Information Security Management System (ISMS)Manual

Ncell

Guideline

Approved date:- 25/11/2024

Procedure Name DOCID: GD-IT-IS-15

Document Control

i. Document Identification

Document Title and Version:	**GD-IT-IS-15 Information Security Management System (ISMS) Manual**
Effective Date:	
Document Author:	Information Security Team
Owner:	CTIO

ii. Distribution List

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

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CTIO
Consulted	Functional Heads
Informed	All Employees and External Parties

iv. Digital Signature

MD / CEO	CTIO		

i. Revision History

Rev	Date	Author	Description	Approved By	Approval Initiated Date
0	22-11-2024		Initial document	MD / CEO	
1					

Table of Contents

0. Introduction

Purpose

This document details the framework established for the Information Security and Privacy Management System at Ncell. The purpose of this policy is to:

i. Establish an organization wide approach towards Information Security.
ii. Establish controls to ensure the protection of sensitive information stored or transferred electronically and the protection of the organization's information technology resources.
iii. Assign responsibility and provide guidelines to protect the organization's resources and data against misuse and/or loss. data against misuse and/or loss.

This manual is a demonstrable and auditable document of Ncell. It gives a clear description of the company's aspiration to implement an Information Security and Privacy Management System within the organization. This is part of the defined management system, detailing the activities implemented in accordance with the prerequisites for ISO 27001:2022 certification. The ISMS applies specifically to Ncell's IT services, customer service, and data center. This ISMS Manual may not be reproduced in whole or in part or otherwise disclosed without prior consent from the Management. This is a confidential document. The Government, customers, or any third party with which a contractual agreement has been established may use this as proof for verification. All controlled copies in .pdf format are indicated by 'Controlled Copy' without a rubber stamp.

The ISMS Manual has been issued by the Information Security Unit and released with the approved authorization of the CEO.

Manual Control Policy:

This manual;

i. Is the sole property of Information Security Unit is controlled as per Documented System Procedure
ii. The revision number shall reflect the current status of this manual.
iii. Shall not be reproduced or photocopied either partly or wholly without the approval of IS Manager.
iv. Is circulated to all the below mentioned copyholders.
v. Shall not be subjected to any unauthorized corrections or amendments.
vi. Shall be subject to audits.
vii. Manual Amendment Policy
viii. Only the Information Security Unit is authorized to make changes to the ISMS Manual.
ix. All changes in the Information Security and Privacy Management System documents shall be reflected in the Amendment Sheet.
x. The changes shall be reflected in all the copies.

Abbreviation

Abbreviation	Description
BAU	Business As Usual
BG	Background
DISO	Departmental Information Security Officer
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission

IQA	Internal Quality Audit
IS	Information Security
ISMS	Information Security Management System
ISO	Information Organization For Standardization
IT	Information Technology
KPI	Key Performance Indicator
NC	Non-Conformity
PII	Personally Identifiable Information
RA	Risk Assessment
RFP	Request for Proposal
SAG	Service Agreement

1. Scope

The provision of the Information Security and Privacy Management System at Ncell encompasses its IT services, customer service, and data center.

2. Normative Reference

The following documents are referred to in the text in such a way that some or all their context constitutes requirements of this document. For dated references, only the edition cited applies. For the undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 27001:2022 Information Security and Privacy Management System

3. Terms and definitions

For the purpose of this document, the terms and definitions given in ISO/IEC 27001 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

i.ISO Online browsing platform: available at https://www.iso.org/obp
ii.IEC Electromedia: available at http://www.electropedia.org/

4. Context of the Organization

4.1 Understanding the organization and its context

Ncell determines the external and internal issues/factors relevant to its purpose and that affect its ability to achieve the intended outcomes of its Information Security and Privacy Management System, including its IT services, customer service, and data center. The following are the internal and external issues/factors that could impact information security: -

External issues/factors that can have an impact on Information Security and Privacy:

i.Legal and Regulatory
ii.Physical Location
iii.Competitor
iv.Natural Disaster
v.Distributer Documentation Misuse
vi.Hackers
vii.Vendors Unauthorized Access

