

Internal and Confidential

Netradyne Information Security Control Framework (ISCF)

v1.0

[Netradyne Information Security Control Framework 0](https://netorg726775.sharepoint.com/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Previous%20Versions/Netradyne%20Information%20Security%20Control%20Framework%20(ISCF).docx#_Toc144999036)

[1 Purpose 3](#_Toc144999037)

[1.1 Confidentiality: 3](#_Toc144999038)

[1.2 Integrity: 3](#_Toc144999039)

[1.3 Availability: 3](#_Toc144999040)

[1.4 Authentication: 3](#_Toc144999041)

[1.5 Authorization: 3](#_Toc144999042)

[1.6 Audit and monitoring: 3](#_Toc144999043)

[1.7 Risk management: 3](#_Toc144999044)

[1.8 Compliance: 3](#_Toc144999045)

[1.9 Incident response: 3](#_Toc144999046)

[1.10 Education and awareness: 3](#_Toc144999047)

[1.11 Continual improvement: 3](#_Toc144999048)

[1.12 Cost-effectiveness: 4](#_Toc144999049)

[2 Scope 4](#_Toc144999050)

[2.1 Data Privacy & Security: 4](#_Toc144999051)

[2.2 Information Technology (IT) Systems & Communication Security: 4](#_Toc144999052)

[2.3 Identity & Access Management: 4](#_Toc144999053)

[2.4 Physical & Environmental Security: 4](#_Toc144999054)

[2.5 Information Security Policy and Procedure: 4](#_Toc144999055)

[2.6 Security Incident Management: 4](#_Toc144999056)

[2.7 Business Continuity and Disaster Recovery: 4](#_Toc144999057)

[2.8 Vendor and Third-Party Risk Management: 4](#_Toc144999058)

[2.9 Employee Training and Awareness: 4](#_Toc144999059)

[2.10 Compliance and Regulatory Requirements: 5](#_Toc144999060)

[2.11 Network Security: 5](#_Toc144999061)

[2.12 Endpoint Security: 5](#_Toc144999062)

[2.13 Cloud Security: 5](#_Toc144999063)

[2.14 Monitoring and Logging: 5](#_Toc144999064)

[2.15 Security Awareness and Training: 5](#_Toc144999065)

[2.16 Security Governance and Risk Management: 5](#_Toc144999066)

[2.17 Vulnerability & Patch Management: 5](#_Toc144999067)

[2.18 Encryption & Data Protection: 5](#_Toc144999068)

[3 Roles and Responsibilities 5](#_Toc144999069)

[4 Procedure 6](#_Toc144999070)

[4.1 Netradyne Information Security Control Framework 6](#_Toc144999071)

[4.1.1 Risk Management Framework 6](#_Toc144999072)

[4.1.2 Netradyne Information Security Control Framework (ISCF)- Stakeholders and Applicability 7](#_Toc144999073)

[4.1.3 Security domain wise control summary: 7](#_Toc144999074)

[4.1.4 Information Security Control Listing 8](#_Toc144999075)

[4.1.5 Revision/refinement of Security Controls 12](#_Toc144999076)

[5 Conduct 14](#_Toc144999077)

[6 Exception 14](#_Toc144999078)

[7 Terms/Acronyms 14](#_Toc144999079)

[8 References 15](#_Toc144999080)

[8.1 Templates 15](#_Toc144999081)

[8.2 Policies 15](#_Toc144999082)

[8.3 Process/Procedures 15](#_Toc144999083)

[8.4 Standards 15](#_Toc144999084)

[8.5 Miscellaneous 15](#_Toc144999085)

[9 Appendix A: Document RACI Matrix 16](#_Toc144999086)

**Document Control**

|  |  |
| --- | --- |
| **Document ID** | NDISCF2023001 |
| **Document Name** | Netradyne Information Security Control Framework |
| **Document Status** | Released |
| **Document Released Date** | 28-JUN-2023 |
| **Document Author** | Sudhansu Kumar |
| **Document Content Contributors** | Sudhansu Kumar |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Saravanan Sankaran |
| **Document Version** | 1.0 |
| **Information Classification** | Confidential |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| 1.0 | 26/JUN/2023 | Released Version | Sudhansu Kumar |
|  |  |  |  |
|  |  |  |  |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Netradyne/Signatory Title** | **Comments** |
| 28/JUN/2023 | Saravanan Sankaran | Senior Director - InfoSec & IT |  |
|  |  |  |  |
|  |  |  |  |

**Distribution of Final Document**

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

# Purpose

The purpose of information security control framework (ISCF) is to safeguard Netradyne's information assets and data from various threats and risks, ensuring the confidentiality, integrity, and availability of information. These controls are essential for protecting sensitive information, maintaining business continuity, and complying with legal and regulatory requirements. Here are the primary purposes of information security controls:

## Confidentiality:

Information security controls are designed to prevent unauthorized access to sensitive data. They ensure that only authorized individuals or systems can view or use certain information. This helps protect confidential data from being disclosed to unauthorized parties.

