

# Encryption Guidelines

Ncell

Guidelines

Approved Date:- 13/12/2019

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Encryption Guidelines</b>	Owner: CIO/Head of IT
		Effective Date: 01-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Guideline Name DOCID: GD-IT-IS-08

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
	Encryption Guidelines	Owner: CIO/Head of IT
		Effective Date: 01-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

i. Document Identification

<b>Document Title and Version:</b>	<b>GD-IT-IS-08 Encryption Guidelines</b>
Effective Date:	01-10-2019
Document Author:	Information Security Team
Owner:	Information Security Team
Approved By:	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	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO

CIO/Head Of IT

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Encryption Guidelines</b>	Owner: CIO/Head of IT
		Effective Date: 01-10-2019
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	01-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	05-12-2019
1	13-12-2019	Tarani Prasad Chaudhary	Revised-Formatting	Andy Chong	13-12-2019
2	22-09-2019	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
3	19-12-2019	Tarani Prasad Chaudhary	Revised-Formatting	Andy Chong	20-12-2019
4	18-08-2023	Information Security Team	2. Review : changed from annually to once in every two years. 4.1 : McAfee is changed to tools 4.4.v: either Triple DES or AES is changed to secure 4.4.vi: such as WPA2 part is removed 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	25-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Encryption Guidelines</b>	Owner: CIO/Head of IT
		Effective Date: 01-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## Table of Contents

<b>Document Control</b> .....	1
<b>1. Purpose</b> .....	5
<b>2. Review and Updating</b> .....	5
<b>3. Scope</b> .....	5
<b>4. Requirements for Encryption</b> .....	5
<b>4.1 Encryption of Laptops</b> .....	5
<b>4.2 Encryption for Backup Media</b> .....	5
<b>4.3 Encryption for passwords</b> .....	5
<b>4.4 Encryption for Data Transmission</b> .....	5
<b>5. Key Management</b> .....	6
<b>6. Governance and Compliance</b> .....	6
<b>7. Associated Documents</b> .....	6

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Encryption Guidelines</b>	Owner: CIO/Head of IT
		Effective Date: 01-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## 1. Purpose

The purpose of this document is to lay out guidelines for encryption requirements for the information assets being used across the organisation.

## 2. Review and Updating

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

## 3. Scope

The Encryption Standard is applicable to all critical systems storing sensitive information and having an asset criticality rating of greater than or equal to 4.

## 4. Requirements for Encryption

### 4.1 Encryption of Laptops

- i. All data stored on the Windows operating system volume shall be encrypted, using McAfee full disk encryption.
- ii. The normal boot process shall be locked until an appropriate password is entered by the user. The password shall be in accordance with Ncell's Password Management guidelines

### 4.2 Encryption for Backup Media

- i. The Ncell's approved backup solution shall be configured to encrypt data using the 128-bit Blowfish algorithm;
- ii. Integrity testing of a sample of backup tapes shall be performed to ensure integrity and availability of data.

### 4.3 Encryption for passwords

- i. Passwords stored in databases shall be protected by using strong one-way hashes (e.g. MD5), Triple DES (128-bit), AES (256-bit).
- ii. All keys and passwords shall be stored in a secure location and access shall be restricted to authorized personnel.

### 4.4 Encryption for Data Transmission

- i. **File transfers:** File transfers shall be performed via the use of an encrypted transmission protocol or network service such as Secure Copy (SCP), OpenSSH, Secure FTP (SFTP), FTP over SSL (FTPS) and Very Secure FTP Daemon (VSFTPD);
- ii. **Interactive sessions:** Login passwords, transmitted during remote login sessions shall be provided using secure applications or protocols;
- iii. **Web-based applications:** Sensitive data communicated between a user's browser and a web-based application shall be provided using secure protocols (e.g., HTTPS, TLS/SSL, etc.). Certified SSL certificates shall be used on Ncell websites to protect the data between browser and server against interception;
- iv. **Application to application communication:** Encryption of sensitive data transmitted between applications shall be provided using commonly available encrypted protocols (e.g., HTTPS) to prevent unauthorized interception;
- v. **Virtual Private Network:** A VPN connection shall be employed to offers an additional option to protecting sensitive data transmitted via the network. IPsec VPN channels shall be used configured with either Triple DES or AES encryption to guard against unauthorized access of data; and
- vi. **Wireless connections:** Wireless (Wi-Fi) transmissions that are used to access Ncell's portable computing devices or internal networks shall be encrypted using secure standards such as WPA2.

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Encryption Guidelines</b>	Owner: CIO/Head of IT
		Effective Date: 01-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## 5. Key Management

It is recommended that key management practices such as the following should be in place:

- i. To ensure that the confidentiality of the secret key is protected, it should be secured by logically and physically securing the device on which the key is stored;
- ii. The shared secret key shall be accessible only by authorized personnel on a need-to-know basis;
- iii. Keys shall be revoked and generated afresh in case of suspected compromise;
- iv. Audit trails of key management activities shall be stored and protected;
- v. Internal CA systems should be managed securely with appropriate physical and logical controls;
- vi. Secure backup of internal CA private keys should be maintained on an independent secure media which provides a source for key recovery. Backed up keys shall be protected from physical and environmental threats. A copy of the backed-up keys should be stored at an off-site location for protection against major failure and/ or disaster;
- vii. Cryptographic keys should be destroyed in a secure manner when they are no longer required;
- viii. Split knowledge / dual control (two persons know their parts of the key, to reconstruct the whole key) shall be required for use of cryptographic key;
- ix. No copy of user's private key should be retained by the internal CA to avoid risk of repudiation; and
- x. Users should keep their private keys strictly confidential and shall be responsible for the safety of their private keys.

## 6. 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.

## 7. Associated Documents

- i. Information Security Policy
- ii. Security Incident Management Procedure