

AWS Identity & Access Management  
Procedural Document

v1.3

Internal and Confidential

Table of Contents

[AWS Identity & Access Management Procedural Document 0](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISO%2027001-Jul2024/INFOSEC/InfoSec2024/Infosec%20docs/InfoSec%20Docs/IAM_Docs/AWS%20IAM%20Procedural%20doc.docx#_Toc158740601)

[Document Control 2](#_Toc158740602)

[1 Purpose 2](#_Toc158740603)

[2 Scope 2](#_Toc158740604)

[3 Roles and Responsibilities 3](#_Toc158740605)

[4 Procedure 3](#_Toc158740606)

[4.1 Manual of authorities 3](#_Toc158740607)

[4.2 Account Types: 4](#_Toc158740608)

[4.2.1 User Accounts: 4](#_Toc158740609)

[4.2.2 Shared Accounts/Generic Accounts: 4](#_Toc158740610)

[4.2.3 Service Accounts: 4](#_Toc158740611)

[4.2.4 Privileged Accounts: 4](#_Toc158740612)

[4.2.5 Enterprise Directory Services: 5](#_Toc158740613)

[4.2.6 Centrally Managed Accounts: 5](#_Toc158740614)

[4.2.7 Non-centrally Managed Accounts 5](#_Toc158740615)

[4.3 User Access Provisioning Process: 5](#_Toc158740616)

[4.3.1 Single Sign On 6](#_Toc158740617)

[4.3.2 Credential generation from Programmatic access: 9](#_Toc158740618)

[4.4 Groups 10](#_Toc158740619)

[4.5 Roles: 11](#_Toc158740620)

[4.6 Policies: 11](#_Toc158740621)

[4.7 Least Privilege: 12](#_Toc158740622)

[4.8 Password Policy: 12](#_Toc158740623)

[4.9 Multi Factor Authentication: 13](#_Toc158740624)

[4.10 Security in AWS IAM 13](#_Toc158740625)

[4.11 Auditing 13](#_Toc158740626)

[5 ISMS Policy adherence: 14](#_Toc158740627)

[6 Exception 14](#_Toc158740628)

[7 Terms/Acronyms 14](#_Toc158740629)

[8 References 14](#_Toc158740630)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDAWSIAM2022001 |
| **Document Name** | Netradyne “AWS IAM Procedural document” |
| **Document Status** | Released |
| **Document Released Date** | 29-09-2022 |
| **Document Author** | Garima Bhatt <Garima.bhatt@netradyne.com> |
| **Document Content Contributors** | Garima Bhatt, Chethan Gangaraju, Roshan Mathews |
| **Document Signatory** | CISO <Saravanan.sankaran@netradyne.com> |
| **Document Owner** | Infosec <Infosec@netradyne.com> |
| **Document Version** | V1.3 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| V0.1 | 22-JUL-2022 | Initial version created | Garima Bhatt |
| V1.0 | 29-SEP-2022 | Document Released | Garima Bhatt |
| V1.1 | 08-AUG-2023 | Annual Review | Garima Bhatt |
| V1.2 | 08-FEB-2024 | Refined document as per data privacy requirements | Garima Bhatt |
| V1.3 | 03-FEB-2025 | Reviewed & revised the process documents | Garima Bhatt |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 29-SEP-2022 | Saravanan Sankaran | Sr. Director Infosec & IT | Approved |
| 29-SEP-2022 | Roshan Mathews | Sr. Director Engineering | Approved |
| 10-AUG-2023 | Saravanan Sankaran | Sr. Director Infosec & IT | Approved |
| 08FEB-2024 | Saravanan Sankaran | Sr. Director Infosec & IT | Approved |
| 05-FEB-2025 | Saravanan Sankaran | Sr. Director Infosec & IT | Approved |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| DevOps, IT Team | Netradyne |

# Purpose

This document is a **Netradyne** Procedural document to establish the requirements necessary to Identity & Access Management, administer access control in AWS environment to ensure that access to and use of AWS resources & data (PII/PHI) is managed in accordance with business requirements, information security requirements.

The organizational risk management strategy is a key factor in the development of the access control policy.