## Integrity:

Information must remain accurate and unaltered. Security controls help detect and prevent unauthorized modifications, tampering, or corruption of data. By ensuring data integrity, Netradyne can trust that their information remains reliable and trustworthy.

## Availability:

Information security controls aim to ensure that information is available when needed. This includes preventing disruptions due to cyberattacks, system failures, or natural disasters. Maintaining data and system availability is critical for business operations and continuity.

## Authentication:

Authentication controls verify the identity of individuals or systems attempting to access information or resources. This helps ensure that only legitimate users or devices gain access, reducing the risk of unauthorized access.

## Authorization:

Authorization controls determine what authorized users or systems are allowed to do with information or resources once they gain access. This helps enforce access permissions and restricts users from performing actions beyond their privileges.

## Audit and monitoring:

Security controls include mechanisms for monitoring and auditing activities related to information assets. These controls help Netradyne to detect and respond to security incidents, track access, and maintain accountability.

## Risk management:

Information security controls assist in identifying, assessing, and mitigating risks to information assets. They enable Netradyne to make informed decisions about resource allocation and risk reduction strategies.

## Compliance:

Netradyne has spread across multiple geographies and subjected to specific legal, regulatory, and industry-specific requirements related to information security. Security controls help ensure compliance with these standards and regulations.

## Incident response:

Controls facilitate the development of incident response plans and procedures to address security breaches, data breaches, or other security incidents promptly and effectively.

## Education and awareness:

Information security controls encompass training and awareness programs to educate employees and users about best practices, policies, and procedures related to information security.

## Continual improvement:

Security controls are part of a continuous improvement process. Netradyne tends to regularly assess its security posture, identify weaknesses, and implement enhancements to adapt to evolving threats and technologies.

## Cost-effectiveness:

Effective information security controls can reduce the financial impact of security breaches, data loss, and downtime, ultimately saving Netradyne from financial, informational, and reputational losses in the long run.

In summary, information security controls serve as a comprehensive framework for protecting Netradyne's information assets, managing risks, and ensuring compliance with various requirements. They are essential for maintaining trust, reputation, and the overall stability of Netradyne’s operations in an increasingly digital and interconnected world.

# Scope

The scope of information security controls in Netradyne is comprehensive and encompasses various aspects of the Netradyne's operations, processes, and technology. Here's an overview of the key areas and elements within the scope of information security controls in an Netradyne:

## Data Privacy & Security:

Information security controls cover all forms of data and information, including sensitive data, intellectual property, customer information, employee records, financial data, and any other critical information assets.

## Information Technology (IT) Systems & Communication Security:

These controls extend to the Netradyne's IT infrastructure, including networks, servers, workstations, databases, and software applications. IT security controls include firewalls, intrusion detection systems, antivirus software, and encryption.

## Identity & Access Management:

Controls ensure that only authorized individuals or systems have access to specific information or resources. Access control mechanisms include user authentication, role-based access control, and access permissions.

## Physical & Environmental Security:

Information security controls encompass physical security measures to protect office premises, data centres, server rooms, and other critical facilities from unauthorized access, theft, vandalism, and natural disasters.

## Information Security Policy and Procedure:

This involves the creation, documentation, and enforcement of security policies, standards, and procedures that guide employees and users on how to handle information securely.

## Security Incident Management:

Controls define the processes and procedures for responding to security incidents, breaches, or data leaks, including incident detection, reporting, and recovery.

## Business Continuity and Disaster Recovery:

Information security controls also include plans and strategies for ensuring business continuity in the event of disruptions, such as cyberattacks, Zone or Region wise failure, natural disasters, or equipment failures.

## Vendor and Third-Party Risk Management:

Netradyne need controls to assess and manage the security risks associated with third-party vendors, suppliers, and service providers who have access to their data or systems.

## Employee Training and Awareness:

Security controls encompass training programs to educate employees and raise awareness about security best practices, policies, and procedures.

## Compliance and Regulatory Requirements:

Netradyne must establish controls to meet legal, regulatory, and industry-specific compliance requirements related to information security, such as GDPR, CCPA, ISO 27001, ISO 27701, CIS, NIST SP 800 -53 etc.

## Network Security:

Controls are implemented to protect the Netradyne's network infrastructure, including firewalls, intrusion prevention systems, and network segmentation.

## Endpoint Security:

Security controls extend to endpoints, including laptops, desktops, mobile devices, and IoT devices, to protect against malware, data loss, and unauthorized access.

## Cloud Security:

As Netradyne majorly adopt cloud services, security controls cover cloud-based infrastructure, applications, and data to ensure they are secure and compliant.

## Monitoring and Logging:

Controls include systems for monitoring network and system activities, as well as collecting and analysing logs to detect and respond to security incidents.

## Security Awareness and Training:

Security controls encompass programs and initiatives to educate employees and users about security best practices, policies, and procedures.

## Security Governance and Risk Management:

The Netradyne must establish governance structures and processes for managing information security risks effectively.

## Vulnerability & Patch Management:

Regular security testing, vulnerability assessments, Patch Management and penetration testing are essential controls to identify and remediate security weaknesses.

