

Information Security Policy

Ncell

Policy

Approved Date:- 05/12/2016


Procedure Name DOCID: Ncell-ICT-2016-0187 Information Security Policy

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

	Ncell	Classification: Internal
	Information Security Policy	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity and Process Management	Approved by MD/CEO

Ncell	Ncell	Classification: Internal
	Information Security Policy	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity and Process Management	Approved by MD/CEO

v. Revision History

Rev	Date	Author	Description	Approved By	Approval Initiated Date
0	2016-09-06	Yasmine Bhattarai	Initial Document Created	CIO	
1	2016-11-18	Yasmine Bhattarai	Minor editing and formatting	CIO	
2	2016-12-05	Simon Perkins	Approval	CIO	
3	2019-04-16	Yasmine Bhattarai	Policy updated to close identified gaps and to align to Axiata IS Policy	CIO	
Do 4	2022-10-14	Tarani Prasad Chaudhary	Change in 5.1.5 Chief Privacy Officer from UH to CIO. Formatting as per new document control	CIO	2022-10-14
5	2024-04-25	Information Security team	Re-branding	CIO/Head of IT	



	Ncell	Classification: Internal
	Information Security Policy	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity and Process Management	Approved by MD/CEO

Table of Contents

1. DESCRIPTION	4
1.1 Description	4
2. SCOPE AND PURPOSE	4
2.1 Scope	4
3. Purpose	4
4. PRINCIPLES	4
5. ROLES AND RESPONSIBILITIES.....	5
5.1 Governance Roles	5
5.1.1 Chief Information Security Officer (CISO).....	5
5.1.2 Board of Directors	5
5.1.3 Single point of Contact (SPOC).....	5
5.1.4 Data Privacy Officer (DPO)	Error! Bookmark not defined.
6. OTHER ROLES	6
7. MINIMUM SECURITY REQUIREMENTS	6
8. EXEMPTIONS	7
9. REFERENCES	7

	Ncell	Classification: Internal
	Information Security Policy	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity and Process Management	Approved by MD/CEO

1. DESCRIPTION

1.1 Description

This is the Security Policy stating the mandatory information security requirements.

Security is an integral part of sound governance. The governance of information security within Ncell is coordinated by Information Security Office in cooperation with all parts of the organization. It aims to control, facilitate, and implement well-balanced security measures throughout our operation.

2. SCOPE AND PURPOSE

2.1 Scope

This Policy shall be applicable to all Ncell employees, third party vendors, contractors, partners and others, including but not limited to subsidiaries, who have access to Ncell computers/systems/network and/or data.

3. Purpose

In Ncell, security measures shall be characterized by appropriate security and risk awareness, prevention, preparedness, and the ability to respond to, and recover from, incidents and changes in the environment. The main drivers for security are:

- Protection of the company's assets and investments
- Ensuring that customers' expectations and business agreements are met
- Ensuring that the business strategies and objectives are not jeopardized due to security risks
- Ensuring that laws and regulatory security related requirements are complied with (legal compliance).

4. PRINCIPLES

The following principles shall apply for the activities under this Policy:

1. Ncell shall implement security measures, which aims to balance risk exposure, business value, vulnerabilities and threats.
2. In order to protect business, measures must be taken to protect assets such as personnel, customers, information, IT infrastructure, internal and public networks, as well as office buildings and technical facilities. Information security is vital for ensuring reliable and secure access to information. Ncell shall implement measures to prevent and detect disclosure of sensitive information to unauthorized parties. Special attention shall be given to information affecting user privacy.
3. Products, services, and key strategic and operational processes must continuously, throughout its life cycle, undergo thorough analysis to identify risks and threats affecting our business. The analysis aims to guide decision making and ensure proper implementation of security measures to meet compliance and balance risk exposure.
4. Ncell does not accept criminal activities or fraud. Appropriate measures, including data preservation, shall be in place to enable detection and prompt response to security incidents and fraud.

