Netradyne IAM Policy

v1.0

Internal and Confidential

TABLE OF CONTENTS

Document Control

Document ID	NDIAM2023001
Document Name	Netradyne IAM Policy
Document Status	Released
Document Released Date	13-SEP-2022
Document Author	Garima Bhatt (Garima.bhatt@netradyne.com)
Document Content Contributors	Garima Bhatt
Document Signatory	Saravanan Sankaran
Document Owner	CISO/MR
Document Version	V1.0
Information Classification	Internal

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised By
V1.0	<31/08/2022>	Initial Version Created	Garima Bhatt

Document Review/Approval

Date	Signatory Name	Organization/Signatory Title	Comments
<06/09/2022>	Saravanan Sankaran	Sr. Director – Info Security & IT	

Distribution of Final Document

Name	Organization/Title
Infosec	Netradyne

1 Purpose

This policy describes types of electronic identities in use for systems and applications; criteria for creating identities and accounts; how identities should be authenticated; Least privilege principle, Individual accountability, how authorizations should be managed; and how accounts and privileges should be deprovisioned.

2 Scope

This policy is applicable to Information System operators responsible for Identity and Access Management for information systems. This policy focuses on requirements for systems and applications.

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 Procedure

Identity and Access Management (IAM) provides fine-grained access control across all the systems and helps to securely control access. IAM is used to control who is authenticated (signed in) and authorized (has permissions) to use resources.

4.1 Account Types

4.1.1 User Accounts:

These are uniquely associated with a specific person. These accounts may either exist in a central repository to which systems may federate to consume the identity and authentication information or they may be created locally on a system or device where federation is not practical or possible. The use of the centrally created account with federated authentication is always the preferred method.

4.1.2 Shared Accounts/Generic Accounts:

The use of shared accounts should be discouraged as it lacks accountability and non-repudiation.

Use of generic/shared IDs is restricted and permitted only after completion of an assessment of the risk of the generic/shared IDs and written approval of the senior personnel of the requesting business unit.

4.1.3 Service Accounts:

A service account is used when it is necessary for systems or applications to authenticate to other systems or applications without any association to a person. These accounts should be created sparingly and documentation of the purpose for them should be kept. Their use must be periodically reviewed. Further, the password requirements for service accounts must be no less stringent than user accounts. Finally, service accounts may not be used by people to authenticate aside from initial testing. Service accounts with elevated privileges must be closely monitored for abuse.

4.1.4 Privileged Accounts:

Certain accounts may have extra privileges related to the management of a device or application. This is often thought of as an account type, but it is more accurately described as an account with privileged authorizations. Administrative privilege can be added to any of the three account types. Having at least one account with privileges is generally unavoidable but the use of privilege should be limited and the direct use of shared accounts with privileges should be discouraged as it lacks accountability.

4.1.5 Enterprise Directory Services:

Information about centrally created accounts and identities are stored in central directory run by Information Services and Technology. The implementation of the directory services in Netradyne is Azure Active Directory (AAD). Netradyne information systems should use enterprise directory services whenever possible and avoid creating local accounts and authorizations.

4.1.6 Centrally Managed Accounts:

The process of requesting a centrally managed account is defined by Information Services & Technology's Identity and Access Management Service and adhere to the following guidelines:

- Limit the use of generic or shared accounts.
- Systems storing Restricted Use and/or Confidential information must not be configured to allow access using shared or anonymous accounts.

4.1.7 Non-centrally Managed Accounts

When accounts or authorizations are created outside of the enterprise directory and/or enterprise authentication system, the unit creating the accounts must define the procedure by which they will be approved and created. The procedure must be consistent with the guidelines expressed for centrally managed accounts.

4.2 Separation of Duties:

When an authorization is granted to an account it must be approved by multiple individuals. Multiple approvers ensure that the Principle of Least Privilege is followed from both a technical and process perspective, decreases opportunity for conflict of interest or fraud, and reduces the risk of error. As applied to authorization, separation of duties requires that the administrative and technical approver are not the same person, or if they must be, then the Data Custodian is not filling either role.

