

Network Security Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

Ncell	Ncell	Classification: Internal
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Procedure Name DOCID: PR-IT-IS-11

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
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

i. Document Identification

Document Version:	Title and	PR-IT-IS-11 Network Security Procedure
Effective Date:		1 st October, 2019
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	Transport Network Team
Accountable	CIO/Head of IT
Consulted	Information Security Team
Informed	All Employees and External Parties

iv. Digital Signature

CEO

CIO/Head Of IT

v. Revision History

Ncell	Ncell	Classification: Internal
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Rev	Date	Author	Description	Approved By	Initiated Date
0	01-10-2019	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	26-09-2023	Information Security Team	2. Review changed from annual to once every two years 4.5.iv Firewall rules review changed to annual for DMZ firewall and removed for rest 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
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

Document Control	1
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Network Security Controls	5
4.1 Network Diagram	5
4.2 Hardening	5
4.3 Password Management	5
4.4 Use of Router Access Control List	5
4.5 Use of Firewall	5
4.5.1 Firewall Rule Review	5
4.6 Use of Network Sniffers	6
4.7 IP Assignment and Backup	6
4.8 Network Monitoring and Security Settings	6
4.9 Wireless Security	6
4.10 Wireless Access Points	7
5. Governance and Compliance	7
6. Associated Documents	7

	Ncell	Classification: Internal
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

This document sets out Ncell's policy for the protection of the confidentiality, integrity and availability of the network, establishes the security responsibilities for network security and protect the network from unauthorized or accidental modification ensuring the accuracy and completeness of the organization's assets.

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 procedure applies to all networks within Ncell used for information systems and information processing facilities.

4. Network Security Controls

4.1 Network Diagram

- Ncell should have a formally documented and approved network diagram.
- The network diagram should be updated in case of any changes and should be reviewed annually by the Packet Transport Network team.
- Updated Diagram approval should be done via Jira. The process shall be governed by the respective Section Manager.

4.2 Hardening

- All network devices (server, routers, and firewalls, IPS, IDS, load balancers, switches etc.) should undergo hardening before being put in production. Changes to these devices should be tracked through change management process.
- Network Time Protocol (NTP) Synchronization should be implemented for all devices in the network to ensure that all devices have uniform time to ensure consistency in timestamps captured in logs

4.3 Password Management

- The Transport Network team should ensure that default passwords of all network equipment (i.e. routers, switches) should be changed when installed.
- Password composition and rotation of all network equipment should be in accordance to the organization's password management guidelines.

4.4 Use of Router Access Control List

- The Transport Network team should use access control lists on routers to restrict unauthorized users from accessing the company's network.

4.5 Use of Firewall

- All hosts that run applications or contain data that are non-public must be isolated behind a firewall from external networks.
- All traffic from inside Ncell to external networks, and vice-versa, must pass through the firewall.
- Only authorized traffic, as defined by the Network Administrator, should be allowed to pass.
- Firewall rules should be reviewed at least annually by the Network Administrator for DMZ firewall.
- Changes in firewall rules (if any) should be routed through the change management procedure.
- Network should be segregated (e.g. using firewall) to separate zones for web, applications, database, management consoles etc based on risk.
- The placement of network devices in the DMZ should be based on the risk for the device.

4.5.1 Firewall Rule Review

The Transport Network team should review the rules for the DMZ firewall annually and remaining firewalls annually based on the following inputs :-

Ncell	Ncell	Classification: Internal
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- i. The team should consider deleting any unnecessary rules in place.
- ii. The team should consider adding new rules in place keeping the business needs in mind.
- iii. The team should consider reducing the load by filtering out the unwanted traffic via Edge routers.
- iv. The team should review the devices listed in the rule list and should remove the devices on regular basis which are have been decommissioned.
- v. The team should give 1st priority to all "Deny All" rules defined.
- vi. The teams should avoid the use of "Any" in "Allow" firewall rules, due to potential traffic and flow control issues. Use of "Any" may have the unintended consequence of allowing every protocol through the firewall.
- vii. The teams should ensure that all rules are documented and approved.
- viii. The teams should inform the relevant stakeholders/admins before implementing a firewall rule.

4.6 Use of Network Sniffers

- i. Only authorized security testers may use packet/data capturing tools on Ncell's network.
- ii. Such tools should only be used for troubleshooting purposes.
- iii. The team should use such tools after taking approval from Networking-in-charge and under notice to Information Security Team, who will keep the record of all such usage.
- iv. The authorized security testers may use sniffing tools with proper authorization from the Information Security Officer.
- v. Data captured using sniffers should be deleted once the troubleshooting is completed, if the captured data is required to be sent out of Ncell then approval needs to be taken from the Head of IT.

