Netradyne Acceptable Usage Policy

v2.1

Internal and Confidential

TABLE OF CONTENTS

Document Control

Document ID	NDAUP2021002
Document Name	Netradyne Acceptable Usage Policy
Document Status	Released
Document Released Date	23-JUN-2021
Document Author	INFOSEC
Document Content Contributors	IT
Document Signatory	Saravanan Sankaran<saravanan.sankaran@netradyne.com>
Document Owner	INFOSEC
Document Version	V2.1
Information Classification	Internal

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised By
v1.0	23-JUN-2021	Original Release	InfoSec
v2.0	31-AUG-2022	Aligned with standard template	Melwin
v2.1	29-MAY-2023	Modifications in mobile device usage	Melwin

Document Review/Approval

Date	Signatory Name	Organization/Signatory Title	Comments
30-JUN-2021	Saravanan Sankaran	Senior Director InfoSec & IT	
01-SEP-2022	Saravanan Sankaran	Senior Director InfoSec & IT	
30-MAY-2023	Sudhansu Kumar	Senior Staff-InfoSec	

Distribution of Final Document

Name	Organization/Title
All Organization	Netradyne

1 Overview

The Information Security Department "**InfoSec Team**" is committed to protecting Netradyne employees, contractors, and other technology users from illegal or damaging actions by individuals. This Acceptable Usage Policy (this "**Policy**") generally aligns with the information security management systems standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (EC) as more specifically set forth in ISO 27001 and 27002. Implementing this Policy will therefore help Netradyne comply with various aspects of such international data security standards.
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network resources and network accounts providing electronic mail, online browsing, and file transfer protocols (collectively, "**IT assets**"), are the property of Netradyne. These systems should only be used for business purposes in support of Netradyne and its clients and customers during normal operations. Effective security is a team effort involving the participation and support of everyone who handles Company information and information systems.

2 Purpose

The purpose of this Policy is to outline the acceptable use of IT assets at Netradyne. These rules are in place to protect Netradyne information against loss or theft, unauthorized access, disclosure, copying, use, modification, or destruction (each an "Information Security Incident"). Information Security Incidents can result in a broad range of negative consequences, including embarrassment, financial loss, non-compliance with standards and legislation and legal liability to third parties.

3 Scope

This policy applies to all employees of Netradyne, as well as third-party contractors and agents of Netradyne who have access to Netradyne information or IT assets. All individual users are responsible for exercising good judgment regarding the appropriate use of Netradyne information and IT assets in accordance with Netradyne policies and standards, and local laws and regulation.

4 Acceptable Use Procedure

4.1 Computer Access Control – Individual's Responsibility

Access to the Netradyne IT assets is controlled using User IDs, passwords, multi-factor authorization ("**MFA**") or tokens. All User IDs and passwords will be uniquely assigned to named individuals and consequently, individuals are accountable for all actions pursuant to such IDs and passwords.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any Netradyne IT assets.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Netradyne IT assets.
- Leave their password unprotected, for example writing it down or storing passwords in an unsecured document or medium.
- Perform any unauthorised changes to Netradyne IT assets or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non- Netradyne authorised device to the Netradyne network or IT assets.
- Store Netradyne data on any non-authorised equipment.
- Give or transfer Netradyne data or software to any person or organisation outside Netradyne without the authority of Netradyne.

4.2 Internet and Email Conditions of Use

Use of the Netradyne 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 Netradyne in any way, is not in breach of any term or condition of employment and does not place the individual or Netradyne in breach of statutory or other legal obligations.

All individuals are accountable for their personal actions on the Netradyne Internet and email systems.

Individuals must not:

- Use the Netradyne 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 could be reasonably considered offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
- Use the Netradyne Internet or email to make personal gains or conduct a personal business.
- Use the Netradyne Internet or email to gamble.
- Use Netradyne email systems in a way that could affect its reliability or effectiveness, for example by distributing chain letters or spam.
- Place any information on Internet that relates to Netradyne, alter any information about it, or express any opinion about Netradyne, unless they are specifically authorised to do this.
- Send or share with third parties any unprotected, sensitive, or confidential information without company authorisation.
- Forward Netradyne mail to personal (non- Netradyne) email accounts (for example a personal Hotmail/Gmail account).
- Make official commitments through the Internet or email on behalf of Netradyne unless authorised to do so.
- Download copyrighted material such as, but not limited to, music media (MP3) files, film, and video files without appropriate approval.
- Knowingly infringe any copyright, database rights, trademarks, or other intellectual property rights.
- Download any software from the Internet without the prior approval of the IT Department.
- Connect Netradyne devices to the Internet using non-standard connections.

