Netradyne Information Security Exception Process

v1.0

Internal and Confidential

TABLE OF CONTENTS

Document Control

Document ID	NDEM2022001
Document Name	Netradyne Exception Management Process
Document Status	Released
Document Released Date	04-Aug-2022
Document Author	Kavitha Shetty
Document Content Contributors	Kavitha Shetty; Sudhansu Kumar; Vijaykumar Dalal
Document Signatory	Saravanan Sankaran
Document Owner	Infosec
Document Version	v1.0
Information Classification	Internal

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised By
v0.1	13/JUN/2022	Draft Version	Infosec
V1.0	04/Aug/2022	Incorporated the process flow	Infosec

Document Review/Approval

Date	Signatory Name	Organization/Signatory Title	Comments
04/AUG/2022	Saravanan Sankaran	Sr. Director Infosec & IT	Approved

Distribution of Final Document

Name	Organization/Title

1 Purpose

This document is a Netradyne Information security exception policy. The purpose of this policy is to provide a method for obtaining an exception to compliance with a published information security standard, policies and procedures.

2 Scope

All process/procedures/policies set by Infosec team of Netradyne

3 Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

Role	***Responsibilities***
Owner	• Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. • Is the point of contact for the document. • Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process.
Reviewers/Stakeholders	Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality)
Approvers	The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead.
Document Release	Document Owner/team to work with repository administrator to make release version available.

4 Process

An exception may be granted by the Chief Information Security Officer (CISO) of Netradyne, or their designee, for non-compliance, non-adherence with a policy or standard resulting from:

- 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.
- Inability to implement the policy or standard due to some limitation (i.e., technical constraint, business limitation or statutory requirement).

Exceptions are reviewed on a case-by-case basis and the approval is not automatic. Exceptions will be reviewed and governed by Infosec in alignment with business

objectives and stakeholder's approvals. All the exceptions will be tracked in the exception tracker or SD+

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 approved by the following:
    - <Supervisor/Manager>
    - <Business Owner>

If the non-compliance with the security policy or standard is due to a superior solution, an exception is still needed and will normally be granted until the published policy or standard can be revised to include the new solution.

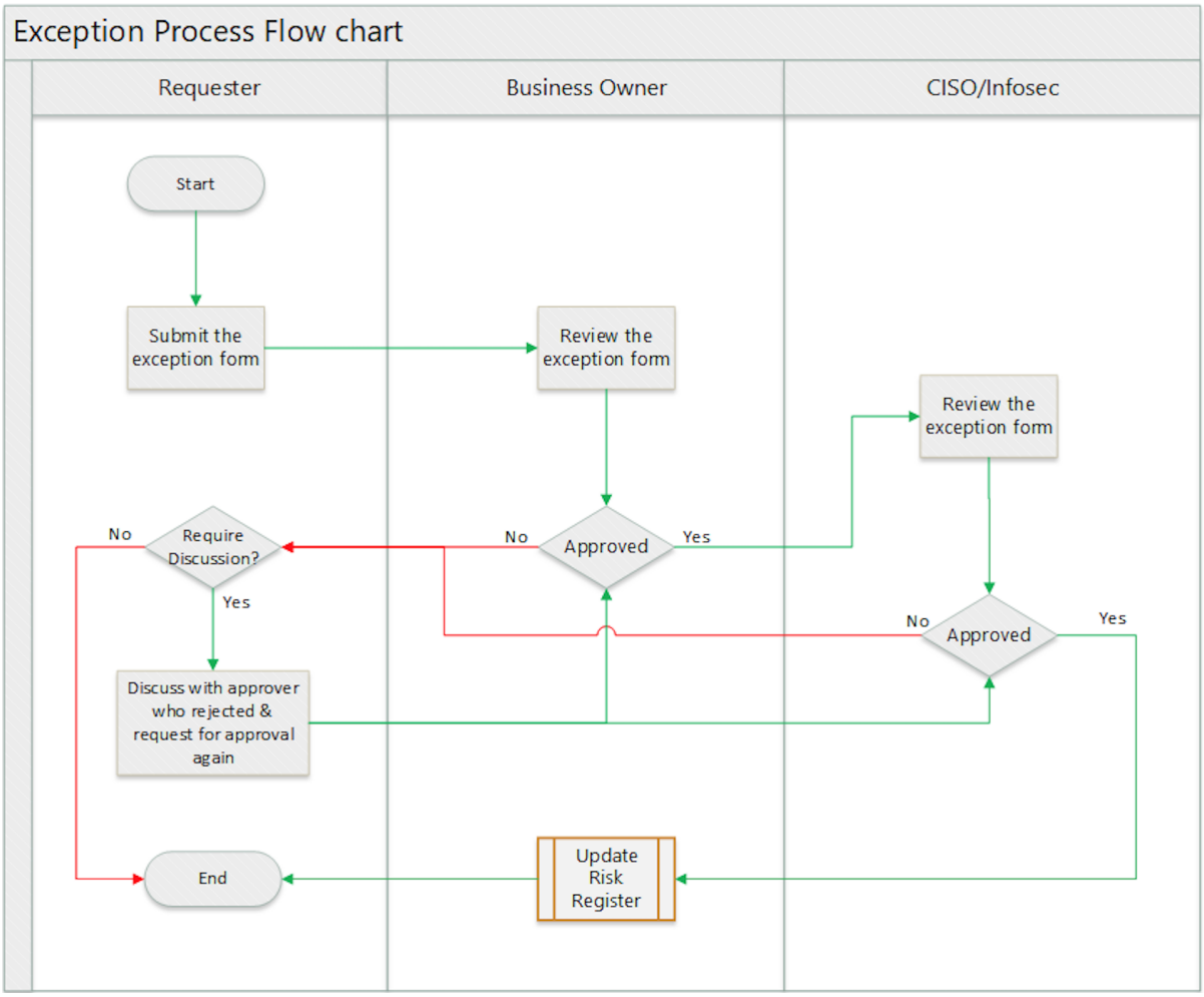
Upon submission of the Exception Request Form, the Infosec team will contact the requester to confirm receipt and request more information, if needed. Once all required information has been received, the CISO or designated person will either grant or deny the request.

Upon approval, the Infosec team will communicate the same to the requestor. If the request is rejected, a brief explanation of why the CISO or designated person rejected the request will be communicated to the requestor.

If the request is denied, the business owner/team may request a meeting with Infosec team to discuss the circumstances giving rise to the request and means of addressing those circumstances.

If the request is approved, the requestor needs to capture the risk into the function's risk register with the relevant information.

4.1 Exception Process Flow:



5 Conduct

Compliance checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

6 Exception

Compliance is expected with all policies and standards of the organization. Policies and standards may be amended at any time.

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.

7 Terms/Acronyms

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

8 References

8.1 Exception Request Form

8.2 Exception Tracker

8.3 Policies

Information Security Policy

8.4 Process/Procedures

NA

8.5 Standards

NA

8.6 Miscellaneous

NA

9 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