Information Security Governance Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

Procedure Name DOCID: PR-IT-IS-01

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS-01 Information Security Governance Procedure v1.0**
Effective Date:	1st October, 2019
Document Author:	Information Security Team
Owner:	Information Security Team
Reviewed by (Head of legal Dept)	CEO

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/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO	CTIO

v. Revision History

Rev	Date	Author	Description	Approved By	Approval 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	17-12-2019
2	02-05-2023	Information Security Team	Approval	Andy Chong	02-05-2023
3	28-09-2023	Information Security Team	No Change	Rajesh Lal Nyachhyon	27-12-2023
4	27-12-2023	Tarani Prasad Chaudhary	Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
5	25-04-2024	Information Security Team	Re-branding	CTIO/Head of IT	06-06-2024
6	21/11/2024	Information Security Team	Approval	CEO	25-11-2024

Table of Contents

1. Purpose

Ncell. has established an organizational security framework to help achieve an effective and efficient way of managing the Information security. Ncell believes in a multi-disciplinary approach to information security, e.g. involving the co-operation and collaboration of business heads, service line managers, administrators, users, application owners, auditors, security staff and personnel with specialist skills in areas such as Legal, Finance, Physical Security and HR. Information Security Organization is established to coordinate and control the implementation of information security within the organization.

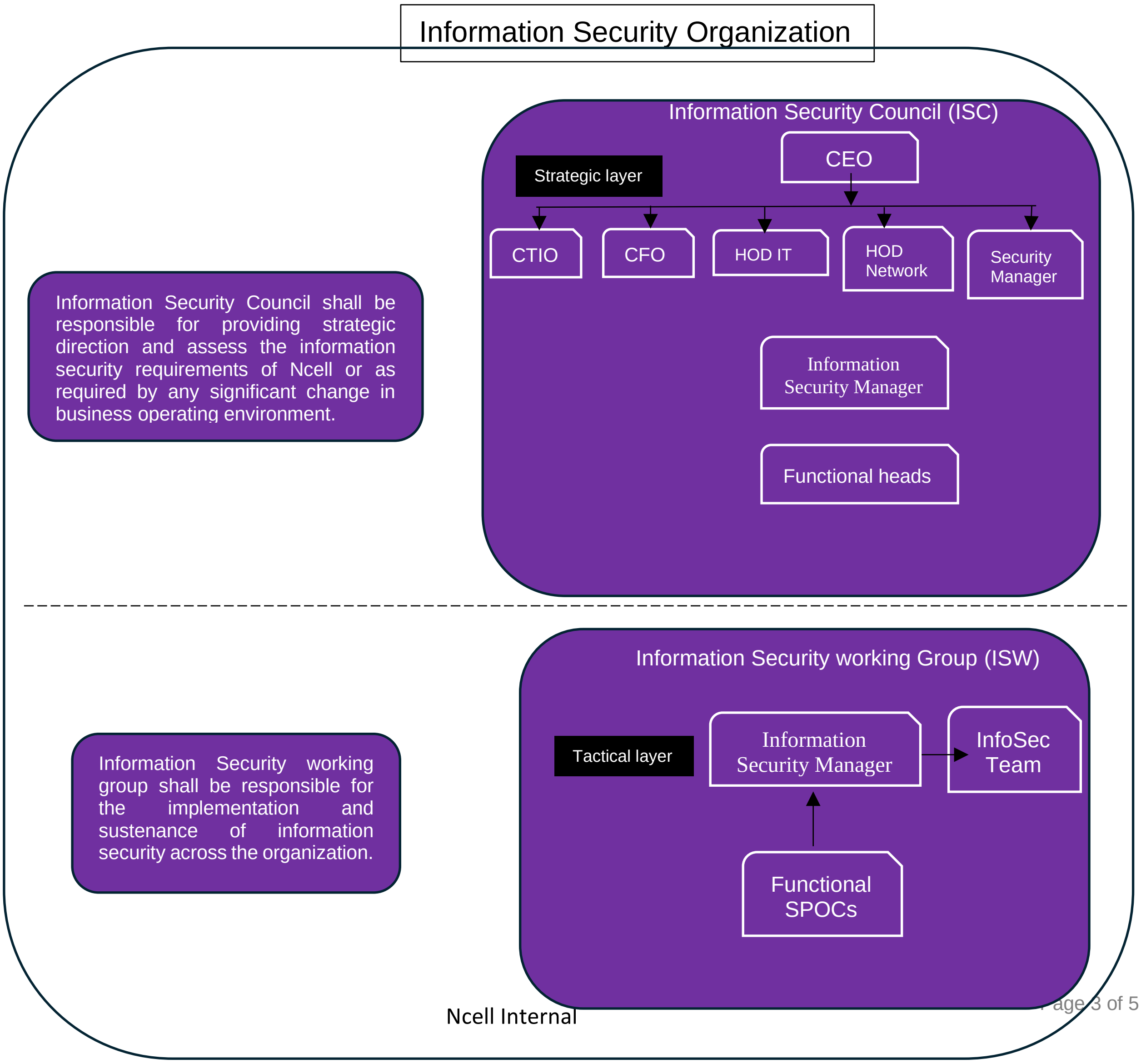
2. Review and Updating

This procedure shall be reviewed annually or whenever significant changes occur in the organization.

3. Scope

The scope of the ensuing document is to detail the Information Security Organization structure and the roles and responsibilities of the organization. The users of this document are the individuals identified for the roles mentioned in the document. All personnel at Ncell are required to be aware of the roles and responsibilities mentioned in this document.

4. Information Security Organization



Information Security Organization

Information Security Council (ISC)

Strategic layer

CEO

CTIO

CFO

HOD IT

HOD Network

Security Manager

Information Security Manager

Functional heads

Information Security Council shall be responsible for providing strategic direction and assess the information security requirements of Ncell or as required by any significant change in business operating environment.

Information Security working Group (ISW)

Tactical layer

Information Security Manager

InfoSec Team

Functional SPOCs

Information Security working group shall be responsible for the implementation and sustenance of information security across the organization.

4.1 Information Security Council

4.1.1 Roles and Responsibilities - Information Security Council (ISC)

S. No.	Role/ Designation
1	Chief Executive Officer
2	Chief Financial Officer
3	Chief Technology and Information Officer
4	Head of IT
5	Head of Network
6	Security Manager
7	Information Security Manager
8	Functional Heads

i. The ISC will undertake the following:
   a. Provide direction and support for the information security and constantly strive to improve the security of information assets at Ncell;
   b. Provide adequate resources to support improvement of information security;
