
| **Document Signatory** | Sudhansu Kumar |
| **Document Owner** | Chethan Gangaraju |
| **Document Version** | v2.3 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 10-Dec-2021 | New policy document for IT Asset Management | Vijaykumar Dalal/Chethan G |
| V2.0 | 21-Jun-2022 | Updated reference to ServiceDesk+ | Vijaykumar Dalal |
| v2.1 | 20-Feb-2023 | Aligned with standard template | Chethan Gangaraju |
| v2.2 | 4-Jun-2024 | Revised the document with latest date | Chethan Gangaraju/Priyesh Parashar |
| v2.3 | 30-May-2025 | Annual Revision | Chethan Gangaraju/Priyesh Parashar |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Sign atory Title** | **Comments** |
| 21-Dec-2021 | Kavitha Shetty | Sr. Program Manager  - InfoSec |  |
| 22-Jun-2022 | Kavitha Shetty | Sr. Program Manager  - InfoSec |  |
| 22-Feb-2023 | Sudhansu Kumar | Sr Staff- Risk and Compliance | Aligned with standard template |
| 5-Jun-2024 | Sudhansu Kumar | Sr Staff- Risk and Compliance |  |
| 3-Jun-2025 | Kavitha Shetty | Sr Staff- Risk and Compliance |  |

**Distribution of Final Document**

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

# Purpose

This document of Netradyne serves to outline the policy on the use and storage of company provided IT Assets like laptops, mouse, keyboards, monitors etc.

# Scope

This Policy and the procedures herein affect all employees who use laptops for official purposes. Employees are also advised that in addition to the terms and conditions of laptop usage as reflected in this Policy, employees shall also have to adhere to any terms of their respective employment agreement which mandate or restrict any action in this regard.

An employee using company provided laptops & other devices is responsible for its security, regardless of whether the laptop or device is used in the office, at one's place of residence, or in any other location such as a hotel, conference room or while travelling. This Policy contains certain guidelines and restrictions on the usage of the laptop that are required to be strictly adhered to by all employees while using these laptops.

# 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  Approvers Document Release | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| 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 Owner/team to work with repository administrator to make release version available. |

# Procedure

An IT asset policy procedure is a document that outlines the policies and procedures for managing IT assets within an organization. The goal of an IT asset policy procedure is to ensure that IT assets are accounted for, properly managed, and used effectively

## Intended Use of Netradyne IT Assets

All the IT assets provided to the employees shall be always the property of the Company and the employee will not have any right or interest in the said asset except using such asset during employment or for such duration as may be decided by the Company. Employees must ensure that the laptop is being used only for official purposes and during the rightful discharge of their duties and not for generating, transmitting, corresponding to any content that is contrary to Company policies. This may lead to the employee being subject to discipline or any other appropriate action as per Company policies.

* + - When traveling (in cars, hotels, conference and meeting rooms, public places) an employee shall take reasonable precautions to protect his Company assets 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 Company IT Asset should be reported to IT Team [(it@netradyne.com)](mailto:(it@netradyne.com) and their reporting manager immediately
    - 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 that 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 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 the right to install any software on the laptops given to them.
    - In case of a business requirement, users shall get approvals from the department head and contact the IT Engineer.
    - IT team shall ensure all Laptops/handheld devices have Antivirus installed on them
    - IT Team to ensure the Netradyne Asset Inventory Registry is up to date in ServiceDesk+

## Laptop Security Controls

All laptops acquired for employees on behalf of the Company shall be deemed to be Company property. Each employee issued with a laptop shall be responsible for the security of that laptop, regardless of whether the laptop is used in the office, at the employee’s place of residence, or in any other location such as a hotel, conference room, car or airport. Employees shall ensure security of the laptop in each of the following domains as per the stated guidelines. Laptops must compulsorily be protected by a username and password.

## Data Security Controls

Employees are expected to ensure the security of the data within their laptops. In this regard employees should adhere to the following:

* + - Employees are personally accountable for all network and systems access under his/her user ID. Never share the passwords with anyone, not even with family members, friends, or IT staff
    - Corporate laptops are provided for official use for authorized employees. Do not loan laptop or allow it to be used by others such as family and friends
    - Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine

## Data Backups Controls

* + - Employees are highly recommended to save their data in OneDrive or enable the sync of local storage with OneDrive
    - Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Saving the data in one drive will save you a lot of headaches and extra work.

## Virus Protection

Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.

