


Backup Guidelines

Ncell

Guidelines

Approved Date:- 05/12/2016

	Ncell	Classification: Internal
	Backup 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-04

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
	Backup 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

Document Control

i. Document Identification

Document Title and Version:	GD-IT-IS-04 Backup Guidelines
Effective Date:	05-12-2016
Document Author:	Information Security Team
Owner:	ESPP Team
Approved By:	CEO

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)

iii. Document Roles and Responsibilities

Responsible	ESPP Team
Accountable	CIO/Head of IT
Consulted	Information Security Team
Informed	All Employees and External Parties

iv. Digital signature

CEO

CIO/Head Of IT

Ncell	Ncell	Classification: Internal
	Backup 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

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	15-08-2019	Information Security Team	Revised Formatted, Aligned to existing processes – Vishal Upadhyay	Mani	05-12-2019
2	01-09-2019	Tarani Prasad Chaudhary	Revised Formatting -	Andy Chong	13-12-2019
3	21-09-2019	Information Security Team	Reviewed with no change	Vishal Upadhyay	Mani 14-12-2021
4	13-12-2019	Tarani Prasad Chaudhary	Revised- Formatting	Andy Chong	15-12-2019
5	26-09-2023	Information Security Team	2.Review changed from annual to once every two years. 9.ii Restoration testing period changed to yearly for critical data and removed for rest. 9.iii Restoration period change to be as per the local regulations. 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	25-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

Ncell	Ncell	Classification: Internal
	Backup 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

Table of Contents

Document Control	2
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Definitions	5
5. Roles and Responsibilities	5
5.1 OS/Database Planning and Management Team	5
5.2 IT Service Desk/ Help Desk	5
5.3 System/Service Owners	6
5.4 Information Owners	6
6. Types of Data to be Backed Up	6
7. Backup Procedures	6
7.1 RTO/RPO	6
7.2 Backup Frequency	6
7.3 Labelling	7
8. Protection of Backup	7
9. Data Validation and Retention	7
10. Governance and Compliance	8
11. Associated Documents	8

Ncell	Ncell	Classification: Internal
	Backup 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

1. Purpose

This document provides guidelines for efficient handling of backup of electronic data, including backup and restore procedures for the Ncell Critical / Non-Critical systems as applicable. The goal is to ensure all relevant data will be backed up correctly, and recovery will be possible within the agreed Recovery Time Objective (RTO) / Recovery Point Objective (RPO).

2. Review and Updating

This procedure shall be reviewed annually 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. **Backup:** The saving of files onto offline/online mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- ii. **Archive:** The saving of old or unused files onto offline mass storage media for the purpose of releasing on-line storage room.
- iii. **Restore:** The process of bringing offline storage data back from the offline media and putting it on an online storage system such as file server.
- iv. **Hosts:** The server whose data will be backed up. Also contains the description of the data that will be backed up.
- v. **Backup Server:** The server that will perform the backup (writing to the tape).
- vi. **Retention Period:** This will define the period for which the backup will be retained.
- vii. **Backup Media:** The type of media that will be used to store the backup. It can be virtual library system, tape drives, file system or mirrored system.
- viii. **Backup Administrator:** This is the staff responsible for executing the backups and maintain the backup system configuration.

5. Roles and Responsibilities

A backup catalogue shall be maintained for all information backed up. For online backup solution, maintaining the backup catalogue shall be the responsibility of the backup solution owner.

In case of offline backup (e.g.: FTP scripts), the system owner shall be responsible to maintain the backup catalogue, either daily or weekly. The backup logs shall be checked every day to ensure that backup is successful. This shall be the responsibility of the backup solution owner. A backup of the backup catalogue shall be maintained by the respective owners.

5.1 OS/Database Planning and Management Team

- i. For data backed up by Ncell managed backup solution, OS/Database Planning and Management Team shall be responsible for maintaining the backups, ensuring that these backup work when needed, storing the backups according to the defined processes, labelling them properly and ensuring protection of the backups. They will be the ones who will be contact person in case data recovery and restoration is required.
- ii. OS/Database Planning and Management Team shall be responsible for maintaining the template for data backup request.
- iii. For all new solutions/systems, information shall be backed up on Ncell managed backup system.

5.2 IT Service Desk/ Help Desk

Backup of end user data shall be the responsibility of the IT service desk/help desk.

Ncell	Ncell	Classification: Internal
	Backup 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

5.3 System/Service Owners

There might be some solutions which has the backup system included. In such cases, for data backed up by respective stakeholders, OS/Database Planning and Management Team should be primary responsible team. Else, a memorandum of understanding shall be established between the solution owner and backup team wherein the solution owner shall ensure backups are maintained, tested regularly, stored according to the defined processes, labelled accordingly and protected.

5.4 Information Owners

- i. Data/information owners shall be responsible for defining the data that needs to be backed up. The data to be backed up shall be mutually agreed between information owner and backup administrator either in the "Backup Request Form" or in the form of an email with required details.
- ii. In case the system owner is responsible for the backup solution, the information owner shall request data backup with the system owners and agreements shall be between the two.

