Remote Access Guidelines

Ncell

Approved Date:- 05/12/2016

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

Guideline Name DOCID: GD-IT-IS-09

Document Control

i. Document Identification

Document Title and Version:	**GD-IT-IS-09 Remote Access Guidelines**
Effective Date:	05-12-2016
Document Author:	Information Security Team
Owner:	CIO/Head of IT

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

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	01-10-2019	Information Security Team	Revised – Formatted, Added detailed procedure for VPN access to external parties		
2	05-12-2020	Information Security Team	Revised – No Change	Andy Chong	15-12-2020
3	18-08-2023	Information Security Team	2.Changed review period to once every two years 4. Definition of MFA added 6.1.vi and 6.2.ii One Time password and passphrase changed to MFA 6.3.v Enforcement of MFA for CJ vendors 7.1 access as per access management procedure Added Head of IT		
4	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
5	13-05-2024	Information Security	Re-branding	CIO/Head of IT	

Table of Contents

1. Purpose

The purpose of this guideline is to define standards for connecting to Ncell's network from any systems remotely. These standards are designed to minimize the potential exposure to Ncell from damages which may result from unauthorized use of Ncell resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ncell internal systems, etc.

2. Review and Updating

This procedure shall be reviewed once in every two years or whenever significant changes occur in the organization.

3. Scope

This guideline applies to all Ncell employees, contractors, vendors and agents with a Ncell-owned or personally-owned computer or workstation or other mobile devices (tablets, smart phones) used to connect Ncell network remotely. The requirements stated in this guideline shall be considered by the project owner or solution owner when agreements are made with third parties and vendors

4. Definitions

i. **IPSec:** Internet Protocol security (IPSec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks using cryptographic security services.
ii. **Remote Access:** Any access to Ncell's network through a non-Ncell controlled network or medium.
iii. **SSH:** Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
iv. **VPN:** A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to their organization's network.
v. **MFA:** Multi factor authentication is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

5. Roles and Responsibilities

5.1 Transport Network Team

Transport Network Team shall be responsible for enforcing the requirements of this guidelines for all systems connected to Ncell network that can be connected remotely. This team shall be responsible to provide adequate network security to systems that do not need remote connection.

5.2 System Owners

System owners shall be responsible for ensuring that their systems are not accessible remotely if not required and if required, then adequate security mechanisms shall be put in place to protect the system and log the access of remote users for audit purposes.

5.3 Information Security Team

The Information Security Team shall be responsible for approving non-standard connections to Ncell network.

5.4 Department Directors

Department directors shall be responsible for ensuring that employees under their supervision follow and comply with this guideline.

5.5 Employees

Employees shall take optimum care while accessing Ncell systems remotely. Users shall be responsible for ensuring that they are sufficiently familiar with the remote access operation before gaining access for remote connection. At all times, users shall need to exercise caution while using remote access connection such that confidential information in not disclosed in public or even to family members.

6. Remote Access Guidelines

6.1 Remote Access Usage

i. Remote access to Ncell equipment is to be used for the business purposes only; all other activities are strictly Prohibited.
ii. It is the responsibility of employees, contractors, vendors, and agents with remote access privileges to Ncell's network to ensure that their remote access connection is given the same consideration as the user's on-site connection.
iii. Non-standard remote access connection configurations shall be approved by Transport Network Team. Organizations or individuals who wish to implement non-standard remote access solutions to the Ncell network shall obtain prior approval from Transport Network Team and Information Security team.
iv. All computers (including personal computers) that are connected to Ncell internal networks via remote access technologies shall use the most up-to-date anti-virus, anti-malware software.
v. Users shall not use remote access connections to access the internet for outside business interests.
vi. Remote access shall be strictly controlled with encryption (i.e., VPNs) and MFA.
vii. The following actions shall be strictly prohibited:
    a. Attempting to bypass the remote access session authentication process.
    b. Allowing non-authorized person to access information/services obtained via remote access.
    c. Performance of illegal activities (e.g.: using pirated material, harassment) through the network by any use.

6.2 Ncell Users

i. By default, Ncell employees can access their mails remotely.
ii. Ncell employees shall be provided VPN access to Ncell network on request. They shall be required to use multi factor authentication to connect to Ncell network.
iii. Remote access is a privilege and shall be regarded as Ncell's faith in its employees to act responsibly.
iv. Users shall protect their login credentials, even from family members.
v. Users shall be responsible for protection of Ncell information and are accountable for the inappropriate use and dissemination of the information obtained through remote access communications.
vi. Personal equipment that is used to connect to Ncell networks shall meet the requirements as of Ncell owned equipment for remote access.
vii. Users shall not use public infrastructure (WiFi) to access Ncell network remotely.
viii. All employees with remote access privileges shall ensure that their laptop, which is remotely connected to Ncell network, is not connected to any other network at the same time, except for personal network under the control of employees.
ix. Should remote access be misused, the employee shall bear all responsibility for the consequences.

6.3 External Teams

i. External teams of third-party contractors and vendors shall establish IPSec tunnel via Ncell equipment for remote connection.
ii. Bypassing Ncell remote access solution for remote access to Ncell equipment shall not be permitted.

iii. Support Teams shall be allowed access to the systems that are under their support. Their activities shall be monitored.
iv. Secure remote access shall be strictly controlled. Control shall be enforced via multifactor authentication or encryption keys, wherever applicable.
v. For crown jewel vendors, multifactor authentication shall be enforced.

6.4 Audit

All remote access connections shall be logged, and the logs reviewed. It shall be possible to monitor the activities of the remote access users in the network. These logs shall be reviewed when required.

7. General Procedures

7.1 Gaining Remote Access

For both Ncell employees and external parties access shall be granted as per Access Management Procedure[1]

7.2 Security Incident

If any Ncell equipment connected to Ncell network is suspected to have been compromised via remote access, the incident shall be reported to the Information Security Team

8. 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.

9. Associated Documents

i. Information Security Policy
ii. Security Incident Management Procedure
iii. Access Management Procedure

[1] PR-IT-IS-07 Access Management Procedure