## Encryption & Data Protection:

Controls for encrypting sensitive data both in transit and at rest to protect it from unauthorized access or exposure.

The specific information security controls and their scope can vary depending on the Netradyne's dynamic risk profile. A comprehensive and well-implemented information security program considers all these aspects to protect the Netradyne's information assets and maintain trust with stakeholders.

# 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

## Netradyne Information Security Control Framework (ISCF)

Netradyne Information Security Control Framework (ISCF), also known as Security Control Framework or Cybersecurity Framework, is a structured and organized set of policies, standards, procedures, and technical controls that an organization uses to manage and mitigate information security risks. Its primary purpose is to provide guidance and a systematic approach for safeguarding an organization's sensitive information, data, systems, and technology infrastructure. All controls are listed below. A few controls might not be applicable at present and marked accordingly, but going forward those controls might be relevant to Netradyne Dynamic risk profile.

On the Policy and Procedure front, Netradyne Information Security Control Framework is governed by [Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=gjHq5I) and other policies, processes and procedures mentioned in [Section 8](#_References) of this document.

Netradyne security control framework stems from Netradyne risk management framework.

### Risk Management Framework

It is a structured and systematic approach that Netradyne uses to identify, assess, manage, and mitigate risks across its various operations and activities.

Risk Management Framework aligned with Netradyne Business Objectives and provides a set of guidelines, processes, and tools that help to make informed decisions about how to deal with risks effectively.

In the below chart, key components and aspects of Risk Management Framework is demonstrated:



### Netradyne Information Security Control Framework (ISCF)- Stakeholders and Applicability

A summarized, function wise overview of applicability and responsibilities of ISCF for FY 2023 are provided below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Function** | **ISMS SPOC(s)** | **Functional Owner** | **Risk Owner** | **Applicable controls** |
| [BUSINESS SYSTEM](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#BusinessSystem_SoA!A1) | Robin Mahto; Sam Kang (For Salesforce Only) | Nagarjuna Cherukuri | Vinay Rai | 30 |
| [CLOUD](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#Cloud_SoA!A1) | Gaurav Agarwal | Ankit Srivastava | Vinay Rai | 15 |
| [DEVICE](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#Device_SoA!A1) | Ajay Kamath | Subba Rao | Teja Gudena | 27 |
| [FINANCE](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#Finance_SoA!A1) | Priyesh Tripathi; Mihir Parekh | Ashwin Kumar | Ashwin Kumar | 18 |
| [HR & ADMIN](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#RANGE!A1) | Ranjini Shetty; Harsha Vishwanath, Bijesh Sudharma | Pooja Madappa | Pooja Madappa | 31 |
| [INFRA](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#INFRA_SoA!A1) | Sudharsan S., Soham C. | Roshan M | Vinay Rai | 47 |
| [IT](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#IT_SoA!A1) | Chethan G., Mauricio T | Saravanan Sankaran | Vinay Rai | 50 |
| [PRODUCT MANAGEMENT](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#ProductManagement_SoA!A1) | Arun Lal | Arun Lal | Pramod Akkarachittor | 12 |
| [PRIVACY](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#Privacy_SoA!A1) | Shivesh Ranjan | Shivesh Ranjan | Michael Campos | 16 |
| [INFOSEC](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#InfoSec_SoA!A1) | Rajeev Ghosh, Garima Bhatt, Gautam Kumar | Saravanan Sankaran | Vinay Rai | 65 |
| [LEADERSHIP](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#Leadership_SoA!A1) | Vinay Rai,  Pooja Madappa, Teja Gudena, Ashwin Kumar, Michael Campos | Avneesh Agarwal | Avneesh Agarwal | 8 |
| [ANALYTICS](file:///C:/Users/sudhansuk/AppData/Local/Microsoft/Windows/INetCache/Content.MSO/B3FF1FDB.xlsx#Analyitics_SoA!A1) | Hisham | Pratik Verma, Suresh Kumar Yerakaraju | Sreekanth Annapureddy | 42 |

### Security domain wise control summary:

|  |  |  |
| --- | --- | --- |
| **Security Domains** | **Domain Notation** | **#Controls** |
| Acceptable Use Policy | AUP | 1 |
| Asset Management | AM | 3 |
| Business Continuity/Disaster Recovery | BCDR | 4 |
| Capacity Management | CP | 1 |
| Change/Configuration Management | CM | 9 |
| Data Privacy | DP | 7 |
| Encryption & Data Protection | EDP | 3 |
| Governance, Risk & Compliance | GRC | 9 |
| Human Risk Management | HRM | 5 |
| Identity & Access Management | IAM | 9 |
| Monitoring | LM | 5 |
| Network Security | NS | 3 |
| Physical & Environmental Security | PES | 1 |
| Security Incident Management | IR | 2 |
| Supplier Relationship | SR | 2 |
| Vulnerability & Patch Management | PVM | 2 |
| **Grand Total** |  | **66** |

