

Netradyne Password Policy

v1.3

Internal and Confidential

***Table of Contents***

NetradynePasswordPolicy 0

[Document Control 2](#_bookmark0)

1. [PURPOSE 3](#_bookmark1)
2. [SCOPE 3](#_bookmark2)
3. [ROLES AND RESPONSIBILITIES 3](#_bookmark3)
4. [PROCEDURE 3](#_bookmark4)
   1. [Password Requirements 3](#_bookmark5)
   2. [Password Expiration 4](#_bookmark6)
      1. [Standard Users 4](#_bookmark7)
      2. [Privilege Users 4](#_bookmark8)
   3. [Password Creation 4](#_bookmark9)
   4. [Password Change 4](#_bookmark10)
   5. [Password Reset 4](#_bookmark11)
   6. [Password Reset 5](#_bookmark12)
5. [PENALTIES 5](#_bookmark13)
6. [CONDUCT 5](#_bookmark14)
7. [EXCEPTION 5](#_bookmark15)
8. [TERMS/ACRONYMS 5](#_bookmark16)
9. [REFERENCES 6](#_bookmark17)
   1. [Policies 6](#_bookmark18)
10. [APPENDIX A: DOCUMENT RACI MATRIX 6](#_bookmark19)

## Document Control

|  |  |
| --- | --- |
| **Document ID** | NDPP2022001 |
| **Document Name** | Netradyne Password Policy |
| **Document Status** | Released |
| **Document Released Date** | 14-Jun-2024 |
| **Document Author** | Chethan Gangaraju |
| **Document Content Contributors** | Blaize Mathews, Mauricio Taxman, Priyesh Parashar |
| **Document Signatory** | Sudhansu Kumar |
| **Document Owner** | Chethan Gangaraju |
| **Document Version** | v1.3 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised**  **By** |
| v1.0 | 10-Mar-2022 | New document for Netradyne Password Policy | Vijaykumar Dalal |
| v1.1 | 20-Feb-2023 | Aligned with standard template | Chethan Gangaraju |
| V1.2 | 7-Jun-2024 | Revised the document with latest date | Chethan Gangaraju/Priyesh  Parashar |
| V1.3 | 7-May-2025 | Revised the document with latest date | Chethan Gangaraju/Priyesh  Parashar |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 22-Feb-2023 | Sudhansu Kumar | Sr Staff- Risk and  Compliance | Aligned with standard template |
| 12-Jun-2024 | Sudhansu Kumar | Sr Staff- Risk and Compliance | Aligned with standard template |
| 13-May-2025 | Kavitha Shetty | Sr Staff- Risk and Compliance | Aligned with standard template |

**Distribution of Final Document**

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

# Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. Netradyne IT Team will keep will modify and amend this document from time to time for any changes in the process, policy & procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome

# Scope

The scope of this document is applicable to all the Netradyne employees. The document is updated and developed as part of the day-to-day IT Operations of the organization. This policy applies to all the employees, contractors, vendors & guests of the organization who connects to the Netradyne network & systems.

# 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

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 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.

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.

## Password Requirements

* Be a minimum length of eight (8) characters.
* Password should be combination of upper case, lower case, numbers & special symbols.
* Not be a dictionary word or proper name.
* Restrict sequential and repetitive characters (e.g. 12345 or aaaaaa).
* Not be the same as the User ID.
* Not be identical to the previous (4) passwords.
* Not be transmitted in the clear or plaintext outside the secure location.
* Not be displayed when entered.
* Ensure passwords are only reset for authorized user over call with approvals from manager.
* If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

## Password Expiration

Password expiration is a security practice that requires users to change their password after a certain period of time. This is done to help prevent unauthorized access to user accounts. Password expiration policies are commonly used in organizations to ensure that users maintain strong, secure passwords and to reduce the risk of a data breach.

## Standard Users

The password expiration for all the outsourced applications will follow the manufacturer password expiration policy.

## Privilege Users

The admin accounts/user profile are considered as Privilege Users. The password expiration for all the outsourced applications will follow the manufacturer password expiration policy.

## Password Creation

The password is generated for the Netradyne users using the Password Generator application which will follow the password requirements (i), (ii) & (iii) from section 3.1. Once the default password is generated, it will be shared to their personal email address of the end users. User will be prompted to setup new password for the first-time login.

## Password Change

The password change is required when user feels that there is a threat of password being exposed. For few applications, the password reset is available as self-help where user can reset password on their own by clicking on “Forget Password” options on login pages.

For end users requesting the password change or reset, the below steps should be followed:

* Manager should request the password change or reset on behalf of the user, if user is unable to send the email to IT Team. IT Team will inform the manager with the new password for the requested user. Manager must communicate the same to the user over call.
* If user has requested the password change or reset, the user must create an SD+ ticket and get the same approved by their manager.

## Password Reset

Various options are available to assist users with changing a forgotten or expired password.

1. Users can reset password on their own by using ‘Forgot Password’ link for the applicable application/services
2. If user is unable to rest the password or don’t have option to reset themselves, they need to raise a SD+ request with IT Support team through their manager. Follow instructions as per section 3.4 in this document

## Password Reset

Do not use your User ID as your password. Do not share passwords with anyone, including administrative assistants or agents. All passwords are to be treated as sensitive, Confidential information.

Here is a list of “do not’s”

* Don’t reveal a password over the phone to anyone
* Don’t reveal a password in a mail message
* Don’t reveal a password to the mangers
* Don’t talk about a password in front of others
* Don’t reveal a password on questionnaires or security forms
* Don’t share a password with family members
* Don’t reveal a password to a co-worker while on vacation
* Don’t use the "Remember Password" feature of applications
* Don’t write passwords down and store them anywhere in your office/home/desk
* Don’t store passwords in a file on any computer system unencrypted

If an account or password is suspected to have been compromised, report the security incident to IT team & InfoSec and change all passwords.

# Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

# 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.

* 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.
* In case of manager is not available to approve the request, the user can reach to

manager’s manager or check for the delegation of the manager as authorized approver.

# Terms/Acronyms

**Term/Acronym Definition**

Information Technology

IT

# References

## Policies

*Netradyne Information Security Policy & Procedure.pdf Netradyne Information Technology Policy.pdf*

# 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