* + - The user system should be removed from the network for any suspicious virus intrusion or infection
    - Report any security incidents (such as virus infections) promptly to the IT Team to minimize the damage
    - Always virus-scan any files downloaded to your computer from any source (USB hard disks and memory sticks, network files, email attachments or files from the Internet).
    - Virus scans normally happen automatically if your virus definitions are up to date, but you can also initiate manual scans if you wish to be certain.
    - Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g., by unusual file activity) by contacting the IT Team

## Use of Unauthorized Software/Content

* + - Employees are required to ensure that they do not download, install, or use unauthorized software programs.
    - Unauthorized software could introduce serious security vulnerabilities into the Company networks as well as affecting the working of your laptop.
    - The employee shall not install any unauthorized accessories/software like messengers, chatting software or any malicious software, which may cause problems to the functioning of the laptop and strictly adhere to Company’s software
    - As you might expect, Company will not tolerate inappropriate materials such as pornographic, racist, defamatory, or harassing files, pictures, videos, or email messages that might cause offence or embarrassment to either the Company, its employees or any third party
    - The Company’s IT staff shall routinely monitor the Company network and systems for such materials and track the use of the Internet by all employees. Such IT staff shall report serious/repeated offenders and any illegal materials directly to Company management, and appropriate disciplinary processes will be initiated against such employees by the management.
    - Further, in the event any employee is unsure of the status of any digital/electronic information that he or she may discover on any laptop system provided to such employee, the employee must forthwith and without any further delay communicate the existence of such information to the Company’s IT team on the assumption that all such information is potentially Confidential Information, and thereafter follow the instructions of the IT team in this regard.

# IT Asset Return Policy

All the Netradyne employees, on or before the last day of employment must return all company owned IT assets to IT team where IT Team is responsible for ensuring that all company owned IT assets are returned by the departing employee. Failure to return the company IT Asset, HR will

withhold the Full & Final settlement for the concerned employee, or the IT Asset value will be recovered as part of Full & Final settlement.

The below procedure must be followed to return the IT Asset:

## Employee Exit/Termination:

* + - The employee manager must initiate the offboarding process for the departing employee by sending an email request to HR.
    - HR to intimate IT via email & ServiceDesk+ request for the returning of the assets & revoking the access of the employee
    - The departing employee must return all the company owned assets to the IT Team and IT Team will update the asset inventory, revoke the access & clear the record. Revoke the access within 24 hrs
    - IT Team will send the email confirmation to manager & HR team for the asset clearance

## Ad-hoc Return of IT Asset:

* + - The employee must initiate the email request with IT Team for the return of company IT Asset
    - IT Team must provide clearance over the mail once the assets are collected and update the Asset Inventory List

# IT Asset Lost/Stolen Procedure

In case of any Netradyne IT Asset lost or stolen, the user (Custodian) must follow the below process:

* Custodian reports theft to local police where asset was stolen
* Custodian immediately reports theft to Netradyne InfoSec team and IT Team on below email address along with his line manager:
  + InfoSec <[infosec@netradyne.com](mailto:infosec@netradyne.com)>;
  + IT Team <[it@netradyne.com](mailto:it@netradyne.com)>
* Custodian should log a Security Incident via ServiceDesk+ & provide the below details to InfoSec & IT Team reporting Lost or Stolen IT Assets in the Description:
  + Full Name:
  + Department Name:
  + Manager Name:
  + Asset Type: (Laptop/Monitor/Desktop/)
  + Asset No.: (To be filled by IT Team)
  + Incident Location:
  + Stolen or Lost or Unknown:
  + Date of Lost:
  + Estimated Value of the Asset: (To be filled by IT Team)
  + Did you file the FIR with Police (Yes/No)?
  + If above answer is Yes, provide FIR No.:
  + Name of Police Station:
  + Any confidential data associated with stolen IT asset? (Yes/No):
  + Remarks
* InfoSec team to review the details provided and taken necessary actions. Also, they will validate for any data loss or theft.
* IT Team to disable the system login and revoke all the application access.
* IT Team must update the Asset Inventory Registry with State as “Stolen”

# IT Asset Maintenance and Repair

IT Asset maintenance & repair is defined as a process in which working condition of a company asset is maintained at the optimum level as to give maximum output. Maintenance is done through repair, partial replacement, and total replacement. Following is the significance of the maintenance policy:

* Assets are always in ready and reliable condition. This ensures company is able respond to any sudden change in demand
* Ensures that there are no major breakdowns
* Ensures that costs are always controlled

The following procedure is followed for any asset repair:

* Employee should reach out to IT Team for any asset repairs/replacements
* IT Team will assess the issue and take necessary actions to fix it
* Any asset being repair or under maintenance must be updated into Asset Inventory

Registry with status “In Repair”

* If the asset repair needs involvement from vendor/manufacturer, IT Team will communicate the same with the vendor/manufacturer & take appropriate actions accordingly
* Any assets being repaired will be done at Netradyne office premises
* If asset needs to be taken out of Netradyne office premises, the same has to be updated in front-office register
* Once the asset is returned by the vendor, update the asset registry and handover the laptop to the employee

# IT Asset Disposal & Scrapping Policy

The IT asset disposal policy is concerned with managing the secure disposal of equipment owned by the Netradyne but no longer required. The disposal of an IT asset is required due to its need for replacement or upgrade, or it has become obsolete, surplus, or redundant. Netradyne aims to ensure that all its IT assets are managed effectively, including its disposal.