   c. Approve the organization's Information Security frameworks and overall responsibilities;
   d. Promote information security education, training and awareness throughout Ncell;
   e. Review internal audit report and follow-up on the status of corrective actions taken on a periodic basis; and
   f. Approve the decisions (acceptance / mitigation) related to risks or residual risks, as applicable;
   g. Ensure that user IDs for the employees within their department are created/ modified/ deleted post their approvals; and
   h. Ensure that audit findings pertaining to their respective departments are closed effectively.

ii. The Information Security Council will meet at least once a year to assess the security requirements of Ncell or as required by any significant change in the business operating environment.

4.1.2 Authorities

i. Provide direction and support to constantly strive to improve the Information Security at Ncell;
ii. Approve the organization's Information Security framework and overall responsibilities; and
iii. Approve methodologies and processes for information security management.

4.2 Information Security Working Group

4.2.1 Roles and Responsibilities: ISWG-Corporate Level

S. No.	Designation
1.	Manager – Application Planning and Management
2.	Manager – Products and Services
3.	Manager – Network Planning and Strategy

S. No.	Designation
4.	Manager – Network Operations and Maintenance
5.	Unit Head – Enterprise Support and Platform Planning
6.	Unit Head – Business Support System
7.	Unit Head – Customer Support Systems
8.	Unit Head – Operating Support Systems
9.	Senior Engineer – Products and Services
10.	Unit Head – Core Network
11.	Specialist – Physical Security and General Services
12.	Unit Head – Transport Network
13.	Unit Head – Radio Network
14.	Unit Head – Rollout and Core Infra Support
15.	Technical Specialist- IS Engineer, InfoSec Team
16.	Senior Engineer- Compliance Officer, InfoSec Team
17.	Senior Specialist- Internal Audit

The Information Security Working Group (ISWG) is entrusted with the responsibility of managing security related operations on a day-to-day basis and co-coordinating with the Info Sec team for maintenance of the Information security. The ISWG will meet on a need basis for the same. They will have the following responsibilities:

i. Work with the InfoSec manager to ensure effective process for implementing and maintaining the security controls along with Information Security KPIs;
ii. Attend internal education and awareness programs to remain current and update on current policy requirements;
iii. Review assessment reports dealing with the IS issues and ensure that they are acted upon in timely manner;
iv. Coordinate any Incident Response procedures undertaken in response to (current /potential) security breaches and coordinate or assist in the investigation of security threats or other attacks on the information assets;
v. Report security incidents and violations to the InfoSec manager; and
vi. Ensure that all critical operations are carried out in accordance with the security policy, standards and guidelines;

4.2.2 Authorities

i. Coordinate with asset custodian to assess the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of information or information systems in their unit's ownership/ custodianship;
ii. Coordinate with asset custodian to take appropriate closure actions for the audit observations and non-conformances; and
iii. Suggest department specific initiatives to enhance information security.