Internal issues/factors that can have an impact on Information Security and Privacy:

i.Organizations’ culture
ii.Relationships and perceptions and values of internal stakeholders
iii.Human Resource Security and Capabilities (knowledge)

iv. Governance, organization and roles and responsibilities
v. Standard working procedures and guides
vi. Power Backup Failure
vii. Electrical Short Circuit
viii. Unauthorized Access Control
ix. Internal Audit

4.2 Understanding the need and expectations of Interested Parties

Ncell has determined the needs and expectations of the interested parties and their requirements relevant to the organization. This includes a commitment to ensuring that the Information Security and Privacy Management System thoroughly meets the needs of IT services, customer support, and data center operations. Ncell is dedicated to continually monitoring, reviewing, and analyzing information and relevant requirements of the interested parties to ensure their needs are effectively managed within the ISMS.

i. Interested parties/key stakeholders

Ncell will ensure that its Information Security and Privacy Management System effectively addresses the requirements of key stakeholders. These stakeholders include customers and clients, where adherence to contractual obligations within the defined scope is essential. Additionally, employees, vendors, contractors, visitors, and third parties play a significant role, requiring Ncell to ensure the compliance with company standards while supporting Information Security and Privacy activities as per agreed service levels. The provision of IT services, customer service, and data center further emphasizes Ncell's commitment to safeguarding information security and Privacy. Public authorities and government bodies also hold critical influence, necessitating adherence to legal requirements such as the Company Act, Labor Law, and IT Act, along with ensuring the secure movement of bonded assets, maintaining a safe working environment, and promoting employee welfare.

Regulatory requirements impacting the information security and privacy are listed below:

i. The Companies Act 2063 (2006)
ii. Telecommunications Act 2053 (1997)
iii. The Labour Act 2074 (2017)
iv. Legal, regulatory, and contractual duties
v. The Privacy Act, 2075 (2018)
vi. Cyber Security Byelaw, 2077 (2020)
vii. NIST CSF 1.1, 2018

Ncell will ensure that the Information Security and Privacy Management System effectively addresses the contractual requirements outlined in the contractual agreements and Contractual Agreements with clients, specifically related to its IT services, customer service, and data center.

4.3 Determining the scope of the information security and privacy management system

Ncell has determined the boundaries and applicability of the information security and privacy management system. The clauses of the information security management system are all applicable.

The provision of Ncell is applicable to its IT Services, Customer Service, and Data Center.

4.4 Information security and privacy management system

Ncell has established, implemented, and is maintaining an Information Security and privacy Management System in accordance with ISO requirements, with a commitment to continually improving its effectiveness.

Reference Document(s):

i. *Ncell-ICT-2016-0187 Information Security Policy – Section 4. Principals*

5. Leadership

5.1 Leadership and Commitment

Ncell's top Management along with their teams is committed to motivating the organization and authorizing employees to contribute for the effectiveness of Information Security and Privacy Management System.

5.1.1 Management Commitment

Ncell management is committed to developing effective Information Security and Privacy Management System's policies and practices that apply to its IT services, customer service, and data center. Roles and responsibilities for information security and privacy are clearly defined and communicated, emphasizing compliance with Information security and privacy policies and legal requirements. Management will provide the necessary resources for establishing, implementing, monitoring, and continually improving information security and privacy.

Reference Document (s):

i.*Ncell-ICT-2016-0187 Information Security Policy - 5. Roles and Responsibilities*
ii.*PR-IT-IS-01 Information Security Governance Procedures – Section 4 Information Security Organization Chart*
iii.*Respective Departmental KPIs of IT, Customer Service and Data Center*

5.2 Policy

Ncell top level management has established an information security and privacy policy that has considered:

1. Purpose of the organization
2. Information Security Objectives
3. Commitment to satisfy applicable requirements related to information security and privacy
4. Commitment to continual improvement

The information security and privacy policy is available as documented information and is communicated within the organization and is also available to relevant interested parties.