# Scope

The **Netradyne** IAM Procedural document applies to individuals who are responsible for managing AWS resource access & data (PII/PHI), and those grant/authorize access privileges, including special access privileges, to any AWS resources.

|  |  |
| --- | --- |
| **Intended Audience:** | DevOps, Infosec & IT |
| **Asset Used By:** | All Netradyne Users |
| **Asset Owned By:** | Roshan Mathews |
| **Owned By Department:** | DevOps/Infra |
| **Managed By Department:** | DevOps/Infra |
| **Control Implementer:** | DevOps/Infra |
| **Control Operator** | Infosec Team |
| **Security Officer:** | Saravanan Sankaran |
| **Access Provisioning Team:** | IT Team |

# 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. |

# Procedure

AWS Identity and Access Management (IAM) provides fine-grained access control across all of AWS resources and helps to securely control access the system, resources, application and data (PII/PHI). IAM is used to control who is authenticated (signed in) and authorized (has permissions) to use resources.

# Manual of authorities

|  |  |
| --- | --- |
| **Application Name:** | AWS |
| **Application Description:** | AWS |
| **Application Used By:** | Cloud, Analytics, Business Systems |
| **Application Owned By:** | Infra Team |
| **Owned By Department:** | Infrastructure |
| **Application Managed By:** | Infrastructure |
| **Managed By Department:** | Infrastructure |
| **Control Owner:** | Infrastructure |
| **Control Operator** | Infosec |
| **Security Governance:** | Infosec |
| **Access Provisioning/Deprovisioning Team:** | IT Team |

# Account Types:

# 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.

Each user is assigned a unique identifier, such as a username or employee ID, to ensure accountability and traceability. Unique identifiers are used for authentication and are tied to specific individuals within the organization.

# 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.

# 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.

# 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.

The allocation and use of privileged access rights shall be restricted and controlled. In order to connect to Netradyne systems for administrative activities, a user must authenticate through Netradyne permitted VPN (Virtual Private Network) which requires MFA (multi-factor authentication) or be on the Netradyne core network business.

# 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.

# 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.

# 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.

# User Access Provisioning Process:

User to submit the request as per the service catalogue template ensuring all the required information is updated.

1. User Line Manager to review the request details in ServiceDesk+ portal and then approve or reject the request.
2. If approved, Asset Owner to review the request details in ServiceDesk+ portal and then approve or reject the request. Should understand the purpose of requester for seeking access to your applications. Go to Step 3.
3. If rejected, Request gets cancelled.

1. Request for High-Privileged Role?

YES: If user has requested for high-privileged roles such as admin, the approval will be triggered to Infosec team. Infosec to review the request and then approve or reject as applicable. Go to Step 4.

NO: Go to Step 4.

1. IT team will review the request details & approval status and provision the access. Send mail confirmation & close the ticket in tool.

1. IT team will send confirmation & close the ticket.

Note: Rejection of the request from approvers at any level will lead to cancelling of the request. User should get clarification with approver who rejected & then submit new request

Diagram

Description automatically generated

# Single Sign On

To enhance security, SSO is implemented on all the critical applications in Netradyne. In order to login to AWS a user must follow below steps:

1. Users can login to AWS through [My Apps (microsoft.com)](https://myapps.microsoft.com/)
2. User will get below screen at first login, user need to enter his/her email credentials & password (Screenshot attached),

A screenshot of a computer

Description automatically generated

1. Once logged in, below screen will appear, click on AWS and you will be logged in directly to the AWS console.

A screenshot of a browser

Description automatically generated

1. Below console will appear with the AWS environment you have access to. Click on the management console to connect to that environment.

A screenshot of a computer

Description automatically generated

# Credential generation from Programmatic access:

 To configure both an IAM Identity Center profile and sso-session to your AWS CLI

1. Run the aws configure sso command and provide your IAM Identity Center start URL and the AWS Region that hosts the Identity Center directory.
2. $ aws configure sso   
   SSO session name (Recommended): my-sso   
   SSO start URL [None]: <https://my-sso-portal.awsapps.com/start>   
   SSO region [None]: us-east-1   
   SSO registration scopes [None]: sso:account:access
3. The AWS CLI attempts to open your default browser and begin the login process for your IAM Identity Center account.
4. Attempting to automatically open the SSO authorization page in your default browser.
5. If the AWS CLI cannot open the browser, the following message appears with instructions on how to manually start the login process.
6. If the browser does not open or you wish to use a different device to authorize this request, open the following URL:   
      
   <https://device.sso.us-west-2.amazonaws.com/>   
      
   Then enter the code:   
      