5. Chief Executive Officer (CEO)

5.1 Roles and Responsibilities

i. Ensure that security gaps pertaining to the respective departments are closed effectively;
ii. Ensure that their team members attend the Information Security awareness sessions planned as per the Information security team; and
iii. Ensure that the new employees within their respective teams are formally inducted after attending the Information Security awareness module.

6. Chief Technology and Information Officer (CTIO)

6.1 Roles and Responsibilities

The CTIO is accountable for development and maintenance of the information security at Ncell and to provide strategic direction.

6.2 Authorities

i. Review and approve initiatives recommended by InfoSec Manager/ Unit Heads to enhance information security;
ii. Ensure that periodic risk assessment is performed in accordance with the risk management procedure; and

7. Head of Network

7.1 Roles and Responsibilities

i. Ensure that security gaps pertaining to the respective departments are closed effectively;
ii. Approve exception/deviation from procedures whenever business justification is given;
iii. Ensure that their team members attend the Information Security awareness sessions planned as per the Information security team; and
iv. Ensure that the new employees within their respective teams are formally inducted after attending the Information Security awareness module.

8. Head of IT

8.1 Roles and Responsibilities

i. Ensure that security gaps pertaining to the respective departments are closed effectively
ii. Approve exception/deviation from procedures whenever business justification is given
iii. Ensure that their team members attend the Information Security awareness sessions planned as per the Information security team; and
iv. Ensure that the new employees within their respective teams are formally inducted after attending the Information Security awareness module
v. Ensure that root cause analysis is carried out, including investigations, for the reported security incidents
vi. Ensure IS effectiveness through audits, SLA/KPI reporting and governance programs;

9. Internal Audit Team

9.1 Roles and Responsibilities

i. Perform internal audit to check the effectiveness of information security;
ii. Identify the internal and/or external resources required to conduct the internal audits to ensure policies, procedures and manuals are consistently complied with;
iii. Report on the identified/assessed risks, non-conformities and provide recommendations for improvements Information security policies and procedures to sustain compliance;
iv. Verify and review the effectiveness of the corrective action taken to correct the deficiencies reported, if any, during the previous audit(s);

v. Inform the security officer about the results of the audit;
vi. Prepare audit report; and
vii. Report audit finding to the information security council.

10. Respective Function Head/ Risk Owners/Section Heads

10.1 Roles and Responsibilities

The various department heads shall have the following responsibilities:

i. Ensure that their team members are aware of and comply to Ncell’s Information Security Policy, procedures and standards;
ii. Ensure that their team members attend the Information Security awareness sessions planned as per the training calendar;
iii. Lead as PII controller, processor, asset owner and risk owner.
iv. Ensure that the new employees within their respective teams are formally inducted after attending the Information Security awareness module; and
v. Lead by example to promote a ‘security-aware’ corporate culture.

11. All Ncell Employees and Third-Party Employees

11.1 Responsibilities

Employees play a critical role in information security management at Ncell. Employees should follow and comply with the requirements of Information security, data security and the applicable legal and contractual obligations. All employees should undertake the necessary preventive precautionary, as well as designated reactive, steps with regards to incidents. Following are the responsibilities of all employees at Ncell:

i. Shall be aware of and comply to the information security Policy and Objectives;
ii. Ensuring active participation in IS initiatives like information security training and awareness, Information security audits, reviews, etc.
iii. To report about incidents/security breaches and suspected incidents to either their reporting manager or nominated InfoSec manager or security team;
iv. To understand the importance of data protection and data security responsibilities as part of their job functions;
v. Maintaining the strict confidentiality of personal data and organizational data;
vi. To dispose confidential and restricted information in their possession in accordance with the organizations disposal policy; and
vii. Taking all appropriate legal, organizational, and technical measures, in accordance with Ncell’s policies, to protect the confidentiality of organizations data, against accidental or unlawful disposal or accidental loss, alteration, unauthorized disclosure and against all other unlawful forms of processing, keeping in mind the nature of such data.

12. Governance and Compliance

i. Exception management process shall be followed to raise the exception for this procedure.
ii. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

13. Associated Documents

i. Information Security Policy
ii. ISMS/PIMS Procedure