Reference Document (s):

i.*Ncell-ICT-2016-0187 Information Security and Privacy Policy*
ii.*Ncell-ICT-2016-0187 Information Security Policy –* Section 4 Principles
iii.*RNC-P-2022-001 Data Privacy Policy - 7. Data Privacy Principles,*
iv.*Departmental KPIs of IT, Customer Service and Data Center.*

5.3 Organizational Roles, Responsibilities and Authorities

Ncell has established an Information Security and privacy Management System that encompasses its IT services, customer service, and data center. The details of the organization structure, along with roles and responsibilities, are outlined in the Ncell's existing 'Roles and Responsibilities' document and Governance document.

Reference Document(s):

i. *PR-IT-IS-01 Information Security Governance Procedures Section 4*
ii. *Ncell-ICT-2016-0187 Information Security Policy - Section 5, 6*

6. PLANNING

6.1. Actions to Address Risks and Opportunities

6.1.1 General

The issues/risks identified while establishing, implementing or maintaining the ISMS should be tracked.
In Ncell, a Risk Register for ISMS is available to track these risks and other unforeseen issues to:

a. Ensure ISMS achieve its intended outcome.
b. Prevent or reduce the undesired effects.

c. Achieve continual improvement.

This action will help to address the ISMS risks and issues and to implement the actions in policies/methodology and strengthen the effectiveness of ISMS.

Reference Document(s):

i. *TE-PR-2018-0007 Crisis Management Plan*
ii. *Risk Register-IT, Customer Service, Data Center.*
iii. *F&P-PR-2023-0007 Enterprise Risk Management Procedure*

6.1.2 Information Security Risk Assessment

Ncell adopts a unique Risk Management approach for its information assets, which includes a comprehensive evaluation of its IT services, customer service, and data center. This approach is based on a qualitative risk analysis model for assessing, and maintaining the risk framework and risk acceptance criteria, while also implementing certain formulas that align with a quantitative approach. This unique method ensures the proper identification and measurement of risks associated with these assets, along with the corresponding mitigation controls that have been implemented.

The Risk Management Team comprises individuals from various departments within Ncell encompassing the business and the support groups. Representatives who are called Departmental Information Security Officers (DISO) from the business and support groups work together and identify the assets within their team and conduct the risk assessment and risk treatment process with due contribution from the Information Technology team (Senior Manager – IT) as well as Director.

Reference Document(s):

i. *TE-PR-2018-0007 Crisis Management Plan*
ii. *Risk Register-IT, Customer Service and Data Center*
iii. *F&P-PR-2023-0007 Enterprise Risk Management Procedure*

6.1.3 Information Security Risk Treatment

The provision of IT services, customer service, and data center shall be evaluated for risks against the established risk acceptance criteria, with appropriate risk treatment options selected accordingly. Additionally, necessary controls for risk treatment will be determined, and a risk treatment plan shall be developed to prioritize and mitigate the risks identified during the risk assessment.

Reference Document(s):

i. *TE-PR-2018-0007 Crisis Management Plan*
ii. *Risk Register-IT, Customer Service and Data Center*
iii. *F&P-PR-2023-0007 Enterprise Risk Management Procedure*

6.2. Information security objectives and plans to achieve

Ncell has established information security and privacy objectives for its IT Services, Customer Service, and Data Center.

Reference Document (s):

i. *Departmental KPIs of IT, Customer Service and Data Center*

6.3. Planning of Changes

Ncell has determined the need for changes to the information security and privacy management system. The organization has considered:

1. The purpose of the changes and their potential consequences.
2. The integrity of the information security management system.
3. The availability of resources.
4. The allocation or reallocation of responsibilities and authorities.

Reference Document (s):

i. *TE-PS-2015-0103 - Change-Management-Process*

7. SUPPORT

7.1 Resource

Ncell ensures that adequate resources are provided to the processes, projects of its IT services, customer support, and Data center in terms of hardware, software, manpower, infrastructure, and budget for:

1. Implementation and effective maintenance of the ISMS, PIMS and continual improvement of its effectiveness.
2. Ensuring that IT services, customer service, and data center adhere to security protocols.
3. Members of the IS Team coordinating with functions to define and implement processes across these areas.
4. Collaborating with Functional Heads to define, document, and ensure the implementation of processes in their respective domains.

