Information Security Training and Awareness Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

	Ncell	Classification: Internal
Ncell logo	**Information Security Training and Awareness Procedure**	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Procedure Name DOCID: PR-IT-IS-05

	Ncell	Classification: Internal
Ncell logo	**Information Security Training and Awareness Procedure**	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Document Control

i. Document Identification

Document Title and Version:	PR-IT-IS-05 Information Security Training and Awareness Procedure v1.0
Effective Date:	01-09-2019
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	HR
Informed	All Employees and External Parties

iv. Digital Signature

CEO	CIO/Head Of IT

	Ncell	Classification: Internal
Ncell	**Information Security Training and Awareness Procedure**	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
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	01-09-2019	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	28-09-2023	Information Security Team	2. Review changed from annual to once every two years, 4. ISMR changed to Information Security Unit, ISC changed to RCMC, 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	

	Ncell	Classification: Internal
	Information Security Training and Awareness Procedure	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

	Ncell	Classification: Internal
	Information Security Training and Awareness Procedure	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

The purpose of this standard operating procedure is to define the Information Security Management System (ISMS) training and awareness framework for Ncell Pvt. Ltd. (hereinafter referred to as 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

Applicability of the training procedure is on all employees and ISMS roles defined as part of Governance procedure of Ncell

4. Responsibilities

The Information Security Team is responsible for developing, implementing, and maintaining the awareness and training program. All Ncell employees are responsible for participating in the program, for being knowledgeable about information security policies, and for complying with the procedures and instructions provided in the training. The progress on the training and awareness shall be presented to the senior management through appropriate forums such as Risk & Compliance Management committee (RCMC) meetings by the Information Security Team.

Following is the high level responsibility matrix for training and awareness activities as part of ISMS training procedure:

Sr. No.	Training & Awareness Program Activity	Responsibility
1.	Identification of training needs for ISMS roles & responsibilities, keeping in mind respective requirements	Information Security Team
2.	Approval on the identified training needs and competency requirements	Information Security Unit Head
3.	Preparation of training and awareness budget for the financial year	Information Security Team
4.	Approval on the training and awareness budget	Head of IT
5.	Preparation of a training calendar basis the identified training needs and competencies	Information Security Team
6.	Approval on training calendar	Information Security Unit Head
7.	Execution of training and awareness program	Information Security Team with support of HR
8.	Collective training feedback analysis and reporting results to Management	Information Security Team
9.	Review of training and awareness program & content on periodic basis	Information Security Team

5. Information Security Training Program

5.1 Training Needs Analysis

Training Needs Analysis is needed to enhance the capability of employees having Information Security Management roles and to bridge the gaps in performance for achieving the overall information security objectives.

Training needs shall be identified and drafted by the Information Security team by considering the role requirements, functional focus, individual development, etc. It shall be approved by the Head of HR Learning & Development. In addition, ISWG members are also expected to discuss their requirement of information security management training with the Information Security Team.

The information security management training program will be driven by the Training Needs Analysis, which is conducted annually (or due to major organizational change).

[Refer Appendix A: S. No. A1-Training Needs Analysis]

	Ncell	Classification: Internal
Ncell logo	**Information Security Training and Awareness Procedure**	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

5.2 Training Design Development and Delivery

It is the responsibility of the Information Security Team at Ncell to develop and deliver the information security training programs in coordination with the Information Security Team and HR Learning & Development team. The development of the training program shall consider the following parameters:

i.   Mode of Delivery (Internal/ External);
ii. Identification of Instructor/ vendor;
iii. Training content and material; and
iv. Cost of the training program.

It is the responsibility of the Information Security Team.to choose internal or external trainer for any of the management system role based training programs, in discussion with the ISC.

5.3 Training and Awareness Program Calendar

Training Calendar shall be drafted by the Information Security Team. The Information Security Team. has the authority to evaluate and prioritize the information security management system training based on the urgency of the need (timelines), the extent of the need (how many employees need to be trained) and the scope of training. The training program will be eventually be signed off by the Information Security Team..