4.3 Clear Desk and Clear Screen Policy

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

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

4.4 Working Off-site or Working from Home

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with the Netradyne remote working policy.
- Netradyne IT assets taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.

- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

4.5 Mobile Storage Devices

Mobile storage devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. If there is a requirement of mobile storage devices such as pen drives/hard disk is required, please file an exception request using ServiceDeskPlus (SD+) ticket with business justification and relevant approvals as defined in Netradyne Exception Management Process for consideration as an exception.

4.6 Software

Employees must use only software that is authorised by Netradyne on Netradyne IT assets. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Netradyne computers must be approved and installed by the Netradyne IT department.

Individuals must not:

- Store personal files such as music, video, photographs, or games on Netradyne IT equipment.

4.7 Blogging and social media

Limited and occasional use of Netradyne IT assets to engage in blogging and social media activities ("blogging") is acceptable, provided that it is undertaken in a professional and responsible manner, complies with the Netradyne Social Media Policy, is not detrimental to Netradyne interests, and does not interfere with an Individual User's regular work duties. Individual Users assume any and all risks and responsibilities associated with using Netradyne IT assets to engage in blogging in a personal capacity. Moreover, blogging from Netradyne Computer Systems may be subject to monitoring by Netradyne.

In addition, the following activities are prohibited:

- Revealing any Netradyne confidential or proprietary information, trade secrets or any other material when blogging.
- Engaging in any blogging that may harm or tarnish the image, reputation and/or goodwill of Netradyne and/or any of its employees.
- Making any discriminatory, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Netradyne Non-Discrimination and Anti-Harassment Policy.
- Attributing personal statements, opinions, or beliefs to Netradyne, or using Netradyne trademarks, logos or any other Netradyne intellectual property without specific authorization from the Netradyne Legal Department.

4.8 Actions upon Termination of Contract

- All Netradyne IT assets, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Netradyne at termination of contract.
- All Netradyne 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.

4.9 Monitoring and Filtering

- All data that is created and stored on Netradyne IT assets is the property of Netradyne and subject to monitoring and filtering.
- IT system logging will take place where appropriate, and an investigation will commence upon a reasonable suspicion of a breach of this Policy. Netradyne retains its right, within applicable legal requirements, to monitor certain activities on its systems, including on the Netradyne Internet and with Netradyne email use, in order to ensure systems security and effective operation, and to protect against misuse.

4.10 Reporting Information Security Incident

- It is an individual's responsibility to report suspected or actual breaches of this Policy without delay to management, the IT department, the InfoSec Team, or the IT helpdesk.
- All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in accordance with Netradyne standard procedures.

5 Acknowledgement

I, [employee's first and last name], understand the requirements and expectations outlined by the Netradyne Acceptable Usage Policy at Netradyne.

I, [employee's first and last name], acknowledge receipt of a printed copy of the Acceptable Usage Policy and agree to abide by the policies and guidelines outlined within as a condition of my employment with Netradyne.

I understand breaching this policy in any way may lead to disciplinary action pursuant to Netradyne's standard policies and procedures.

I understand that if I have questions regarding this Policy, I will consult with my immediate supervisor or the Info Sec Team.

Employee Signature: _____

Employee ID: _____

Employee Printed Name: _____

Date: _____

Location: _____

Acknowledgement received by: _____

6 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.

7 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.

7.1 POLICY COMPLIANCE

The InfoSec Team will monitor compliance with this Policy using various methods, such as business tool reports, internal and external audits, and feedback provided to the InfoSec Team

.

7.2 NON-COMPLIANCE

All Individual Users are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment for cause, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

8 Exception

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

9 Terms/Acronyms

Term/Acronym	Definition

10 References

10.1 Templates

NA

10.2 Policies

NA

10.3 Process/Procedures

NA

10.4 Standards

NA

10.5 Miscellaneous

NA

11 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