Reference Document(s):

i.*PR-IT-IS-02 Asset Management Procedure*

7.2 Competence

Appropriate competence needed is determined in accordance with the ISMS processes. Adequate and competent human resources are provided to carry out these processes, including those related to IT services, customer service, and data center. Required training is provided to improve the desired skill and competency. Effectiveness of training is evaluated. The training and awareness program will include the implications of not conforming to ISMS requirements and various other aspects of ISMS and PIMS. Ncell will ensure that personnel assigned to information security and privacy are sufficiently trained and competent to handle their roles and responsibilities. Related documentation, such as training records, experience, qualifications.

7.3 Awareness

Ncell ensures that all personnel involved in IT services, customer service, and data center are aware of the Information Security and privacy Policy, understand their contributions to the effectiveness of the ISMS and PIMS, recognize the benefits of improved information security performance, and are informed of the consequences of failing to conform to information security requirements.

In addition to ensuring an acceptable level of understanding of the organization's IS commitments, Department Heads will be responsible for promoting awareness among their staff regarding the importance of information security within IT services, customer service, and data center. Managers, supervisors, and team leaders will support their staff in identifying training needs from an IS perspective across these critical areas.

Reference Document (s):

i.*PR-IT-IS-05 Information Security Training and Awareness*

7.4 Communication

Channel for internal communication relevant to ISMS are established within the organization at different levels, such as:

1. Team briefings & meetings
2. Electronic mail
3. Intranet based
4. Employee Induction & Awareness Training

The communication regarding the effectiveness of the information security and privacy management system is done by means of:

1. Documentation Reviews
2. Internal Quality Audit (IQA) Reports

The effectiveness of communication is measured through various tools like audits and KPIs.

Reference Document (s):
i.*GD-IT-IS-10 Email Guidelines*
ii.*Intranet Platform*
iii.*Ngage Platform*

7.5 Documented Information

7.5.1 General

Ncell establishes effective control over the creation, authorization, issuance, distribution, maintenance, integrity, and subsequent changes (if any) of IS documents across all domain areas, including IT services, customer service, and the data center. The Information Security and Privacy Manager will oversee the process of the ISMS, document structure, and control, which encompasses identifying, approving, issuing, and assessing the effectiveness of these documents. The documentation includes:

1. IS Policy and Objectives
2. ISMS Manual, Procedures, Forms.
3. Supporting Records (Log Sheets, Incident reports)

7.5.2 Creating and updating

When creating and updating documented information the organization has ensured:

1. Identification and description
2. Format and media
3. Review and approval for suitability and adequacy.

7.5.3 Control of Documented Information

Document Control Procedure is established to define the controls needed:

1. To identify the documented information.
2. To format for suitability of the documented information.
3. To approve documents for adequacy prior to issue.
4. To review and update as necessary and re-approve documents.
5. To ensure that changes and the current revision status of documents are identified.
6. To ensure that relevant versions of applicable documents are available at points of use.
7. To ensure that documents remain legible and readily identifiable.
8. To ensure documents of external origin that are relevant to ISMS are identified and their distribution is controlled by the respective processes.
9. To prevent the unintended use of obsolete documents, and to apply suitable identification to them, if they are retained for any purpose.

Documented information of external origin determined by the organization and required for planning and operating ISMS and PIMS should be stored appropriately and controlled by ISMS Manager and respective areas within the organization impacted by this information.

Access control list is available for Information Security and Privacy Management team members and respective process/projects/program/enabling function to access the documented information.

Reference Document(s):
i.*F&P-2020-0001 Controls of Documents*

8. OPERATION

8.1 Operation Planning and Control

Ncell is committed to planning, implementing, and controlling processes to meet information security and Privacy requirements and objectives at the project and process levels, particularly within its IT services, customer service, and data center. To ensure effective management of ISMS and PIMS requirements at the operational level, documentation and practices must be established according to specified criteria, with appropriate controls implemented, and documented information maintained up to date to instill confidence.