4.3 Least Privilege:

As a security best practice, it's important to regularly review organization's access policies to ensure they're granting least privileges. Each policy should come with a policy summary, which is a good place to start when auditing IAM policies.
"*Information Security & Asset Owner is responsible for authorizing privileged access."*

Before granting access to a system or application, Infosec must ensure the following policy is adhered to:

1. Use role-based authorization schemes over individual authorizations whenever practical.
2. Ensure the access granted is as granular as possible in authorizations.
3. Ensure that the authorization has the appropriate approvals following UAM process workflow. Click on References for approval workflow.

4. Privileged access may be granted permanently only if that specific person's job duties routinely require that level of access approved by Infosec & Asset owner, otherwise, the access must be temporary.

5. All authorization requests must be documented, including the nature of the request, the time for which it has been granted, all related approvals that were obtained, and the names of the approvers.

4.4 Individual Accountability

The addition, deletion, and modification of user IDs, credentials, and other identifier objects is controlled by the NETRADYNE IT Operations and Security team such that each user's or service account's identity is uniquely and positively always established. Individual access to, and activity in, a specific area or function is controlled and open to scrutiny. Individual access to controlled areas will not be allowed without establishing identity, authenticating that identity, and authorization based upon that identity. These activities are centrally logged for audit purposes.

Every person with access to Netradyne systems is responsible for selecting strong passwords, keeping the passwords secure, and reporting any unauthorized use of accounts.

Users must:

1. Create passwords that confirm to best practices for selecting passwords which address length and complexity and adhere Netradyne Password Policy.
2. Not share passwords related to any Netradyne system with any other person.
3. Not use passwords related to any Netradyne system for non-Netradyne accounts.
4. Immediately change passwords and notify the appropriate system administrator and/or Information Security if there is reason to believe that a password has been improperly disclosed, accessed, or used by an unauthorized person.
5. Use privileges associated with an account only for the purpose for which they were authorized and no more.
6. Use privileged accounts and authorizations only when such privilege is needed to complete a function.
7. Log off or use screen locking technologies that require authentication when leaving a device unattended.

4.5 Application Access

NETRADYNE's security policies are defined around the principle of "least privilege" and "need-to know". There are a limited set of NETRADYNE employees that will have physical and logical access to a given system, and this is true for both production customer systems, as well as QA and Engineering systems. This list of employees is defined and controlled throughout the customer relationship period. Access lists are reviewed quarterly to ensure that NETRADYNE employees have only the necessary access to do their job.

User access and Privilege access is granted and documented in Role Based access control matrix along with the access level.

4.6 Authentication

Authentication is the process by which a system or application confirms that a person or device really is who or what it is claiming to be and through which access to the requested resource is authorized. Strong authentication protocols help both to protect personal and Netradyne information and prevent misuse of Netradyne resources.
All accounts, centrally defined or not, must require authentication before use.

4.6.1 Multi Factor Authentication:

For increased security, we recommend configuring MFA in all user's accounts to help protecting the systems. As a best practise, enabling MFA is a requirement for all the cloud services, that is being used in Netradyne. MFA requires users to type a unique authentication code from an approved authentication device when the users sign into any Netradyne resources.

4.7 Roles in Authorization

Authorizing an account to use a system or application is a distributed responsibility shared by Information Services & Technology, our IT partners, and sometimes external partners who might create authorizations at our direction.

4.7.1 Administrative and Technical Approvers

All requests for authorization must be approved from an administrative and technical approver. These approvers must be two different people to ensure separation of duties. These approvers are responsible for ensuring the Principle of Least Privilege is applied from their respective viewpoints.

4.7.1.1 Administrative Approval:

The administrative approval confirms that the authorization requested is needed to perform a required function. The approver should sufficiently understand the full scope of the authorization being granted before making a decision and ensure Least Privilege is applied.

4.7.1.2 Technical Approval:

The technical approval confirms that the privilege requested is required to achieve the approved administrative need. The approver should sufficiently understand the full scope of the authorization being granted before making a decision and ensure Least Privilege is applied.

4.7.2 Information Security

Information Security is solely responsible for authorizing privileged access to IS&T servers and applications that process or store client data and any Netradyne system containing Restricted Use information. Information Security will confirm that the user to be authorized has signed the appropriate confidentiality agreement(s), taken appropriate training, and/or holds appropriate credentials for accessing the resource.

4.7.3 Application and System Authorizations

Authorizing access may be automated based on a person's membership in a specific group or a manual process. When authorizing a person to use an application or a system, a Data Custodian must adhere to the following authorization policy.