The following information security management system role-based needs shall be considered while formulating the training and awareness program calendar:

S. No.	Information Security Management System Training type	Recipient
1.	Understanding of the international ISMS standard ISO 27001:2013 and NIST framework.	Information Security Team., Network Security & Audit Team and ISWG members
2.	Initial information security awareness in Employee Induction Program	All new joiners
3.	All employee general information security awareness	All employees of Ncell
4.	Communication of responsibilities for roles defined as per ISMS Governance Structure. This can be achieved through classroom sessions or by conveying responsibilities over emails.	Identified members of: • Information Security Steering Committee • Information Security Management Representative • Information Security Working Group • Internal Auditor • Facility Manager

5.4 Training Execution

5.4.1. Training program communication

The HR Learning & Development team shall ensure communication about the schedule and venue of the trainings to the nominated employees as per the developed training calendar. In case the participants are not able to attend the training program, an approval from the reporting manager is to be submitted to the HR with a copy to the Information Security Team with business justification.

5.4.2. Training program logistics

The HR Learning & Development team shall arrange for training logistics such as training room, stationery, projector requirements and other arrangements during training sessions.

5.4.3. Training program delivery and monitoring effectiveness

The Information Security team shall be responsible to execute ISMS training and awareness program as per their roles and responsibilities and identified needs. A post-training evaluation will be conducted to measure the effectiveness of the training imparted. Training shall be considered to be effective if a score of 70% and above is achieved by the employee during post-training evaluation. Basis the results, further improvements shall be made either with the conduct of repeat training sessions or content revision of the training modules.

	Ncell	Classification: Internal
Ncell	**Information Security Training and Awareness Procedure**	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

5.5 Training Feedback

Wherever feasible, the Information Security Team shall obtain feedback from the training participants, post the training session. The collective feedback analysis report, based on inputs from all participants shall be shared with the Information Security Team.for future improvement of the program.
[Refer Appendix A: S. No. A3-Training Feedback Form]

6. Information Security Awareness Program

Awareness programs are critical to promote and embed the information security management culture at Ncell. The awareness programs shall be conducted at Ncell to make all employees aware of their responsibilities towards information security and to make them cognizant of their roles and responsibilities during an information security incident.
Following mechanism may be utilized to successfully run awareness campaigns at Ncell:

i. **Awareness through emails:** Useful information security hints and tips, consisting of key points emphasized during the trainings may be communicated to all employees through emails;
ii. **Computer desktop wallpapers and screensaver:** The IT Office Support team, with guidance from the NSA team can apply relevant desktop wallpapers and screensavers to all machines making employees aware of information security responsibilities; and
iii. **Visuals:** Posters and flyers communicating security tips may be distributed across the premises to create conceptual awareness.
iv. **Intranet:** Useful information security hints and tips, consisting of key points emphasized during the trainings may be communicated to all employees through the organization's intranet portal;

6.1 Measuring Awareness & Effectiveness

6.1.1. Quizzes

The Information Security Team, in consultation with the HR may conduct quiz on information security as per program calendar

6.1.2. Rewards and Recognition

Rewards and recognitions may be given to employees performing well in training and awareness initiatives.

7. Management Reporting

The Information Security team shall be responsible for consolidating the details (training results, feedback, and awareness effectiveness) of the training and awareness sessions conducted at Ncell in the form of a Training MIS. The Information Security Team.shall provide an update on the progress of training and awareness activities to the ISC during scheduled information security Management Review Meetings.

Appendix A

Annexure No	Template/ Form Name
A1	Ncell_ISMS_Training Needs Analysis Templ
A2	Ncell ISMS Training MIS Template .xlsx

	Ncell	Classification: Internal
Ncell	**Information Security Training and Awareness Procedure**	Owner: CIO/Head of IT
		Effective Date: 01-09-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Annexure No	**Template/ Form Name**
A3	Training Feedback Form.doc