For outsourced processes, Ncell ensures that IS requirements are regularly reviewed and controlled through requirement verification checklist and project plan (Response to the RFP), logging any discrepancies identified by the IS team through requirement.

8.2 Information security Risk assessment

Ncell performs information security risk assessments at least at planned intervals or when any significant changes are proposed or occurred.

8.3 Information security risk treatment

Ncell has implemented the information security and Privacy risk treatment plan, which covers its IT services, customer service, and data center.

Reference Document(s):

i.*Risk-Register-IT, Customer Service and Data Center.*
ii.*F&P-PR-2023-0007 Enterprise Risk Management Procedure*

9. Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

Monitoring, measurement, analysis, and evaluation are critical for assessing the performance and ongoing effectiveness of the Information Security and Privacy Management System. Ncell conducts annual performance reviews across various audits, including IT Audit, Statutory Audit, By-Law Audit, and through Key Performance Indicators (KPIs) related to its IT services, customer service, and data center.

Reference Document(s):

i.*IA-Policy_Final_14-Feb-2023*
ii.*GD-IT-IS-11 System and Information Maintenance Guidelines*
iii.*Departmental KPIs of IT, Customer Service and Data Center*

9.2 Internal Audit/Assessment

9.2.1 General

The Information Security and Privacy Management System is continuously monitored through scheduled internal audits conducted by qualified auditors. The audits cover all areas and all activities of the ISMS along with PIMS and determine whether the activities and their results:

1. Conform to the requirements of this International Standard and
2. The established ISMS is effectively implemented and maintained.

9.2.2 Internal Audit Program

The audit program is planned with suitable audit frequencies taking into consideration the status and importance of activities / area or process to be audited and results of previous audits conducted. All areas / activities are audited as per established criteria at least once in a year. Records & results of audits are

maintained including commitment for timely executing corrective actions to close the reported non-conformances by eliminating the root-cause.
Internal audit is conducted once in a year. Ncell has formulated audit procedures to:

a. Evaluate the compliance of existing organizational practices to ISO 27001 and ISO 27701.
b. Evaluate the compliance of existing organizational practices with Ncell’s Information Security and Privacy Policy and Objectives
c. Evaluate the compliance of existing organizational IS practices with Ncell’s legal, contractual and regulatory requirements.
d. To identify any potential gaps in the existing IS program/ arrangements and to provide recommendations to address the identified gaps.

The management responsible for respective areas should ensure that necessary corrections and corrections are taken on time without undue delay to eliminate detected NCs and their causes. Also, verification of the actions taken by the teams to be and result of the same also get reported.

9.3 Management Review

9.3.1 General

Management review of ISMS and PIMS will be conducted at planned intervals, which shall suggest improvements to the ISMS including Information Security and Privacy policies and procedures, Incident Management Plans to ensure continuing suitability, adequacy and effectiveness and any needs for changes to ISMS.

9.3.2 Management Review Inputs

Management Review includes the following agenda:

1. Status of actions of previous management review
2. Change in internal, external issues relevant to ISMS
3. Change in needs and expectations of interested parties that are relevant to the information security management system
4. Feedback on IS performance
5. IQA status (including NC’s and corrective actions)
6. Monitoring & Measurement results
7. Audit results
8. Fulfillment of IS security objectives
9. Feedback from Interested Parties
10. Results of Risk Assessment and status of Risk Treatment Plan and
11. Opportunities for continual improvement

9.3.3 Management Review Results

The output of the management review includes decisions related to continual improvement opportunities and necessary changes to the ISMS, specifically addressing IT services, customer service, and data center.

Reference Document (s):

i. *IA Policy of Ncell*
ii. *SOP for ISMS and PIMS – Section 6 Procedure for Management Review*

10. Improvement

10.1 Nonconformity and Corrective action

In Ncell, non-conformities are being identified by various sources like exercising, testing, audits, review. Management will ensure appropriate corrections are taken to correct the nonconformities and deal with the consequences. Respective department heads will be responsible for implementing the required control in order that it does not recur by reviewing the NC, determining the root causes and if similar NC exist and can occur. The Information Security and Privacy Manager is also responsible for evaluating and taking corrective action to ensure that non-conformities do not recur or occur elsewhere.