Ncell	Ncell	Classification: Internal
	Information Security Policy	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity and Process Management	Approved by MD/CEO

5. All Ncell employees and line managers are obligated to report security incidents and fraud according to established routines.
6. Ncell must ensure that critical business functions will be available to customers and other stakeholders. Business continuity plans must be in place for all business-critical services to maintain service resilience and recoverability according to business, legal and regulatory demands.
7. To ensure Ncell's ability to handle unpredictable events, a crisis management organization and corresponding plans must be in place.
8. Security audits (follow-ups) shall continuously be conducted to ensure implementation of corrective actions and compliance to policies, instructions, and legal/regulatory demands. Non-compliance of the Security Policy shall be reported to the Security Officer.
9. These principles apply to the extent that they do not place Ncell in violation of domestic laws and regulations.

5. ROLES AND RESPONSIBILITIES

5.1 Governance Roles

5.1.1 Chief Information Security Officer (CISO)

This role is held by the Information Security Unit Head and all below related responsibilities will be handled by Information Security Unit Head:


- Performing information security duties as the primary duty.
- Heading an office with the mission and resources to assist in ensuring compliance with information security requirements.
- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;
- Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of Ncell;
- Ensuring that employees, including contractors, receive appropriate information security awareness training;
- Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices.
- Developing and implementing procedures for detecting, reporting, and responding to security incidents;

5.1.2 Board of Directors

The Information Security policy is approved by Board of Directors. Any updates must also be approved by the Board of Directors

5.1.3 Single Point of Contact

This role of Single Point of Contact (SPOC) for Security can be in IT and Technology or wider range within organization, appointed by respective line managers to support the Information Security Team. The information system security officer is the official assigned responsibility by the CISO,

	Ncell	Classification: Internal
	Information Security Policy	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity and Process Management	Approved by MD/CEO

authorizing official, management official, or information system owner for ensuring that appropriate operational security posture is maintained for an information system or program. The information system security officer has the following responsibilities related to system security plans:

- Assists the Chief information security officer in the identification, implementation, and assessment of the common security controls.
- Plays an active role in developing and updating the system security plan as well as coordinating with the information system owner any changes to the system and assessing the security impact of those changes.

5.1.4 Data Privacy Officer

The responsibilities under this role will be handled by Unit Head of Information Security until otherwise communicated. Detail roles and responsibilities are governed by Data Privacy Governance Procedures.

6. Other Roles

Each Director reporting to the MD/CEO of Ncell is responsible for ensuring that this Policy is duly communicated and implemented, and that the employees within his/her area of responsibility are familiar with and follow this, Policy.

All Ncell employees are however individually responsible for reading, understanding and following this Policy. Each employee is also obliged to speak up and raise concerns about actual or possible violations of this Policy.

Violations of this Policy can lead to disciplinary action up to and including termination.

7. Minimum Security Requirements

7.1 Access Control

Please refer to Access Management Procedure

7.2 Password management

Please refer to Password Management Guidelines

7.3 vulnerability and Patch Management

Please refer to vulnerability and Patch Management Procedure

7.4 Data Loss Prevention

Please refer to Data Loss Prevention Procedure

7.5 Privileged Access Management

Please refer to Privileged Access Management Procedure

7.6 Project Go Live

Please refer to Project GoLive Procedure

7.7 Training and Awareness

A. Security Awareness Training

Ncell	Ncell	Classification: Internal
	Information Security Policy	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity and Process Management	Approved by MD/CEO

Provide basic security awareness training to information system users (including managers, senior executives, and contractors):

- As part of initial training for new users;
- When required by information system changes; and
- At least annually thereafter.

B. Role-based Security Training

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

- Before authorizing access to the information system or performing assigned duties
- When required by information system changes; and
- At least annually thereafter.

8. EXEMPTIONS

If there will be any exemptions to this policy, such exemption(s) must be approved by the MD/CEO of Ncell.

9. REFERENCES

NIST Cybersecurity Framework is available online at:

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>