   QCFK-N451
7. IAM Identity Center uses the code to associate the IAM Identity Center session with your current AWS CLI session. The IAM Identity Center browser page prompts you to log in with your IAM Identity Center credentials. This gives permissions to the AWS CLI to retrieve and display the AWS accounts and roles that you are authorized to use with IAM Identity Center.
8. The AWS CLI displays the AWS accounts available for you to use. If you are authorized to use only one account, the AWS CLI selects that account for you automatically and skips the prompt. The AWS accounts that are available for you to use are determined by your user configuration in IAM Identity Center.
9. There are 2 AWS accounts available to you.   
   > DeveloperAccount, [developer-account-admin@example.com](mailto:developer-account-admin@example.com) (123456789011)    
     ProductionAccount, [production-account-admin@example.com](mailto:production-account-admin@example.com) (123456789022)
10. Use the arrow keys to select the account you want to use. The ">" character on the left points to the current choice. Press ENTER to make your selection.
11. The AWS CLI confirms your account choice, and displays the IAM roles that are available to you in the selected account. If the selected account lists only one role, the AWS CLI selects that role for you automatically and skips the prompt. The roles that are available for you to use are determined by your user configuration in IAM Identity Center.
12. Using the account ID 123456789011   
    There are 2 roles available to you.   
    > ReadOnly   
      FullAccess
13. Use the arrow keys to select the IAM role you want to use and press <ENTER>.
14. Specify the [default output format](https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.html#cli-config-output), the [default AWS Region](https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.html#cli-config-region) to send commands to, and providing a [name for the profile](https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.html) so you can reference this profile from among all those defined on the local computer. In the following example, the user enters a default Region, default output format, and the name of the profile. If you have a previously existing configuration, you can alternatively press <ENTER> to select any default values that are shown between the square brackets. The suggested profile name is the account ID number followed by an underscore followed by the role name.
15. CLI default client Region [None]: us-west-2<ENTER>   
    CLI default output format [None]: json<ENTER>   
    CLI profile name [123456789011\_ReadOnly]: my-dev-profile<ENTER>
16. A final message describes the completed profile configuration.
17. To use this profile, specify the profile name using --profile, as shown:   
       
    aws s3 ls --profile my-dev-profile
18. This results in creating the sso-session section and named profile in ~/.aws/config that looks like the following:
19. [profile my-dev-profile]   
    sso\_session = my-sso   
    sso\_account\_id = 123456789011   
    sso\_role\_name = readOnly   
    region = us-west-2   
    output = json   
       
    [sso-session my-sso]   
    sso\_region = us-east-1   
    sso\_start\_url = <https://my-sso-portal.awsapps.com/start>   
    sso\_registration\_scopes = sso:account:access
20. You can now use this sso-session and profile to request refreshed credentials. Use the aws sso login command to request and retrieve the credentials needed to run commands. For instructions, see [Use an IAM Identity Centre named profile](https://docs.aws.amazon.com/cli/latest/userguide/sso-using-profile.html)

# Groups

All access to the resources, application, or data (PII/PHI) is assigned through the Security groups created in Netradyne Azure Active Directory.

All the groups existing in our current environment are listed following.

|  |  |
| --- | --- |
| **Security Groups** | **Role assigned** |
| AWS-Analytics-Developers-Production | AzureADAWSSSO |
| AWS-Analytics-Devlopers-QA | AzureADAWSSSO |
| AWS-Analytics-Kinesis-Developers-Production | AzureADAWSSSO |
| AWS-Analytics-SuperUsers-Production | AzureADAWSSSO |
| AWS-Cloud-Developers-Production | AzureADAWSSSO |
| AWS-Cloud-Devops-Production | AzureADAWSSSO |
| AWS-Cloud-Hd-Maps-Production | AzureADAWSSSO |
| AWS-Cloud-Ingestion-Production | AzureADAWSSSO |
| AWS-Cloud-Integration-Production | AzureADAWSSSO |
| AWS-Cloud-IOT-Health-Production | AzureADAWSSSO |
| AWS-Cloud-Operations-Admin-Production | AzureADAWSSSO |
| AWS-Cloud-Operations-Production | AzureADAWSSSO |
| AWS-Cloud-QA-Production | AzureADAWSSSO |
| AWS-Cloud-SRE-Production | AzureADAWSSSO |
| AWS-Data-Products-Admin-Production | AzureADAWSSSO |
| AWS-Data-Products-Production | AzureADAWSSSO |
| AWS-Datascience-Production | AzureADAWSSSO |
| AWS-Device-Admins-Production | AzureADAWSSSO |
| AWS-Device-Build-Production | AzureADAWSSSO |
| AWS-Device-CAN-Production | AzureADAWSSSO |
| AWS-Device-Developers-Production | AzureADAWSSSO |
| AWS-Device-QA-Production | AzureADAWSSSO |
| AWS-Documentation Team-Production | AzureADAWSSSO |
| AWS-Finance-Cost-Explorer-Production | AzureADAWSSSO |
| AWS-Infosec-Production | AzureADAWSSSO |
| AWS-IT-Production | AzureADAWSSSO |
| AWS-Product-Success-Production | AzureADAWSSSO |
| David Julian | AzureADAWSSSO |
| Jenkins | AzureADAWSSSO |
| ML-Infra-Analytics | AzureADAWSSSO |

