


# Information Security Compliance Management Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

	<b>Ncell</b>	Classification: Internal
	<b>Information Security Compliance Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Procedure Name DOCID: PR-IT-IS-15

Copyright © Ncell. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior permission in writing from Ncell.

These trademarks are the intellectual property of Ncell and are protected by applicable legislation.

All other products or company names are used for reference only and may be proprietary to their respective hold

	<b>Ncell</b>	Classification: Internal
	<b>Information Security Compliance Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## Document Control

### i. Document Identification

<b>Document Title and Version:</b>	<b>PR-IT-IS-15 Information Security Compliance Management Procedure v1.0</b>
Effective Date:	15-09-2019
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	Legal Team
Informed	All Employees and External Parties

### iv. Digital Signature

CEO

CIO/Head Of IT

	<b>Ncell</b>	Classification: Internal
	<b>Information Security Compliance Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-09-2019
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	15-09-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	13-12-2019
1	13-12-2019	Information Security Team	Approval	Andy Chong	17-12-2019
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	Review and Updating – Period changed from annual to once every two years. 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	CIO/Head of IT	

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Information Security Compliance Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## Table of Contents

<b>Document Control</b> .....	2
<b>1. Purpose</b> .....	5
<b>2. Review and Updating</b> .....	5
<b>3. Scope</b> .....	5
<b>4. Information Security Compliance</b> .....	5
<b>4.1 Identification of relevant legal, statutory, regulatory and contractual requirements</b> .....	5
<b>4.2 Information Security Compliance Review</b> .....	5
<b>4.3 Sharing of information with legal agencies or regulatory body</b> .....	5
<b>4.4 Record Protection</b> .....	6
<b>5. Governance and Compliance</b> .....	6
<b>6. Associated Documents</b> .....	6

	<b>Ncell</b>	Classification: Internal
	<b>Information Security Compliance Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## 1. Purpose

The purpose of the compliance procedure for Ncell Pvt. Ltd. is to ensure service delivery consistently meets the needs and requirements of legal, statutory, regulatory or contractual obligations related to information security.

## 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 procedure is applicable to Ncell employees in accordance with applicable legal requirements and regulatory directives related to information security.

## 4. Information Security Compliance

### 4.1 Identification of relevant legal, statutory, regulatory and contractual requirements


- i. Advice and approval on statutory, regulatory and contractual requirements of Ncell should be sought from the legal team
- ii. The Information Security Team should document the requirements in a register with the corresponding controls associated with each regulatory and legal requirement.
- iii. The key regulatory and business requirements for information security applicable to Ncell are as follows:
  - a. Cyber security directives and initiatives from Nepal Telecommunications Authority
  - b. Directives from the Supreme Court
  - c. Statutory provision
- iv. The information security officer shall incorporate the required aspects to address such requirements.
- v. The information security officer should ensure that the controls are implemented to ensure compliance.

### 4.2 Information Security Compliance Review

- i. Compliance review should be performed to ensure effectiveness of implemented information security controls related to legal and regulatory requirements
- ii. Ncell should conduct periodic reviews to assess that implementation of processes are in accordance with the defined ISMS procedures. Respective function heads should be responsible for educating their teams regarding the security policies and associated procedures
- iii. Each department should regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements. If any non-compliance is found as a result of the review, managers should:
  - a. Determine the causes of the non-compliance
  - b. Evaluate the need for actions to ensure that non-compliance do not recur
  - c. Determine and implement appropriate corrective action
- iv. IS Compliance review report should be shared with controller/management and relevant departments. Also, all findings and recommendations should be shared with relevant departments for tracking and implementation.

### 4.3 Sharing of information with legal agencies or regulatory body

- i. Impact on Ncell for sharing requested IT related information should be analysed prior to sharing with legal agencies/regulatory body.
- ii. Requested information and its related impact analysis should be shared for approval from Ncell's legal team.
- iii. Information shall be shared with legal agencies or regulatory body on approval from the Chief Legal, Regulatory & Corporate Services Officer.
- iv. Formal record of all information shared with legal agencies or regulatory body should be maintained
- v. Information shared with legal agencies and regulatory body should be secure ( e.g. encrypted )

	<b>Ncell</b>	Classification: Internal
	<b>Information Security Compliance Management Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

#### 4.4 Record Protection

- i. Ncell should ensure that relevant controls and mechanisms are in place to protect records from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with the legal, regulatory, contractual and business requirements.

#### 5. Governance and Compliance

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

#### 6. Associated Documents

- i. Information Security Policy
- ii. Media Disposal Procedure