The Information Security and Privacy manager is also responsible for reviewing the effectiveness of the action taken and making changes in ISMS if required.

10.2 Continual Improvement

The management shall continually improve the suitability, adequacy or effectiveness of the ISMS and PIMS on an ongoing basis by performing periodic reviews and taking appropriate and timely decisions for effective implementation, and maintenance of the ISMS and PIMS.

a. Continual improvement will be ensured through the following methods:
b. Feedback/suggestion from interested parties and Process Heads/Program Managers as and when required
c. Any improvement suggestion received during Business as Usual (BAU)
d. Internal quality audit
e. Best practices found during internal audit

11. ANNEX A CONTROLS

Annex A-1 (normative)

Information Security Controls references

The information security controls listed in Table A.1 are directly derived from a signed with those listed in ISO/IEC 27001:2022], Clauses 5 to 8, and shall be used is context with 6.1.3.

5	Organizational Controls		Reference Document(s)
5.1	Policies for information security	Information security policy and topic specific policies shall be defined, approved by management, published, communicated to and acknowledge by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Ncell-ICT-2016-0187 IS Policy
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	PR-IT-IS-01 Information Security Governance Procedures Section 4
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Ncell-ICT-2016-0187 IS Policy, (5. Roles and Responsibilities, PR-IT-IS-17 section 8 of Privileged Access Management Procedure)
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	PR-IT-IS-01 Information Security Governance Procedures
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	RNC-PR-2022-0004 Authority-Request-Response-Flow-Procedures
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	RNC-PR-2022-0004 Authority-Request-Response-Flow-Procedures

5.7	Threat intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	Through SOC
5.8	Information security in project management	Information security shall be integrated into project management.	PR-IT-IS-19 Project Go-Live
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	PR-IT-IS-02 Asset Management Procedure
5.1	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented	GD-IT-IS-02 Acceptable Usage Guidelines Section 5
5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement.	PR-IT-IS-02 Asset Management Procedure Section 9.1
5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	PR-IT-IS-03 Information Classification Procedure Section 4 and 5
5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	PR-IT-IS-03 Information Classification Procedure Section 6
5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	PR-IT-IS-03 Information Classification Procedure Section 6 and 7
5.15	Access control	Rules to control physical and logical access to information and other associates assets shall be established and implemented based on business and information security requirements.	PR-IT-IS-07-Access-Management-Procedure_simplification Section 8 and 9
5.16	Identity management	The full life cycle of identities shall be managed.	PR-IT-IS-17 Privileged Access Management Procedure Section 4.3
5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	GD-IT-IS-01 Password Management Guidelines Section 5
5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.	PR-IT-IS-07 Access Management Procedure Section 8.5
5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier’s product or services.	F&P-PR-2022-0003 Procurement Procedure
5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	F&P-PR-2022-0003 Procurement Procedure
5.21	Managing information security in the information	Processes and procedures shall be defined and implemented to manage the information security	F&P-PR-2022-0003 Procurement Procedure Section 4.0

	and communication technology (ICT) supply chain	risks associated with the ICT products and services supply chain.	
5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practice and service delivery.	F&P-PR-2022-0003 Procurement Procedure
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	GD-IT-IS-14 Cloud security guidelines Section 4
5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	PR-IT-IS-13 Information Security Incident Management Procedure Section 5 and 8
5.25	Assessment and decision on information security events	The organization shall access information security events and decide if they are to be categorized as information security incidents.	PR-IT-IS-13 Information Security Incident Management Procedure Section 6, 8.3.4, TE-PR-2018-0007 Crisis Management Plan Section 1.3 Incident Classification Codes
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	PR-IT-IS-13 Information Security Incident Management Procedure Section 5 and 8
5.27	Learning form information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	PR-IT-IS-13 Information Security Incident Management Procedure Section 8.7 and 8.7.1
5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	PR-IT-IS-13 Information Security Incident Management Procedure Section 8.7.1
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption	PR-IT-IS-13 Information Security Incident Management Procedure Section 8.4
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	TE-PR-2018-0007 Crisis Management Plan Section 3, TE-PR-2018-0008 Business Continuity Policy
5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual, requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Corporate Policy - Legal Policy, regulatory Policy
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Corporate Policy Section 2.6, Subsection 2.6.1, 2.6.2, 2.6.3
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	COUPA and Ngage

