


Mobile Device Security Guidelines

Ncell

Guidelines

Approved Date:- 05/12/2016

	Ncell	Classification: Internal
	Mobile Device Security Guidelines	Owner: CIO/Head of IT
		Effective Date: 5-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Guideline Name DOCID: GD-IT-IS-03

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
	Mobile Device Security Guidelines	Owner: CIO/Head of IT
		Effective Date: 5-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Document Control

i. Document Identification

Document Title and Version:	GD-IT-IS-03 Mobile Device Security Guidelines v2.0
Effective Date:	05-12-2016
Document Author:	Information Security Team
Owner:	CIO/Head of IT
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	Information Security Team and Function Heads
Informed	All Employees and Relevant External Parties

iv. Digital Signature

CEO

CIO/Head Of IT

	Ncell	Classification: Internal
	Mobile Device Security Guidelines	Owner: CIO/Head of IT
		Effective Date: 5-12-2016
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	05-12-2016	Information Security Team	Initial document	Simon Perkins	05-12-2016
1	01-09-2019	Information Security Team	Revised-Formatted and aligned with current processes	Vishal Mani Upadhyay	13-12-2019
2	13-12-2019	Tarani Prasad Chaudhary	Revised-Formatting	Andy Chong	13-12-2019
3	21-09-2019	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	13-12-2021
4	13-12-2019	Tarani Prasad Chaudhary	Revised-Formatting	Andy Chong	14-12-2019
5	12-10-2023	Information Security Team	2. Review : changed from annually to once in every two years. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
6	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
7	30-04-2024	Information Security Team	Re-branding	CIO/Head of IT	


	Ncell	Classification: Internal
	Mobile Device Security Guidelines	Owner: CIO/Head of IT
		Effective Date: 5-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

Document Control	2
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Responsibilities	5
4.1 IT Service Desk / Help Desk	5
4.2 Mobile Device Owners	5
5. Guidelines	5
6. Loss or Change of Mobile Devices	6
7. Governance and Compliance	6
8. Associated Documents	6

Ncell	Ncell	Classification: Internal
	Mobile Device Security Guidelines	Owner: CIO/Head of IT
		Effective Date: 5-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

Mobile devices, be it tablets or phones, have become an integral part of today's corporate world, with company data, at least corporate emails, residing in personally owned mobile devices. Securing such corporate information in personally owned mobile devices becomes a challenge. The purpose of these guidelines is to control and secure corporate information in employees' mobile devices.

2. Review and Updating

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

3. Scope

This document applies to all mobile devices which have Ncell corporate email and/or RSA SecureID application (token generator for authentication into Ncell Virtual Private Network systems) configured. This also applies to the mobile devices which connects to Ncell corporate network via VPN solution.

4. Responsibilities

4.1 IT Service Desk / Help Desk

IT Service Desk / Help Desk team shall be the main point of contact for users. If a mobile device is lost and email configuration needs to be wiped, and/or VPN authentication configuration removed, the user shall inform the manager and the IT Service Desk / Help Desk team who shall wipe the Ncell email configuration from the device remotely.

4.2 Mobile Device Owners

The device owners are responsible to ensure security of their devices. They are also responsible to inform IT Service Desk / Help Desk via their managers, in case the mobile device is lost or stolen.

5. Guidelines

- i. Device must authenticate the user before access to services. Strong password controls in line with the Password Management Procedure shall be employed;
- ii. Devices must be configured to timeout/Auto lock after defined minutes of inactivity as per the Password Management Procedure and must require re-authentication before access to services. The authentication mechanism(s) must not be disabled;
- iii. Users shall take due care and due caution when connecting Ncell laptops to public networks (E.g.: Wi-Fi hot spots). User will be responsible for any resulting security breach;
- iv. Devices must be configured to lock-out after defined number of incorrect password login attempts by the user, defined as per the Password Management Procedure;
- v. Ncell approved full-disk encryption mechanism shall be enabled on laptops that transmit or store Ncell's confidential information.
- vi. USB ports shall be restricted and monitored. Blue tooth and CD/DVD writers shall be blocked or be in read-only mode by default and allowed only on a 'need-to-have' basis on approval of line management and Information Security Team.
- vii. User of personal devices shall not try to gain unauthorized access to Ncell services, run port scans, use penetrating testing tools, use any hacking tools in Ncell network;
- viii. Users of personal devices shall not allow a third party to intentionally or unintentionally gain access to Ncell services;
- ix. Users of personal devices need to ensure devices are patched to the latest version and have appropriate anti-virus product installed;
- x. Personal handheld devices must be secured against unauthorized usage by using a password. Such a password is not to be shared within or outside Ncell premises. Users must also ensure that their device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes;
- xi. Users are accountable for their personally-owned handheld devices and must protect them to minimize the possibility of loss or theft, unauthorized use, or tampering; and

Ncell	Ncell	Classification: Internal
	Mobile Device Security Guidelines	Owner: CIO/Head of IT
		Effective Date: 5-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- xii. Mobile devices must not be left unattended in an unsecure area. When removed from a secure location they must, whenever practical, be kept out of sight when not in use.

6. Loss or Change of Mobile Devices

- i. In case the mobile device is lost or stolen, the user shall immediately wipe out the data on the mobile device themselves or with the support of the IT Service Desk / Help Desk Team.
- ii. In case of theft of the mobile device, a complaint shall be registered with the police by the user.

7. Governance and Compliance

- i. There shall be no exceptions to these guidelines.
- ii. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

8. Associated Documents

- i. Asset Management Procedure
- ii. Password Management Procedure
- iii. Media Handling Guidelines