### Information Security Control Listing

| **Control\_ID** | **Control Description** | **Applicability** | **Notation** | **Security Domain** | **ISO 27001:2013** |  |
| --- | --- | --- | --- | --- | --- | --- |
| NDIS001 | Netradyne identifies, inventories, classifies, and manages assets inventory (Software's, hardware's, Certificates and Licenses etc.). It should be updated upon installation or removal of assets in the production environment. Procedures are established to review the asset inventory for its currency and correctness on a periodic basis. | Yes | AM | Asset Management | A.8.1.1 |  |
| NDIS002 | Assets within the Netradyne environment have a designated owner who is responsible for asset classification and protection in accordance with classification. Assets are labelled and classified as per its significance. | Yes | AM | Asset Management | A.8.1.2 A.8.2.1 A.8.2.2 |  |
| NDIS003 | Assets/Servers are decommissioned via a documented process. The request, approval, and resulting actions are documented. The decommissioning process is tracked and documented in ServiceDeskPlus. | Yes | AM | Asset Management | A.8.1.4 A.8.2.3 A.8.3.2 A.11.2.7 |  |
| NDIS004 | Netradyne has documented policies and procedures that establish what is expected and required of its employees. These AUPs are available to all employees. Personnel are required to read and accept the code of conduct and the statement of security and confidentiality practices upon their hire and to formally reaffirm them annually thereafter. | Yes | AUP | Acceptable Use Policy | A.8.1.3 A.12.1.1 A.7.1.2 |  |
| NDIS005 | Netradyne annually performs a tabletop exercise where top threat scenarios are selected, and Senior Leadership executes the Business Continuity Plan to practice scenarios that could impair Netradyne's ability to recover from various incidents. | Yes | BCDR | Business Continuity/Disaster Recovery | A.17.1.3 |  |
| NDIS007 | Business continuity test plans for infrastructure systems are scoped, and the problems identified are documented and have an associated remediation action. Testing is performed on an annual basis of the BCP or DR plan. | Yes | BCDR | Business Continuity/Disaster Recovery | A.17.1.1 |  |
| NDIS008 | Netradyne system disaster recovery plan is implemented and maintained. Recovery Time Objectives (RTOS) and Recovery Point Objectives (RPOS) are established and monitored based on client requirements pursuant to compliance with the DR/BCP Plan. | Yes | BCDR | Business Continuity/Disaster Recovery | A.17.1.2 A.17.1.3 |  |
| NDIS009 | Backups are scheduled and monitored for successful replication for critical system components in alternative cloud storage location based on business requirements. | Yes | BCDR | Business Continuity/Disaster Recovery | A.12.3.1 A.17.2.1 |  |
| NDIS012 | Secure systems configuration/hardening standards are defined, approved for each server, and workstation operating system used within the system. Any exception to standard baseline configuration shall be authorized following change management policies and procedures prior to deployment, provisioning, and use. | Yes | CM | Change/Configuration Management | A.12.1.2 A.13.1.2 A.14.2.4 |  |
| NDIS013 | A standard build is used for all personnel laptops which includes software, firewall, anti-virus software, anti-spyware software, encryption software, backup software, DLP software, and software distribution tool to apply the most recent approved Operating System patches. | Yes | CM | Change/Configuration Management | A.13.1.2 A.14.2.4 |  |
| NDIS014 | The production environment is logically segregated from the non-production environments. One primary function per server/VM is implemented in production environment to prevent functions that require different security levels from co-existing on the same server | Yes | CM | Change/Configuration Management | A.12.1.4 |  |
| NDIS015 | Changes that affect system user responsibilities or the entity's commitments and requirements relevant to the security and availability of the environment are communicated to the impacted internal and external users via email or other means in a timely manner. | Yes | CM | Change/Configuration Management | A.12.1.2 |  |
| NDIS016 | Information systems are configured to provide access to only specific ports and services | Yes | CM | Change/Configuration Management | A.13.1.2 A.14.2.4 A.15.1.3 |  |
| NDIS017 | A formal change request process is in place, and change requests are documented, tested in a lower environment, and approved prior to implementation. Formal documentation of testing and CAB approval for environment wide changes is documented in post implementation. | Yes | CM | Change/Configuration Management | A.12.1.2 |  |
| NDIS018 | Access to implement changes to the production environment is restricted. Permission to install software in production environment shall be tightly controlled and govern by least privilege principle | Yes | CM | Change/Configuration Management | A.9.2.3 A.12.1.2 |  |
| NDIS019 | Production cloud hosted deployments are subjected to an established and enforced secure development lifecycle methodology which are aligned with DevSecOps requirements | Yes | CM | Change/Configuration Management | A.14.2.6 |  |
| NDIS020 | Security, firmware, or service patches are tested and approved prior to implementation in a production environment (Cloud Resources or Endpoints) and are applied within three months of issue by the vendor. | Yes | CM | Change/Configuration Management | A.14.2.2 A.14.2.9 |  |
| NDIS021 | Network should be scanned for rogue devices and network capacity is monitored on an ongoing basis by the Netradyne Network Operations Center | Yes | CP | Network Security | A.12.1.3 |  |
| NDIS022 | Future processing demand is forecasted and compared to existing infrastructure. Adequate measures shall be taken for Netradyne to auto scale/de-scale the resources. | Yes | CP | Capacity Management | A.12.1.3 |  |
| NDIS023 | Engagement and client data should not be stored on the CDN | Yes | DP | Data Privacy |  |  |
| NDIS025 | Netradyne engagement data is restricted from processing or transfer outside the geo where the engagement is hosted or as per the contractual obligations with Client(s) | Yes | DP | Data Privacy |  |  |