5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Data Privacy Policy of Ncell
5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviews independently at planned intervals, or when significant changes occur.	IA Policy Section 2.1.1
5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Corporate Policy of Ncell, Regulatory Policy
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	F&P-2020-0001 Control of Documents Section 5
6	**People controls**		
6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	IT-IS-PR-2020-12 HR Security Procedure, section 5
6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	HR-G-2022-0005 Recruitment Guidelines
6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	PR-IT-IS-05 Information Security Training and Awareness Procedure
6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Disciplinary Action of Employee Regulation 2062 of Spice Nepal (P.) Ltd.
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	IT-IS-PR-2020-12 HR Security Procedure, section 6
6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's need for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	IT-IS-PR-2020-12 HR Security Procedure, section 7 Access Arrangement, point no. 1
6.7	Teleworking (Remote working)	Security measures shall be implemented when personnel are working remotely to protect information accessed processed or stored outside the organization's premises.	GD-IT-IS-09 Remote Access Guidelines 6. Remote Access Guidelines
6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Section 5.1 of GD-IS-IS-07 Antivirus and Malware Protection Guidelines, Section 6 of PR-IT-IS-13 Information Security

			Incident Management Procedure
7	**Physical controls**		
7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Ncell-ICT-2016-0187 Information Security Policy. Principles point No: 1, 2, Ncell Security Policy (Physical Protection), TE-G-2016-0204 Data Center Operation and Maintenance Guideline section 2
7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	S&A-G-2023-0001 Visitor Management Guideline, Ncell Security Policy (Physical Protection)
7.3	Securing office, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Ncell Security Policy (Physical Protection)
7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Ncell Security Policy (CCTV Systems)
7.5	Protection against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Ncell-ICT-2016-0187 Information Security Policy, Page 4, Point no. 1 of Principle section, Ncell Security Policy (Physical Protection)
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Ncell Security Policy (Site Planning, Physical Protection)
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Ncell Security Policy (Business Requirement for Access Control Point no. E)
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Ncell-ICT-2016-0187 Information Security Policy, Page 4, Point no. 2 of Principle section, Ncell Security Policy (physical Protection)
7.9	Security of assets off-premises	Off-site assets shall be protected.	GD-IT-IS-09 Remote Access Management Guidelines Section 6.2
7.1	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	PR-IT-IS-04 Media Handling Procedure 5. Media Disposal Process
7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	GD-IT-IS-11 System and Information Maintenance Guidelines 5. Maintenance Guidelines
7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Ncell Security Policy (Cabling Security)

7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	GD-IT-IS-11 System and Information Maintenance Guidelines, Ncell Security Policy, TE-G-2016-0204 Data Center Operation and Maintenance Guideline section 2, 3
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Ncell Security Policy (Removal and Disposal of Assets)
8	**Technological controls**		
8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	PR-IT-IS-04 Media Handling Procedure Section 4.2
8.2	Privileged access rights	The allocation and use of privileged access right shall be restricted and managed.	PI-IT-IS-07 Access Management Procedure 9. Privileged Access Management
8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	PI-IT-IS-07 Access Management Procedure, PR-IT-IS-17 Privileged Access Management Procedure
8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Contractual Agreement
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	PR-IT-IS-07 Access Management Procedure 8.4 User Account Revocation, 8.5 Access Logs and Rights Reviews
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Done through VMware Capacity Forecasting tool
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	GD-IT-IS-07 Antivirus and Malware Protection Guidelines 5. Anitivirs and Malware Protection Procedure
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	PR-IT-IS-06 Vulnerability and Patch Management Procedure Section 5.
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	GD-IT-IS-07 Antivirus and Malware Protection Guidelines Section 7, 7.1, PR-IT-IS-11 Network Security Section 4
8.1	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	RNC-P-2022-0001 Data Privacy Policy, Section 7.3 Data retention and disposal
8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control	GD-IT-IS-14 Cloud Security Guidelines 4.7