4.7.4 Authorization Policy

Before granting access to a system or application, the Data Custodian must ensure the following policy is adhered to:

1. Use role-based authorization schemes over individual authorizations whenever practical.
2. Be as granular as possible in your authorizations.
3. Ensure that the authorization has the appropriate approvals:

a) Administrative and Technical Approvals are always required. These approvers must:
b) Ensure the principles of Least Privilege and Separation of Duties are applied.
ii. When approving privileges to a shared account consider everyone who has access to that account and whether such privilege is appropriate for everyone. Document it in a risk register.
c) All requests for access to systems must be approved by the Reporting Manager, Asset Owner & Infosec.
d) All requests for access to a system or application containing Restricted Use information have been approved by Information Security.

Privileged access may be granted permanently only if that specific person's job duties routinely require that level of access, otherwise, the access must be temporary.
5. All authorization requests must be documented, including the nature of the request, the time period for which it has been granted, all related approvals that were obtained, and the names of the approvers.

4.8 Deprovisioning

Systems and applications should be designed and deployed in a way that facilitates easy removal of a person's authorizations and accounts at appropriate times.

4.8.1 Centrally Managed Accounts and Authorizations

The enterprise level accounts or authorizations that are listed in the enterprise directory service and have authentication credentials in our enterprise authentication services shall be deprovisioned in accordance with the policies of our Identity and Access Management service, adhering to the principles that:

- Individuals with no affiliation with the Netradyne should not have an account.
- Accounts for individuals with no lasting associations with Netradyne, identified as affiliates within our IAM policies, should only exist for a limited period of time without reauthorization.

4.8.2 Non-Centrally Managed Accounts and Authorizations

When accounts or authorizations are created outside of the enterprise directory and/or enterprise authentication system, the unit creating the accounts must define a mechanism to deprovision the account in a timely fashion (generally within a few business days unless a specific time frame is requested) and consistent with the conditions expressed for centrally managed accounts.

NOTE: It is insufficient to rely on the central deprovisioning of accounts as a method of terminating locally deployed authorizations, as the timeliness of the account deprovisioning is dependent on a number of factors that are beyond the control of the local systems and application administrators.

4.9 Corporate System Access

Providing access to corporate systems is similar to application access - based on the principle of "least privilege" and "need to know". Additionally, employees are given access to systems based on managerial request and approval, NETRADYNE IT Operations and Security group approval, business/system owner approval, and in some cases, approval from HR. Access levels are reviewed on a quarterly basis to ensure accuracy and validity and these reviews are captured in the NETRADYNE IT Operations and Security group's ticketing system.

4.10 Logical Access Control

Logical access controls are placed on sensitive systems, information and critical applications used by NETRADYNE to perform information processing considered critical to NETRADYNE. All NETRADYNE systems have the ability to accommodate and enforce logical access restrictions. Control is exercised according to the principle of least privilege. System capability restrictions are usually stated in terms of "No access", "Read", "Create", "Modify", "Delete", and "Protected".

Accounts with elevated privileges, such as domain administrator and super-user accounts, are scrutinized and closely controlled and monitored to ensure such authorization is absolutely required to conduct an employee's role and responsibilities. All elevated accounts are reviewed on a quarterly basis.

4.11 Physical Access

1. Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
2. Physical access to all (Organization) restricted facilities must be documented and managed.
3. All **Information Resource** facilities must be physically protected in proportion to the criticality or importance of their function at Organization.
4. Access to **Information Resources** facilities must be granted only to Organization support personnel and contractors whose job responsibilities require access to that facility.
5. All facility entrances, where unauthorized persons could enter the premises, must be controlled.
6. Secure areas must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This includes:
    i. information processing facilities handling **confidential information** should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use.
    ii. controls should be adopted to minimize the risk of potential physical and environmental threats.
    iii. environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.
7. Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.
8. Equipment must be protected from power failures and other disruptions caused by failures in utilities.
9. All **Information Resources** facilities that allow access to visitors will track visitor access with a sign in/out log.
10. Card access records and visitor logs for **Information Resource** facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
11. Visitors in controlled areas of **Information Resource** facilities must be accompanied by authorized personnel at all times.
12. Personnel responsible for **Information Resource** physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