| NDIS026 | Sensitive Information/PII must not be stored in log files or meta data. In case of storage, it should be masked/anonymized or protected by suitable measures. | Yes | DP | Data Privacy |  |  |
| NDIS027 | PRIVACY Policy and procedures are established; Supported business processes, roles and responsibilities & technical measures are implemented for the protection of personally identifiable information (PII) as required by applicable legislation and regulation where applicable. | Yes | DP | Data Privacy | A.12.4.2 A.18.1.3 |  |
| NDIS028 | A Data privacy risk management process is in place to assess the privacy risk in accordance with applicable laws or any existing organizational policy and procedure. | Yes | DP | Data Privacy |  |  |
| NDIS029 | Netradyne cloud hosted environment is designed to support privacy by automating privacy controls. | Yes | DP | Data Privacy |  |  |
| NDIS030 | A defined data life cycle exists providing guidance for : -Data Type -Who can access data -Who can access data within the application -Who can delete the data on request -Who can transfer the data | Yes | DP | Data Privacy | A.7.1.2 A.13.2.4 |  |
| NDIS032 | Policies and processes shall be established, and supporting business processes and technical measures implemented for defining and adhering to data retention period(s) as per established procedures as well as applicable legal, statutory, or regulatory compliance obligations | Yes | EDP | Encryption & Data Protection | A.9.4.5 |  |
| NDIS033 | Processes are in place for cryptographic controls in order to implement encryption for data at rest and in motion. Keys are stored/managed securely and rotated on a periodic basis using a secured repository. | Yes | EDP | Encryption & Data Protection | A.10.1.1 A.10.1.2 |  |
| NDIS034 | Traffic between end users and the Cloud environment is encrypted using a protocol that is authorized in accordance with Netradyne policy. | Yes | EDP | Encryption & Data Protection | A.13.2.1 A.13.2.2 |  |
| NDIS038 | Netradyne communicates its objectives and changes to objectives (i.e., technology changes, leadership changes, policy changes, etc.) through various channels such as a post on NetradyneNet and/or email. | Yes | GRC | Governance, Risk & Compliance | A.5.1.1 A.7.3.1 |  |
| NDIS042 | Risk assessment/Audits are performed periodically either by internal or external parties to identify risks and associated mitigation strategies, including controls. Relevant information resulting from InfoSec/Privacy assessments conducted by internal/external parties is communicated to management on a periodic basis. | Yes | GRC | Governance, Risk & Compliance | A.6.1.5 A.15.1.2 A.18.2.1 A.18.2.3 |  |
| NDIS043 | A risk governance framework is defined and established, maintained, and reviewed for accuracy and completeness against applicable regulatory requirements. The framework includes maturity scopes, identified risks across the environment, and controls that help mitigate those risks. These controls are designed and implemented based on applicable regulatory requirements and to achieve management objectives. The framework should also include a risk governance plan, risk policy and procedures, business assets to be evaluated, threat types, risk training, and risk evaluation criteria. | Yes | GRC | Governance, Risk & Compliance | A.6.1.5 A.11.1.2 A.14.1.1 A.15.1.2 A.18.2.2 A.18.2.3 |  |
| NDIS046 | Information security and related policies are defined, established, maintained, reviewed by the InfoSec group, and revised annually. | Yes | GRC | Governance, Risk & Compliance | A.5.1.2 |  |
| NDIS048 | Netradyne's Information Security Management Systems (ISMS) is reviewed by an independent firm for ISO 27001 certification. | Yes | GRC | Governance, Risk & Compliance | A.18.2.1 |  |
| NDIS050 | Netradyne Leadership has defined its organizational structure, reported lines, authorities, roles, and responsibilities and evaluated them on a periodic basis. | Yes | GRC | Governance, Risk & Compliance | A.5.1.1 A.5.1.2 A.6.1.1 |  |
| NDIS051 | Documentation of the system boundaries and the system description is available to authorized users via the internal site and communicated to external users via the SOW. | Yes | GRC | Governance, Risk & Compliance | A.5.1.1 A.6.1.5 |  |
| NDIS053 | Written processes and procedures for operations, security, and availability processes are provided to personnel responsible for the operation of the system. | Yes | GRC | Governance, Risk & Compliance | A.5.1.1 A.7.2.2 A.12.1.1 |  |
| NDIS054 | During an onboarding meeting, customers are provided policies and procedures that include how customers report issues, failures, and incidents, including security and availability, etc. through online support forms and/or their regular Netradyne representative. | Yes | GRC | Governance, Risk & Compliance | A.7.1.2 A.14.2.7 A.15.1.2 |  |
| NDIS058 | Minimum education and prior work experience is documented as part of the hiring requirements for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting Organization InfoSec posture. | Yes | HRM | Human Risk Management | A.7.1.2 |  |
| NDIS059 | Background investigation policy includes verification of identity, employment, education, and criminal record. | Yes | HRM | Human Risk Management | A.7.1.1 |  |
| NDIS060 | The entity's code of conduct outlines guidelines for personnel who violate the code of conduct. | Yes | HRM | Human Risk Management | A.7.2.3 |  |
| NDIS062 | Contracted employees are required to sign an NDA which establishes standards of conduct related to confidentiality, privacy, PII and disclosure of such information. | Yes | HRM | Human Risk Management | A.7.1.2 A.13.2.4 |  |
| NDIS063 | Netradyne provides Security Awareness, compliance, and role-based training opportunities to employees on a periodic basis. New hires undergo security awareness training within 90 days of hiring. Employees have certain mandatory training requirements that are monitored on an ongoing basis. | Yes | HRM | Human Risk Management | A.7.2.2 |  |
| NDIS064 | In order to obtain remote network access, the connecting workstation must: -be a recognized Netradyne laptop (for Netradyne employees) or pass a security scan (for Vendors or Contractors), and -authenticate using multi-factor authentication with a valid user ID that belongs to Netradyne's permitted Active Directory, password, and enter a code that the user receives from a text message or a mobile application. | Yes | IAM | Identity & Access Management | A.9.4.2 A.6.2.2 |  |
| NDIS065 | Authentication credentials transmitted to network devices are encrypted in transit. | Yes | IAM | Identity & Access Management | A.9.2.4 A.14.1.2 |  |
| NDIS066 | An approval process is established to provision appropriate and required access to new users to the authorized Endpoint, Infra subscriptions and servers. | Yes | IAM | Identity & Access Management | A.9.2.1 A.9.2.2 |  |
| NDIS068 | 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 | Yes | IAM | Identity & Access Management | A.9.2.3 A.9.1.2 A.9.4.4 A.13.1.1 |  |
| NDIS069 | Access to the Netradyne's environment is authenticated through unique user IDs and passwords. Password parameters are in conformity with Information Security password policies and standards (e.g., password for minimum length, complexity, and account lockout). | Yes | IAM | Identity & Access Management | A.9.4.1 A.9.4.2 A.9.4.3 |  |
| NDIS070 | The security policy requires that user's Endpoint access, Infra/App subscriptions, and server access is removed upon termination of employment or job transfer, on the same day. | Yes | IAM | Identity & Access Management | A.7.3.1 A.9.2.2 A.9.2.6 |  |
| NDIS071 | 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. | Yes | IAM | Identity & Access Management | A.9.1.1 A.9.2.3 |  |
| NDIS072 | An annual review of users with access to endpoints/Cloud Infra/resources and server occurs to confirm that access to the Netradyne's resources is restricted to authorized personnel only | Yes | IAM | Identity & Access Management | A.9.2.5 |  |
| NDIS073 | Administrative access to Infra subscriptions and servers is restricted to appropriate personnel via Active Directory groups based on job responsibilities. | Yes | IAM | Identity & Access Management | A.9.1.2 |  |
| NDIS075 | Information security incident management policy is maintained, reviewed within 12 months (contains revision history), approved, includes organization structure, response procedures, timelines for incident resolution, communication of incidents, and changes to the system follow the established change management policy. | Yes | IR | Security Incident Management | A.5.1.1 A.12.1.2 A.16.1.1 |  |
| NDIS076 | The Operations team performs monitoring, including documentation, classification, escalation, coordination, and resolution of incidents per documented procedures. | Yes | IR | Security Incident Management | A.16.1.1 A.16.1.2 A.16.1.4 |  |
| NDIS078 | Administrative activity performed on Cloud resources is logged, monitored, and alerted based on a defined ruleset. | Yes | LM | Monitoring | A.12.4.1 A.12.4.3 A.16.1.1 |  |
| NDIS079 | Systems are monitored for availability on an ongoing basis through automated alerting, and corrective action is implemented in a timely manner. | Yes | LM | Monitoring | A.12.1.3 |  |
| NDIS080 | Intrusion Prevention Systems (IPS) are in place and are updated with the latest rule set on a regular basis (at least weekly). | Yes | LM | Monitoring | A.13.1.2 |  |
| NDIS081 | Anti-Malware/EDR solutions are installed and updated on a regular basis. | Yes | LM | Monitoring | A.12.2.1 |  |
| NDIS082 | Events are logged and monitored by the Security Operations Center (SOC). Logs are securely stored at a centralized location for a predefined period as applicable by compliance or contractual requirements. | Yes | LM | Monitoring | A.12.4.1 A.12.4.2 A.16.1.1 |  |
| NDIS084 | A network diagram is documented and shows the relevant network segmentation and points of access. | Yes | NS | Network Security | A.13.1.1 A.13.1.3 |  |
| NDIS085 | Firewalls are in place to prevent unauthorized access to the network. New firewall rules or changes to existing firewall rules are reviewed and approved prior to implementation. | Yes | NS | Network Security | A.6.2.2 A.13.1.2 A.13.1.3 |  |
| NDIS086 | Vulnerability Assessments/Penetration Tests are conducted periodically on Infrastructure, Application, APIs, and Devices to detect new and unremediated vulnerabilities. Relevant stakeholders should research and remediate "Critical," "High" or "Medium" rated vulnerabilities within the prescribed timeline. | Yes | PVM | Vulnerability & Patch Management | A.12.6.1 |  |
| NDIS087 | Vulnerability Management Process is defined and established and identified vulnerabilities are remediated as per the prescribed timeline. Periodic cadence shall be established by the InfoSec team with relevant stakeholders to review, track and close the pending vulnerabilities. | Yes | PVM | Vulnerability & Patch Management | A.12.6.1 |  |
| NDIS088 | Netradyne has established and assigned responsibility and accountability for the management of vendor/third party risks. Additionally, based upon completed impact assessments, the InfoSec team performs corresponding 3rd party security assessments, audits, and monitoring. Security reassessments for contracted vendors is performed based on criticality of engagement. | Yes | SR | Supplier Relationship | A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A. 15.2.2 |  |
| NDIS089 | Vendor/Third party compliance requirements, service levels, privacy, and confidentiality requirements are written into the contract with the vendor as necessary based on the service provided. Standard contract templates are used for third party vendors and deviations from those are reviewed and approved by key stakeholders (Legal/Business) | Yes | SR | Supplier Relationship | A.15.1.2 |  |
| NDIS090 | Controls are defined and implemented for unauthorized physical access, damage and interference to the organization's information and information processing facilities. This includes Physical entry controls, securing offices and facilities, protection against external and environmental threats, secure disposal & reuse, clear desk, and clear screen policy etc. | Yes | PES | Physical & Environmental Security | A.11.1 A.11.2 |  |

### Revision/refinement of Security Controls

Security controls should be regularly reviewed and revised to adapt to changing threats, technologies, and organizational needs. Here are some common scenarios that may necessitate revisions to security controls:

#### New Threats and Vulnerabilities:

As new cyber threats and vulnerabilities emerge, security controls should be updated to address these specific risks. Regular threat assessments and vulnerability scans can help identify these changes.

#### Regulatory Changes:

Laws and regulations related to data protection and cybersecurity often evolve. When these regulations change, security controls must be adjusted to ensure compliance.

#### Technological Changes:

The adoption of new technologies or changes in existing ones (e.g., cloud computing, IoT, mobile devices) can introduce new security challenges. Security controls may need to be updated to secure these technologies effectively.

#### Incident Response Improvements:

After experiencing a security incident, Netradyne should review its security controls to identify weaknesses and gaps. Lessons learned from incidents can lead to control enhancements.

#### Business Process Changes:

If Netradyne will undergoes significant changes in its business processes or IT infrastructure, security controls shall be reassessed to align with potential changes.

#### Third-Party Relationships:

Netradyne relies on third-party vendors or partners for services or data handling, security controls should be reviewed to ensure these relationships don't introduce additional risks.

Employee Turnover:

High turnover or changes in staff responsibilities can result in security controls becoming outdated or misconfigured. Regular training and access reviews can help mitigate this risk.

#### Advanced Persistent Threats (APTs):

If there are signs of persistent and advanced threats targeting Netradyne, it may be necessary to revise security controls to better defend against those sophisticated attacks.

#### Security Audit Findings:

Security audits and assessments may uncover weaknesses or deficiencies in existing controls. Netradyne should address these findings promptly by revising controls as necessary.

#### Budget Constraints:

Changes in budget allocations can impact the ability to maintain or upgrade security controls. Netradyne shall find ways to balance budget constraints with the need for effective security.

#### Emerging Technologies:

The adoption of emerging technologies such as artificial intelligence, blockchain, or quantum computing can require new security controls to address their unique risks.

#### Data Privacy Concerns:

Growing concerns about data privacy, such as the implementation of GDPR (General Data Protection Regulation) and similar laws, may require the revision of controls periodically to protect sensitive data.

#### Security Control Maturity:

Netradyne security controls are governed by its Risk management framework where maturity is the predominant consideration in its security posture, it may need to upgrade or enhance controls to meet higher standards or compliance requirements.

#### User Feedback:

Soliciting feedback from end-users from different functions can provide insights into security control effectiveness. Issues or concerns raised by users should prompt reviews and possible revisions.

#### Security Breaches:

In case of experiencing any security breach, it's critical to revise security controls to prevent similar incidents in the future and to address any lessons learned.

#### Business Growth:

Rapid business growth can lead to changes in the threat landscape and require adjustments to security controls to accommodate increased data and Netradyne’s system complexity.

Regular security assessments, risk assessments, and continuous monitoring are essential components of a comprehensive security program. By staying vigilant and responsive to these scenarios, Netradyne can maintain effective security controls and better protect their assets and data.

# Conduct

Compliance Checks to Information Security Control Framework 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 Information Security Control Framework must be approved through the Netradyne Exception Management Process. Any deviation in remediation/deployment timeline shall be approved as an exception with proper justifications and recorded in Netradyne Risk Register.

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 or Mitigation is practically not possible within the prescribed duration To request a security exception, contact the InfoSec team. Below are the examples of exceptions:

* Patching on Production systems like GPU machines hosted in our data centre may require complex testing and installation procedures
* Deviations from normal patch schedules shall require authorization from IT & InfoSec Head
* Inability to remediate a vulnerability due to lack of solution
* Patch/Remediation are not feasible with application and business requirements
* Special access permission needed on valid reasons
* Business requirements are on conflict with Netradyne Information Security Policy and exception needed

For any exception in Information Security Process on valid reasons, approvals are needed from System Owner (First Level) and InfoSec Head (Second Level)

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| **Resources** | include computing, networking, communications, application, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services. |
| **ISCF** | Netradyne Information Security Control Framework |
| **Production Environment** | This is commonly used for any live environment in Netradyne e.g. SaaS Hosting, Netradyne Products used by our partners, SaaS products used by Netradyne, Netradyne Internal System Managed by IT Team etc. *(In future Patch & Vulnerability Management Procedure document will be more refined and dedicated procedures will be added to different type of production environment(s) as mentioned above.)* |
| **Patch** | is a software update comprised of code inserted (i.e., patched) into an executable program code. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited, to the following:   * Upgrading software * Fixing a software bug * Installing new drivers * Addressing security vulnerabilities * Addressing software stability issues |
| **Remediation** | is an effort that resolves or mitigates a discovered vulnerability. |
| **Vulnerability** | is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. |
| **Vulnerability management** | is the practice of identifying, classifying, remediating, and mitigating vulnerabilities. |
| **DL** | Distribution List |
| **ND** | Netradyne |

# References

## Templates

[NetradyneDocumentationTemplate\_v1.0.dotx](https://netorg726775.sharepoint.com/:w:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NetradyneDocumentationTemplate_v1.0.dotx?d=w15edb35bf0bd47b39b325132e1ab95fb&csf=1&web=1&e=IjO5cq)

[Netradyne TPRM Preliminary Assessment Accelerator\_v1.1.xlsx](https://netorg726775.sharepoint.com/:x:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20TPRM%20Preliminary_Assessment%20Accelerator_v1.1.xlsx?d=w46ab396527c54f1fbbb32abf02229f88&csf=1&web=1&e=hUSAFe)

[ISMS\_RiskRegister\_MASTER.xlsx](https://netorg726775.sharepoint.com/:x:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/General/RISK%20REGISTER%202022/ISMS_RiskRegister_MASTER.xlsx?d=w41fe8cc8e11b46488cafb429c940b19a&csf=1&web=1&e=bPA1LK)

## Policies

[Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=gjHq5I)

[Personal\_Data\_Protection\_Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Personal_Data_Protection_Policy.pdf?csf=1&web=1&e=J83cFd)

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=VhC3aG)

[NetradyneOpen-SourceSecurityPolicy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NetradyneOpen-SourceSecurityPolicy.pdf?csf=1&web=1&e=w4ASdk)

[Netradyne Information Technology Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20Information%20Technology%20Policy.pdf?csf=1&web=1&e=5989Lb)

[Cryptography Standards Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Cryptography%20Standards%20Policy.pdf?csf=1&web=1&e=01bAeq)

## Process/Procedures

[Netradyne Vulnerability & Patch Management Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20Vulnerability%20%26%20Patch%20Management%20Process.pdf?csf=1&web=1&e=J15BVF)

[NETRADYNE BUSINESS CONTINUITY PLAN.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NETRADYNE%20BUSINESS%20CONTINUITY%20PLAN.pdf?csf=1&web=1&e=OFEVZj)

[NETRADYNE DISASTER RECOVERY PROCESS.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NETRADYNE%20DISASTER%20RECOVERY%20PROCESS.pdf?csf=1&web=1&e=Qluqs9)

[Netradyne Information Security Exception Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20Information%20Security%20Exception%20Process.pdf?csf=1&web=1&e=mKM5sw)

[Netradyne Antimalware Crowdstrike Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20Antimalware%20Crowdstrike%20Procedure.pdf?csf=1&web=1&e=YYHVxv)

[Netradyne SOP Malware Analysis.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Netradyne%20SOP%20Malware%20Analysis.pdf?csf=1&web=1&e=uOcOhp)

[NetradyneSecurityIncidentResponsePlan.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NetradyneSecurityIncidentResponsePlan.pdf?csf=1&web=1&e=4CelNO)

[Third Party Risk Management.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/Third%20Party%20Risk%20Management.pdf?csf=1&web=1&e=aakiV3)

## Standards

## Miscellaneous

[InfoSec\_RiskRegisterOverview\_Mar2023.pptx](https://netorg726775.sharepoint.com/:p:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/General/RISK%20REGISTER%202022/InfoSec_RiskRegisterOverview_Mar2023.pptx?d=wbcce57dd921d482e936efd803156f009&csf=1&web=1&e=PaOr48)

# 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 |