The purpose of this policy is to outline the proper disposal of media. This policy applies to employees, contractors, 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 Asset Inventory Registry must be updated with state as “Retired” for all those assets under disposal.

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.

Any non-working IT assets that will be disposed will be intimated/updated to the finance team.

All the Working and Non-working IT assets which are end of life or out warranty are currently stocked in the Storage room with all the inventory details.

## Ground of condemnation

The IT assets can be condemned on the below grounds:

1. IT Asset outlived its prescribed life or certified as unfit by the IT Team or as per the company scraping policy for renewal. The prescribed life of the IT assets is as following
   1. Servers/printers: 05 years
   2. Laptops/Desktops: 05 years or until its certified as unfit by IT Team
   3. Networking devices like LAN Cables/Routers/Switches: 05 years
2. IT Assets which have become obsolete technology-wise and can't be upgraded and support from vendor either paid or unpaid does not exist and their use may result in security threat/ unauthorized access to data
3. Beyond economical repair: When repair cost is considered too high (exceeding 50% of residual value of equipment taking depreciation into account), and the age of the equipment
4. IT Asset that has been damaged due to fire or any other unforeseen reason and have been certified as beyond repair by the IT Team and associated vendor/manufacturer.

## Disposal Methods

The IT Assets can be disposed based on the working condition of the IT assets and as per disposal methods as per the information below:

## Working/Non-Working IT Assets:

* **Hardware Destruction:** All the hardware assets used for storage of data should be formatted and physically destroyed using various methods such as drilling/scratching/cutting of platters for 2.5-inch hard drives, and for 3.5-inch hard drives is recommended to be destroyed by professional hard drive destruction/shredding company due to the hardness of the case and material. residual of the hardware should be disposed of as E-waste.
* **E-Waste Management:** It shall be the endeavour of every user to maximize utilization of all IT assets to their full productive life. Apart from internal re-use, option to extend use outside company through donation to Bonafide charitable institutions will also extend the useful life of IT assets. Only such IT assets which are non-operational and cannot be reused for any other alternate purpose should be considered as IT E-waste for disposal with the certification form IT Team.

# Physical Security & Theft Prevention

To ensure physical security of laptops and data therein, all employees are required to undertake the following actions:

* The physical security of Company provided laptops is the employee’s personal responsibility. He/she is therefore required to take all reasonable precautions, be sensible and stay alert to the risks.
* Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag, or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.
* Never leave the laptop unattended when using it outside the office.
* Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel.
* Never leave a laptop visibly unattended in a vehicle. If necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.
* Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage
* Employees may not take the laptop for repair to any external agency or vendor at any point of time
* In case of any failure, employees are required to report the same to the management
* In case of the loss of laptop- be it on, or off Company premises, due to negligence of the employee, the Company may recover the cost of the laptop from the employee. It is the Company’s discretion to impose further penalties on account of loss of sensitive Company information
* If there is damage on account of the above the employee may be liable to pay the damages at cost to the Company/the same may be deducted from their monthly salary
* Company maintains the right to conduct inspections of any computer equipment, including all laptop it owns or manages without prior notice to the Employee who is at the time the user or custodian of such computer equipment. Employee will submit the laptop for random audit by Company to check the physical presence as well as the functional usability of the asset
* In case of leaving the employment or being terminated for any reason, employee must hand over the asset to Company IT team in good condition failing which Company is authorized to charge penalty against the employee
* IT team to ensure all end point security controls are implemented in all system before allocating the IT Assets to the employees. The remote access should not be enabled for any systems.

# Media Sanitization

When transferring company IT assets to another trustee/party, any confidential information on the device must be protected and/or destroyed. The method of data destruction is dependent upon the sensitivity of the data on the device and the next user of the device (i.e., within the organization and its control or outside the organization).

# Consequences of Breaches

* Any action of the employee that are inconsistent with this Policy shall be treated as serious professional misconduct on the part of the employee, and the employee concerned shall be subject to any disciplinary proceeding, or action, by the Company
* The Company shall bear expenses for laptop maintenance and repairs arising out of the normal wear and tear However, in the event of any damage to the laptop arising out of the negligence, misuse or abuse of the laptop by the employee, the employee shall be solely liable to make the payment for all the expenses arising therefrom. The Company shall have the right to reclaim such expenses and deduct the same from your monthly salary.

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

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

# Terms/Acronyms

**Term/Acronym Definition**

|  |  |
| --- | --- |
| ND IT LAN | Netradyne |
| Information Technology |
| Local Area Network |
|  |

# 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*

Responsible

*R A C*

*I*

Accountable

Informed

Consulted