4.11.1 Access Cards

1. The process for granting card and/or key access to Information Resource facilities must include the approval of a member of the physical security committee.
2. Each individual that is granted access rights to an **Information Resource** facility must sign the appropriate access and non-disclosure agreements.
3. Access cards and/or keys must not be shared or loaned to others.
4. Access cards and/or keys that are no longer required must be returned to personnel responsible for **Information Resource** physical facility management. Cards must not be reallocated to another individual, bypassing the return process.
5. Lost or stolen access cards and/or keys must be reported to the person responsible for **Information Resource** physical facility management physical security committee as soon as possible.
6. Physical security committee must remove the card and/or key access rights of individuals that change roles within the Organization or are separated from their relationship with the Organization.
7. Physical security committee must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

4.12 User Access Review

Infosec conducts User Access review every quarter on all the critical assets/applications to minimize threats and provide assurance that the right people have the right access to critical asset(s) and infrastructure.

Infosec is responsible for ensuring that an audit trail of activity exists that includes the following:

1. Ensuring that any account or authorization created, deleted, removed, or changed is audited in a system of record and available for review. This log would contain proof of approvals for the creation, deletion, removal, or change and the system and any system or application-level log that the account or authorization was modified, if such can be logged.
2. Any system or application that authenticates or authorizes an account to take an action should log that activity to a standard location and format. The log should include both successful and failed authentications and authorizations.
3. Ensuring that the system or application audit logs are properly configured and function normally over time.
4. Conducting quarterly audits of account and authorization activity to ensure that only authorized use is occurring and maintain audit documentation accordingly. As part of this audit:
    a) Provide a list of accounts with privileged access to the appropriate management approvers for review.
    b) Support and encourage periodic review by Asset owners.

5 Logging & Monitoring:

All the centrally managed asset(s) logs are captured and logged through Azure Active Directory services and monitored by Security Operations centre. Log analytics & alerts are configured with the security tools and monitored by the SOC Team.

Information security incident management involves the detection and collection of information associated with and reporting on occurrences of information security events and the existence of information security vulnerabilities by manual or automatic means. In this phase, events and vulnerabilities might not yet be classified as information security incidents.

1. Monitor & log unauthorized access activity for the detection of any information security event.
2. Detect & report the event: Perform 24X7 monitoring & support to Detect and report the occurrence of an information security event or the existence of a threat, either manually through ITSM tool or by automated way through the monitoring systems
3. Collect additional details on the event or threat: Collect additional information on an information security event or threat identified. Any observation involving PII data will be immediately bring to the notice of Data Privacy Office for further investigation from DPO along with SIRT.
4. Collect situational awareness information: Collect situational awareness information from internal and external data sources including local system and network traffic and activity logs, external feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies.
5. Log all activities, results, and related decisions for future analysis.
6. Secure storage of the evidence: Secure the digital evidence gathered as part of this investigation and store/preserve in a secure way to retain and maintain the integrity of the evidence.
7. Escalate, on an as-needed basis throughout the phase, for further review or decisions.

Detailed Incident response process is documented and published at Netradyne Security Incident Response Plan

6 ISMS Policy Adherence

According to our ISMS policies, "Individuals are given only a level of authority and granted only those privileges and accesses necessary to successfully accomplish their assigned duties. Individuals are not allowed either functional or physical access to controlled areas or operations unless required by their duties and requested by their supervisor."
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 Asset owner. Non-compliance will be escalated to the Netradyne leadership team.

7 Exception

Information Security is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and the implementation of appropriate compensating controls followed by ND Information Security Exception process.

In addition, Information Security may publish directives aimed at clarifying the intent of a standard to aid in the interpretation of this policy.

8 Terms/Acronyms

Term/Acronym	Definition
I*AM*	Identity & Access Management
ND	Netradyne
ISMS	Information Security Management System
IT	Information Technology
S*IRT*	Security Incident Response Team
SOC	Security Operations Centre

8.1 References

8.1.1 Templates

Netradyne-Access_Control_matrix.xlsx (sharepoint.com)

8.1.2 Policies

Netradyne Information Security Policy & Procedure.pdf
Netradyne Information Security Exception Process.pdf
Acceptable Usage Policy.pdf

8.1.3 Process/Procedures

User Access review

Netradyne Security Incident Response Plan

4. 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