4.7 IP Assignment and Backup

- i. IP assignment to network devices should be based on restrictions as to usage of Public and Private IP address range.
- ii. The configuration files of core network devices should be backed up.
- iii. Whenever changes are made in the configuration, revised configuration file should be backed up.

4.8 Network Monitoring and Security Settings

- i. Use of security event logging - All system platforms and all applications that utilize restricted information should have security related event logging. Log files generated should never be overwritten or deleted until they are backed up in off-line storage. Log files must, at a minimum, record login failures, remote access, modem logs, account lockouts and system administrator actions.
- ii. Packet Transport Network team should use tools to monitor the network operations and provide alerts of unusual activity to the Information Security Team. Evaluation of such products should be done by the Packet Transport Network team in consultation with the Information Security team.
- iii. Tools used for monitoring of servers should be configured for adequate security
- iv. Critical network devices should be periodically reviewed for change management adherence by Head of Department.
- v. All critical segments in DMZ should be protected by NIDS/NIPS
- vi. Concurrent login should be disabled for User IDs with administrative privileges

4.9 Wireless Security

- i. After the initial configuration of Wireless WAN Devices, default Authentication key, SNMP String should be changed and should be kept securely as a confidential document in joint custody
- ii. All the points from where wireless network is integrated to Ncell's network should be identified and protected
- iii. All administrative activities and user session details for Wireless WAN devices should be logged
- iv. Appropriate Network Access Control shall be used to ensure only registered devices should be able to connect to WLAN
- v. Wireless WAN Devices should be monitored continuously for availability and unauthorized access.
- vi. Patches for wireless devices should be updated in accordance with Ncell's Vulnerability and Patch Management procedure.

Ncell	Ncell	Classification: Internal
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- vii. Ncell shall implement multi-factor authentication for authenticating users connecting to wireless networks.
- viii. Separate networks for Ncell employees to access internal network resources and guest-only having restricted permissions must be established.
- ix. Wireless devices should be configured securely including following settings:
 - a. Enable centralized user authentication for the device administrators.
 - b. Choose secure version of Simple Network Management Protocol (SNMP) and set strong SNMP authentication credentials.
 - c. Disable any nonessential services/ protocols provided by the manufacturer
 - d. Use secure protocols, such as Secure Shell protocol (SSH) for administration activities. Telnet should not be used for administration activities.
 - e. Services not in use for remote device management e.g. telnet, ftp, http etc. should be disabled
 - f. IP addresses of clients should be predefined and configured.
 - g. SSID Broadcast should be disabled on the access points
 - h. Power settings of access points should be restricted to the area of usage in order to avoid signal spillage
 - i. Proper channel selection should be ensured in order to avoid RF interference
 - j. Access Points used in the wireless network should be configured to allow propagation of wireless signals only in the identified area.
- x. Only approved device/user authentication mechanisms should be used to connect a Wireless Client to Ncell's network
- xi. In addition, 'MAC (Media Access Control) address based authentication' should be used for wireless clients to provide first level of authentication control against access from unauthorized clients and also to limit access to only approved MAC addresses. MAC authentication along with authentication credential will provide two-factor authentication.
- xii. Authentication keys configured should be complex and not easily guessable
- xiii. Weak authentication schemes such as 'Open or shared key authentication' should not be used.
- xiv. An additional layer of encryption should be used over the wireless traffic
- xv. The area which needs wireless WAN accessibility should be identified and the wireless signal strength should be controlled to restrict the accessibility only to that identified area.

4.10 Wireless Access Points


- i. Network devices used for wireless network should be secured from physical access.
- ii. Physical Security of network devices used for wireless network should be ensured by the respective administrative offices.
- iii. Access points should be secured using mounting locks
- iv. Indoor devices should be secured physically and kept under lock and key to prevent unauthorized access
- v. Locked enclosures should be used to protect outdoor equipment from vandalism, theft etc.
- vi. Ethernet cable that connects the outdoor equipment and the indoor equipment should be protected from physical harm and secured using equipment such as steel conduit pipes.
- vii. Access to outdoor / rooftop premises where the modules are installed should be restricted
- viii. Lightning arrestor should be installed for protection of outdoor equipment / modules such as backhaul / subscriber modules

5. 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.

6. Associated Documents

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

	Ncell	Classification: Internal
	Network Security Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO