Information Security Exception Management Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

Ncell	**Ncell**	Classification: Internal
	Information Security Exception Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Procedure Name DOCID: PR-IT-IS-18

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS- 18 Exception Management Procedure v1.0**
Effective Date:	1st October, 2019
Document Author:	Information Security Team
Owner:	Information Security Team

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor’s (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO	CIO/Head Of IT

Ncell	**Ncell**	Classification: Internal
	Information Security Exception Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	01-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	13-12-2019
1	13-12-2019	Information Security Team	Approval	Andy Chong	13-12-2019
2	20-10-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	27-09-2023	Information Security Team	2. Review and update: changed from annually to once in every two years. 5.1. i Changed SDM into approved tool Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	30-04-2024	Information Security Team	Re-branding 5.ii Added responsibility for exception tracking	CIO/Head of IT	

Table of Contents

Document Control 3

1. Introduction 6

2. Review and Updating 6

3. Scope 6

4. Definitions 6

5. Exception Management Procedure 6

5.1. Exception Request 7

5.2. Guidelines for exception authorization/approval 7

6. Governance and Compliance 7

Ncell	**Ncell**	Classification: Internal
	Information Security Exception Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Introduction

Ncell has published a set of Information Security Policy, processes, and guidelines to address the need to secure information and information processing facilities. There might be some instances where these sets of policies, processes, guidelines might not be met. This document provides guidelines for requesting exceptions to these policy/process/guidelines adopted by Ncell.

2. Review and Updating

This procedure shall be reviewed once in every two years or whenever significant changes occur in the organization.

3. Scope

This document shall be used as a guiding principle by respective teams to raise exceptions against information security requirement.

4. Definitions

i. Exception: Exceptions are defined “non-compliances” to individual controls specified in relevant policies and procedures for IT and IS. All such exceptions should be formally documented in the Exception Request ticket, which will include, at a minimum, the following: -
   - Justification for the exception
   - Risk due to the exception
   - The mitigation controls to manage the risk
   - The plan of action to manage the risk
   - The validity period of the exception
   - Plan suggesting closure of exception

ii. Risk: It can be defined as direct or indirect negative impact caused on information asset and the supporting infrastructure by any given act

iii. Compensating Controls: An internal control that reduces the risk of an existing or potential control weakness

iv. Requester: Requester of exception will be the owner / custodian/ user of the asset. Owner / custodian/ user of the asset(s) is/are the person(s) in whose charge the asset is held. There can be cases where the exception is not for any privilege of any equipment but could be because of non-compliance to any procedure of handling like, security patch not being deployed in the requisite time frame because of some application related constraints

v. Asset Owner: Owner of an information asset is the person on whose name the information asset is held

vi. Custodian: Custodian of an information asset is the person, who is responsible for operation/ maintenance or other such activity on the information asset

vii. User: User of an information asset is the person who is using the asset

viii. Vulnerability: Vulnerability refers to weakness in any system that may allow an attacker to violate the Confidentiality (C), Integrity (I) and Availability (A) of the Information Asset

5. Exception Management Procedure

Exception Management Procedure is categorized in the following phases:

i. **Phase 1 – Exception Request -** The phase of exception request deals with identification of exception, documentation, identification of risk, compensatory controls to mitigate the risk, recommendation and approval/rejection of exception request. The grant of exception for any given asset will be governed by the following:
   - Same exception request for particular asset can be approved for maximum 5 times
   - Every exception request will have a start date and an end date for tracking
   - The identified exception should have sufficient alternate mitigation controls around the same to ensure the risk is mitigated or minimized

- The compounded risk of multiple exceptions on the subject needs to be highlighted and considered before grant of any exception
- Any request for exception beyond 5 times (per user per subject) needs to be deliberated by the Security Team on further course of action

ii. **Phase 2 – Exception Tracking -** Exception tracking is meant to ensure that all exceptions are tracked and relevant communication is sent to the requestor and other stakeholders as reminders for ensuring timely closure of the Exception. The relevant manager shall be responsible for tracking the exceptions within their teams/unit/section and ensuring timely closure of the action items or renewal of the exception request.

iii. **Phase 3 – Exception Closure -** This phase is meant to ensure that all exceptions are closed; artefacts are maintained and duly communicated to all stakeholders

iv. **Phase 4 – Exception Reporting -** This phase will ensure communication regarding exceptions (which were approved, tracked and closed) is cascaded to all relevant stakeholders

5.1. Exception Request

i. All exception requests shall be raised in approved tool

ii. The exception request should comprise of the following details:

   a. Requester Details
   b. Exception Expiry Date
   c. Service Category (Contractual Services, VAPT, Policy Violation)
   d. Details of impacted assets
   e. Exception Description
   f. Business Rationale
   g. Impact Analysis
   h. Compensating Controls

iii. The maximum validity period for an exception shall be 1 year.

iv. The exception needs to approved by the following stakeholders:

   a. Head of Department
   b. Service Owner
   c. Head of IT/CTO

v. For exceptions raised for vendors, the exception shall be raised by the Ncell SPOC on approved tool after obtaining the aforementioned information from the vendor.

5.2. Guidelines for exception authorization/approval

Authorizer / Approver shall reject the Exception application if:

i. The exception request is not complete and inappropriately filled by the requester
ii. The risk for the corresponding exception is not correctly mentioned
iii. The business justification mentioned does not reflect the exact business requirements

6. Governance and Compliance

Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.