		and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Encryption and Key Management
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	PR-IT-IS-10 Data Loss Prevention Procedure 5. DLP Program
8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	GD-IT-IS-04 Backup Guidelines Section 7
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	TE-G-2016-0204 Data Center Operation and Maintenance Documents Section 2.1, 2.2, 3.1, 4.1
8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.	PR-IT-IS-08 Log Management Procedure Section 5
8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	PR-IT-IS-08 Log Management Procedure Section 5, 5.7
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approve time sources.	PR-IT-IS-11 Network Security Procedure 4.2 Network Hardening
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	GD-IT-IS-02 Acceptable Usage Guidelines, 5.9.2 Privileged utility programs
8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	GD-IT-IS-02 Acceptable Usage Guidelines, 5.9.4 Monitoring, 5.9 Software Usage
8.2	Network security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	GD-IT-IS-02 Acceptable Usage Guidelines Section 5.5, PR-IT-IS-11 Network Security Procedure Section 4
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	GD-IT-IS-02 Acceptable Usage Guidelines Section 5.5, PR-IT-IS-11 Network Security Procedure Section 4
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	PR-IT-IS-11 Network Security Procedure, 4.5 Use of Firewall, Point no. 6, Section 4.9 Wireless Security, Point no. 8
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	GD-IT-IS-02 Acceptable Usage Guidelines Section 5.3, 5.4, 5.5, 5.6
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	GD-IT-IS-14 Cloud Security Guideline, 4.7 Encryption & Key Management
8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	PR-IT-IS-16-System Development Life Cycle

			Procedure, RNC-G-2022-0002-Guidelines for Privacy by Design
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	PR-IT-IS-16-System Development Life Cycle Procedure 4.3 Incorporating Security in SDLC
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	PR-IT-IS-16 System Development Life Cycle Procedure 4.3 Incorporating Security in SDLC
8.28	Secure coding	Secure coding principles shall be applied to software development.	Contractual Agreement
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Contractual Agreement
8.3	Outsourced Development	The organization shall direct, monitor and review the activities related to outsourced system development.	Data Assessment Impact Assessment Procedure; Vendor Privacy Assessment, Proposed Projects, RNC-G-2022-0002-Guidelines for Privacy by Design
8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	PR-IT-IS-16 System Development Lifecycle Procedure, RNC-G-2022-0002-Guidelines for Privacy by Design Section 4.4, Appendix D
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	TE-PS-2015-0103 Change Management Process
8.33	Test information	Test information shall be appropriately selected, protected and managed.	PR-IT-IS-16 System Development Lifecycle Procedure Section 4.3.2, point no. 6 , RNC-G-2022-0002-Guidelines for Privacy by Design Section 4.5, Appendix 5
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	IA Policy Final

12. GLOSSARY

Term	Definition
Information Security (IS)	Protection of information assets from unauthorized change, destruction or disclosure, whether intentional or accidental.
Legal, regulatory & Contractual (LRC / L&R)	Reference to all the applicable statutory laws, acts, rules, regulations set by governing bodies and public authorities.

Information Security Management System (ISMS)	An Information Security Management System (ISMS) is a management system based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.
Privacy Information Management System (PIMS)	A Privacy Information Management System (PIMS) is a management system based on a systematic privacy risk approach, designed to establish, implement, operate, monitor, review, maintain, and improve the management of personal data and privacy.
Risk Assessment (RA)	Process of risk identification, analysis and evaluation.
Service Agreements (SAG)	Reference to the respective client/customer contractual agreement for the service level delivery.