Managed By: DevOps Team

# Roles:

As a security best practice, ND follows IAM roles to provide credentials to the application. Roles can have their own set of permissions without any users/groups needing to be attached to them.

Netradyne employs a Role-Based Access Control (RBAC) framework to facilitate the secure management of access to the assets, systems & data. RBAC is a fundamental element of our information security strategy, promoting the principle of least privilege and ensuring that access rights align with job functions and responsibilities.

User access and Privilege access is granted and documented in [Role Based access control matrix](https://netorg726775.sharepoint.com/:x:/s/IT/EXpY9rmMvg1DpdmI6ezzB_UBAtQjvqzgnK4Mmz7kWuneQg?wdLOR=c73A5D5A2-F4FD-4D44-BD1A-A893CC1550E5) along with the access level.

Administrative access to Infra subscriptions and servers are restricted to appropriate personnel via Active Directory groups based on job responsibilities.

Managed By: DevOps Team

# Policies:

All the policies created in AWS are created around least privilege principle and governed by the security team. Access

To add permissions to an IAM identity (IAM user, group, or role), create a policy, validate the policy, and then attach the policy to the identity. Multiple policies can be attached to an identity, and each policy can contain multiple permissions.

Managed By: DevOps Team

* Policy Inheritance:  
  Access levels and associated IAM policies assigned in the C01 environment are inherited by both C03 and C04environments.
* Access Consistency:  
  There is no variation in access permissions across C01, C03, and C04. All users and roles retain the same privileges across these environments to maintain consistency in operations and governance.
* Policy Management:  
  IAM policies are centrally managed in C01. Any updates to access control (additions, modifications, or revocations) in C01 are automatically reflected in C03 and C04.

# Least Privilege:

As a security best practice, it’s important to regularly review organization’s AWS IAM policies to ensure they’re granting least privileges. Each policy should come with a [policy summary](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_understand.html), 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, application or data (PII/PHI), 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](#_Process/Procedures) 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.

# Password Policy:

Password policy should be uniform across the organization and aligned with ND password policy. All the end users are responsible for safeguarding their system access login and password credentials. 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.

**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.

Policy document is mentioned in [References](#_Password_Policy_document).

# Multi Factor Authentication:

Multi-Factor Authentication (MFA) is implemented to enhance the security of accessing the data (PII/PHI). Netradyne recognizes the importance of MFA in mitigating the risk of unauthorized access and ensuring the confidentiality and integrity of the security policies set forth for the organization. As a best practise, enabling MFA is a requirement for all the cloud services including AWS, that is being used at Netradyne.

# Security in AWS IAM

The following topics shows how to configure IAM to meet the best security and compliance objectives.

* [Lock away your AWS account root user access keys](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials)
* [Use roles to delegate permissions](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#delegate-using-roles)
* [Grant least privilege](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege)
* [Get started using permissions with AWS managed policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#bp-use-aws-defined-policies)
* [Validate your policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#best-practice-policy-validation)
* [Use customer managed policies instead of inline policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#best-practice-managed-vs-inline)
* [Use access levels to review IAM permissions](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-access-levels-to-review-permissions)
* [Configure a strong password policy for your users](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#configure-strong-password-policy)
* [Enable MFA](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users)
* [Use roles for applications that run on Amazon EC2 instances](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-roles-with-ec2)
* [Do not share access keys](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#sharing-credentials)
* [Rotate credentials regularly](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials)
* [Remove unnecessary credentials](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#remove-credentials)
* [Use policy conditions for extra security](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-policy-conditions)
* [Monitor activity in your AWS account](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#keep-a-log)

# Auditing

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

* 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.
* 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.
* Ensuring that the system or application audit logs are properly configured and function normally over time.
* 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:
  + Provide a list of accounts with privileged access to the appropriate management approvers for review.
  + Support and encourage periodic review by Asset owners.