6. Types of Data to be Backed Up

Criticality of data will be agreed with the information owners and RTO/RPO will be set. Critical data is defined as customer service impacting or revenue impacting data. Following types of data need to be backed up:

- i. Data required for continued operations at Ncell.
- ii. Data contained in different databases.
- iii. System configuration data for different systems including, but not limited to servers, network
- iv. equipment.
- v. Official data contained in employee laptops/desktop
- vi. Data contained in email
- vii. Data contained in office drives, e.g.: N drive
- viii. System/Application/Database logs

7. Backup Procedures

For critical data, there shall be redundant backup solutions at a minimum of two different datacenters such that primary backup shall be stored at the datacenter where data is generated and secondary backup shall be stored at the other datacenter.

- i. Backup shall be performed using dedicated backup management software,
- ii. A log of backup shall be maintained which includes details of the data backed up, the date and time of the backup, the backup media used and its physical location,
- iii. Backup shall be related to control points in live processes (e.g. by using time-stamps),
- iv. The backup copies shall be reconciled to the live version when copies are taken (e.g. by checking of file size, hash totaling or other methods of verification),
- v. All backup shall be clearly and accurately labelled,
- vi. Backup shall be protected from accidental overwriting, and be subject to the same level of protection as live information, and
- vii. Backup shall be achieved where required for the period defined and agreed on by the information owner and the backup provider.

7.1 RTO/RPO

RTO is the duration by which the data should be recovered from backup. RPO is the data that should be recovered (e.g. the last full backup done). RTO / RPO will be different for each service and should be agreed separately with the information owners and documented. Backup should be performed based on the agreed RTO/RPO.

7.2 Backup Frequency

There will be different types of data backup based on the criticality of data:

Ncell	Ncell	Classification: Internal
	Backup 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

- i. Full back up is a complete backup of the data set. Although full backup of the data is the most secure, it takes a large amount of storage and time for full backup.
- ii. incremental backup includes data that has been changed since the last full or incremental backup, E.g. if a full back was done on a Saturday then Sunday's backup would have data that changed after Saturday's full backup and Monday's backup would have data that changed after Sunday's incremental backup.
- iii. For efficiency, unless otherwise stated, a full backup weekly with an incremental backup daily shall be performed for all data.
- iv. Full back up shall be done on off hours on the weekend with incremental backup done every day, during off hours.
- v. Full back up shall be done before any upgrades or major changes to the system.
- vi. Daily incremental and weekly full data backup will be maintained in virtual library system (storage) situated in the disaster recovery site. For critical data, one set full backup data shall be stored in disaster recovery site.

7.3 Labelling

- i. For offline backups (in case applicable), all backup should be properly labelled with the server name, data type (e.g. logs, configuration files and so on), date, retention period/date, type of backup (full, incremental) and backup level (if relevant) mentioned.
- ii. For online backups, the backup solution itself will maintain labelling.

8. Protection of Backup

To ensure that backup is available when needed, protection of the backup, both physical and technical, shall be in place.

- i. An inventory of all data that is backed up shall be maintained.
- ii. Technical access to the storage systems (e.g. SAN and tape drives) shall be controlled on the need to know basis.
- iii. Physical access control to the area where backup is stored shall be strictly maintained.
- iv. The backup media (e.g. Disk with virtual server snapshots, hypervisor-based backups, DVDs, magnetic tapes, computer disks) shall be stored in accordance with manufacturer specifications.
- v. The backup media shall be located in a locked, fireproof safe on-site, to enable important information to be restored quickly.
- vi. Copies of the backed-up information shall be kept in secure facilities off-site to enable systems or networks to be restored using alternative facilities in the event of a disaster.
- vii. Backups shall be encrypted to protect sensitive information when backups are:
 - a. Transferred to backup media, in order to prevent unauthorized interception
 - b. Stored on media, in order to prevent unauthorized access in the event backup media is stolen or is lost in transit to an alternative location, such as an off-site storage facility.
- viii. Backup servers, storage nodes, and backup devices shall not allow routing traffic between networks other than the network where the backup is taken and the network where the backup servers are placed.
- ix. Reading and writing of backup data, indexes, and similar related information should be logically separated between different hosts and different network security levels.

9. Data Validation and Retention

- i. Backup validation shall be done to ensure backup attempt was successful. This shall be done by checking logs of backup attempt.
- ii. Data restoration test shall be performed periodically to ensure integrity of the data backed up. The period shall be agreed between information owner and backup administrator. If any period is not agreed upon, then half yearly for critical data and once in a year for rest of the data shall be the default period.

Ncell	Ncell	Classification: Internal
	Backup 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

- iii. Unless otherwise agreed and documented, or mandated by local regulations, data shall be stored for a period of 1 year.

10. 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.

11. Associated Documents

- i. Information Security Policy
- ii. Business Continuity Policy