

Internal and Confidential

Table of Contents

[Document Control 2](#_Toc106061611)

[1 Purpose 3](#_Toc106061612)

[2 Scope 3](#_Toc106061613)

[3 Roles and Responsibilities 3](#_Toc106061614)

[4 Procedure Error! Bookmark not defined.](#_Toc106061615)

[4.1 Exception Process Flow: 5](#_Toc106061616)

[5 Conduct 5](#_Toc106061617)

[6 Exception 6](#_Toc106061618)

[7 Terms/Acronyms 6](#_Toc106061619)

[8 References 6](#_Toc106061620)

[8.1 Exception Request Form **Error! Bookmark not defined.**](#_Toc106061621)

[8.2 Exception Tracker **Error! Bookmark not defined.**](#_Toc106061622)

[8.3 Policies 6](#_Toc106061623)

[8.4 Process/Procedures **Error! Bookmark not defined.**](#_Toc106061624)

[8.5 Standards **Error! Bookmark not defined.**](#_Toc106061625)

[8.6 Miscellaneous **Error! Bookmark not defined.**](#_Toc106061626)

[9 Appendix A: Document RACI Matrix 7](#_Toc106061627)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDEM2022001 |
| **Document Name** | Netradyne Exception Management Process |
| **Document Status** | Released |
| **Document Initial Release Date** | 04-AUG-2022 |
| **Document Author** | InfoSec |
| **Document Content Contributors** | Kavitha Shetty; Sudhansu Kumar; Vijaykumar Dalal, Garima Bhatt |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Infosec |
| **Document Version** | V2.0 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| 1.0 | 04-AUG-2022 | Incorporated the process flow | Infosec |
| 1.1 | 30-JUN-2023 | Annual Review | Sudhansu Kumar |
| 1.2 | 30-MAR-2024 | Annual Review | Sudhansu Kumar |
| 2.0 | 07-MAR-2025 | Updated exception process to reflect SD+ ticketing tool | Kavitha Shetty |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 04-AUG-2022 | Saravanan Sankaran | Sr. Director Infosec & IT | Approved |
| 03-JUL-2023 | Saravanan Sankaran | Sr. Director Infosec & IT | Approved |
| 30-MAR-2024 | Saravanan Sankaran | Sr. Director Infosec & IT | Approved |
| 11-Mar-2025 | Saravanan Sankaran | VP InfoSec & IT | Approved |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| Netradyne Internal |  |
|  |  |
|  |  |

# Purpose

The purpose of this Information Security Exception Management Procedure is to establish a systematic process for identifying, reviewing, and managing exceptions to Netradyne’s information security policies, procedures, and standards. This procedure ensures that exceptions are assessed based on risk and approved by the appropriate authorities, with full visibility and documentation in the designated ticketing system (SD+).

# Scope

This procedure applies to all processes, procedures, and policies set by the Infosec team at Netradyne.

# 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. |

# Process

All exceptions to security policies or standards must be requested and tracked through the **SD+ ticketing system**. This replaces all prior methods, including the Exception Request Form or manual trackers.

Exceptions are granted on a case-by-case basis by the Chief Information Security Officer (CISO) or a designated delegate, based on justification, risk analysis, and stakeholder approvals.

* Implementation of a solution with equivalent protection to the requirements in the policy or standard.
* Implementation of a solution with superior protection to the requirements in the policy or standard.
* Impending retirement of a system or control.
* Inability to implement the policy or standard due to some limitations (i.e., technical constraints, business limitations or statutory requirement).

The exception request must be submitted on a completed Exception Request Form and must include:

* Description of the non-compliance
* Anticipated duration of non-compliance
* Proposed assessment of risk associated with non-compliance
* Proposed compensating controls for managing the risk associated with non-compliance
* Proposed corrective action plan
* Proposed review date, to evaluate progress towards compliance
* Process owner / functional owner recommendation
* The Exception Request must be routed (via SD+) approved by:
  + <Supervisor/Manager>
  + <Business Owner>

If the non-compliance with the security policy or standard is due to a **superior solution**, an exception request is still required. In such cases, the exception will typically be granted **temporarily**, until the published policy or standard is formally revised to incorporate the improved solution.

Once an exception request is submitted through **SD+**, the Infosec team will:

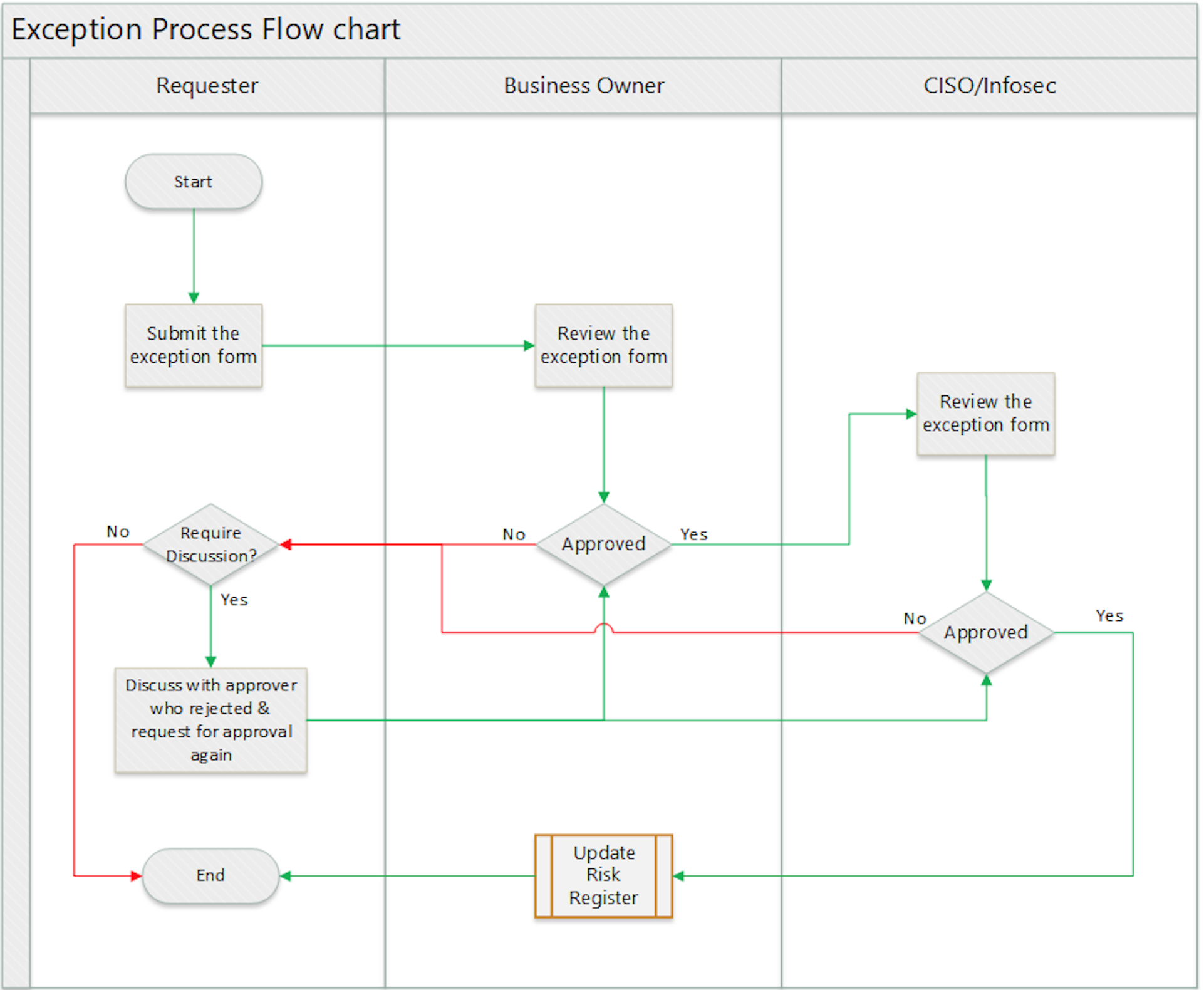
* Acknowledge the request via the SD+ ticket,
* Review the provided details,
* Request additional information if needed.

Upon receipt of all necessary information, the **CISO or their designated representative** will either **approve** or **reject** the request. The outcome will be communicated through the SD+ platform.

If the request is **rejected**, the requester will receive a brief explanation. The business team may also request a follow-up meeting with Infosec to discuss the rationale and explore possible alternatives.

If the request is **approved**, the requester is responsible for ensuring that the associated risk is recorded in the relevant **function’s risk register**, including all supporting details and review timelines

Exception Process Flow:



# Compliance

Compliance with this process will be monitored through various mechanisms, including but not limited to:

* Internal and external audits,
* Reporting and analytics from the exception management system (e.g., SD+),
* Awareness training and assessments,
* Feedback provided to the process owner.

Any instance of non-compliance may be escalated to the Netradyne Leadership Team for appropriate action.

# Exception Handling

Compliance is expected with all policies and standards of the organization. Policies Compliance with all organizational policies and standards is mandatory. However, where compliance is not technically feasible, or where a deviation is necessary tosupport critical business functions, the affected entity must formally request an exception.

Exception requests must be submitted through the Infosec team’s defined process using the SD+ ticketing system. Each request will be reviewed, risk-assessed, and approved or rejected based on established criteria.

Policies and standards are subject to change and may be amended by the Infosec team as needed.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Infosec team exception process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| SME | Subject Matter Expert |
| CISO | Chief Information Security Officer |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

## 

Templates

Policies

[User Access Management v2.0.pdf (sharepoint.com)](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)

[Netradyne Password Policy (sharepoint.com)](https://netorg726775.sharepoint.com/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/HIPAA%202024/Documentation%20Evidence%20HIPAA/ApprovedDocumentFolder/IT2024/Netradyne%20Password%20Policy.pdf?CT=1708607238113&OR=ItemsView)

[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=mRSIq4)

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

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=2jMnrk)

Process/Procedures

[NETRADYNE DISASTER RECOVERY PROCESS.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20DISASTER%20RECOVERY%20PROCESS.pdf?csf=1&web=1&e=xTyHtp)

[NETRADYNE BUSINESS CONTINUITY PLAN.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20BUSINESS%20CONTINUITY%20PLAN.pdf?csf=1&web=1&e=eCZUy6)

[Netradyne Vulnerability & Patch Management Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Vulnerability%20%26%20Patch%20Management%20Process.pdf?csf=1&web=1&e=N697w0)

[NetradyneSecurityIncidentResponsePlan.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NetradyneSecurityIncidentResponsePlan.pdf?csf=1&web=1&e=Nzo34K)

Standards

<List of (or Links to) related Netradyne Standards>

# 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 |