Infosec conducts [User Access review](https://netorg726775.sharepoint.com/:b:/r/sites/InfosecInternal/Shared%20Documents/General/Identity%20%26%20Access%20Management/User%20access%20provisioning%20%26%20management/User%20Access%20review%20process%20flow%20v1.0.pdf?csf=1&web=1&e=FcOt3A) 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.

# 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.

# 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](https://netorg726775.sharepoint.com/sites/InfosecInternal/Shared%20Documents/Forms/AllItems.aspx?ga=1&id=%2Fsites%2FInfosecInternal%2FShared%20Documents%2FGeneral%2FRISK%20%26%20COMPLIANCE%20MANAGEMENT%2FEXCEPTION%20MANAGEMENT%2FNetradyne%20Information%20Security%20Exception%20Process%2Epdf&parent=%2Fsites%2FInfosecInternal%2FShared%20Documents%2FGeneral%2FRISK%20%26%20COMPLIANCE%20MANAGEMENT%2FEXCEPTION%20MANAGEMENT).

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

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| IAM | Identity & Access Management |
| AWS | Amazon Web Services |
| SCP | Service Control Policy |
| ACL | Access Control List |
| STS | Security Token Service |
| MFA | Multi Factor Authentication |
| SSO | Single Sign On |
| ISMS | Information Security Management System |

# References

## Templates

## [[Netradyne-Access\_Control\_matrix.xlsx (sharepoint.com)](https://netorg726775.sharepoint.com/:x:/s/IT/EXpY9rmMvg1DpdmI6ezzB_UBAtQjvqzgnK4Mmz7kWuneQg)](https://netorg726775.sharepoint.com/:x:/s/IT/EXpY9rmMvg1DpdmI6ezzB_UBAtQjvqzgnK4Mmz7kWuneQg)

## Policies

## [ND ISMS Policy](https://netorg726775.sharepoint.com/:w:/s/InfoSecDocumentGovernanceRepository/EWYAGXZpNKxLrwLuOWlgHCwBOVHMNgc_MeFFyjFajZ1dSw?e=faas1x)

## Process/Procedures

[**User Access Management v2.0.pdf**](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/ISMS_ISO27001_2013/ISMS_IT/IT%20Policy%20Documents/User%20Access%20Management%20v2.0.pdf?CT=1708424713504&OR=ItemsView)

**[User Access Review Process v1.0.pdf](https://netorg726775.sharepoint.com/:b:/s/InfosecInternal/EVjmnyW9oAJArvGiYbUJ-Z4BtDnM7ctHs7xwlwgARESlcQ?e=fbBZMt)**

## Exception Management Process

[**ND Information Security Exception Process v1.0**](https://netorg726775.sharepoint.com/sites/InfosecInternal/Shared%20Documents/Forms/AllItems.aspx?ga=1&id=%2Fsites%2FInfosecInternal%2FShared%20Documents%2FGeneral%2FRISK%20%26%20COMPLIANCE%20MANAGEMENT%2FEXCEPTION%20MANAGEMENT%2FNetradyne%20Information%20Security%20Exception%20Process%2Epdf&parent=%2Fsites%2FInfosecInternal%2FShared%20Documents%2FGeneral%2FRISK%20%26%20COMPLIANCE%20MANAGEMENT%2FEXCEPTION%20MANAGEMENT)

## Password Policy document

**[Password Management Policy document](https://netorg726775.sharepoint.com/:b:/s/InfosecInternal/EYvf3T51tvBPuL7oq6ugq98BsfNe17xiuiO0Z_HRtqVeIw?e=2ZU0iQ)**

# SOP

[Application\_Access\_Security\_Document\_AWS.docx](https://netorg726775.sharepoint.com/:w:/r/sites/InfoSecDocumentGovernanceRepository/_layouts/15/Doc.aspx?sourcedoc=%7BB51196FC-C700-4A36-811A-C38FDEA36F39%7D&file=Application_Access_Security_Document_AWS.docx&action=default&mobileredirect=true&CID=6cf8e4d6-15aa-609e-aac1-e49c932b4a64)

# 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 | A, C | - |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | A, R | 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 | R, C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |