

Data Loss Prevention Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

Ncell	Ncell	Classification: Internal
	Data Loss Prevention 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-10

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
	Data Loss Prevention 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 Title and Version:	PR-IT-IS-10 Data Loss Prevention Procedure v1.0
Effective Date:	1 st October, 2019
Document Author:	Information Security Team
Owner:	CIO/Head of IT

ii. Distribution List

DLP Admin Team

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	DLP Admin Team

iv. Digital Signature

CEO

CIO/Head Of IT

v. Revision History

Ncell	Ncell	Classification: Internal
	Data Loss Prevention 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	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	03-09-2021	Information Security Team	Purpose: added Personal data (PII)	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	10-10-2023	Information Security Team	2. Review once every two years and 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	Ncell	Classification: Internal
	Data Loss Prevention 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. Objectives of Data Loss Prevention (DLP)	5
3.1 Data at Rest	5
3.2 Data in Transit	5
3.3 Data in Use	6
4. DLP Solution Capabilities	6
5. DLP Program	6
5.1 Assessment	6
5.2 Data Classification	6
5.3 Regulatory and Privacy Compliance	6
5.4 Monitoring and Incident Handling	6
5.5 Training and Awareness	6
5.6 DLP Policy management Process	6
5.7 Analysis and Reporting	7
5.8 Agent Compliance	7
5.9 Health Status	7
6. Backup, Recovery and Archiving	7
7. Governance and Compliance	7
8. Associated Documents	7

Ncell	Ncell	Classification: Internal
	Data Loss Prevention 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 standard employs a nontechnical, programmatic approach (data protection, information privacy) in unison with a technical approach (information security) to protect Ncell's sensitive corporate data and personal data (PII). It enables the organization to address and influence employee behaviors and choices as they apply to identifying, categorizing, classifying and protecting sensitive corporate data, e.g., data governance; risk assessment; regulatory and privacy compliance; data classification; policies; standards and procedures, and training and awareness. It also enables information security professionals to apply administrative, physical and technical controls to safeguard the same sensitive corporate data (data discovery, remediation processes).

2. Review and Updating

This procedure document shall be applicable to all employees of Ncell; as well as Third party vendors, contractors, partners, collaborators and any others doing business or research with Ncell will be subject to the provisions of this standard. Any other parties, who use, work on, or provide services involving NCell computers, technology systems, and/or data will also be subject to the provisions of this procedure document. The document shall be reviewed once every two years or when significant changes occur in the organization.

3. Objectives of Data Loss Prevention (DLP)

The NIST Cyber Security Framework identifies two states in which information is to be protected. They are as follows:

- i. Data-at-rest - Data that resides on local storage such as Database or server storage.
- ii. Data-in-transit - Data that needs to be protected when in transit such as HTTP/S, S/FTP/S, IM, P2P, SMTP.
- iii. That being said, there is also a third state used to classify 'state' of the information:
- iv. Data-in-use - Data that resides on end user workstation and needs to be protected from being leaked through removable media devices such as USB, laptop Hard disks etc.

3.1 Data at Rest

Ncell should ensure that the DLP Solution:

- i. Has the ability to identify and log where specific types of information is stored throughout the enterprise.
- ii. Must have the ability to seek out and identify specific file types—such as spreadsheets and word processing documents—whether they are on file servers, storage area networks (SANs) or even end-point systems.
- iii. Once found, the DLP solution must be able to open these files and scan their content to determine whether specific pieces of information are present, such as credit card or social security numbers.

3.2 Data in Transit

Ncell shall ensure that to inspect the information being sent across the network, the DLP solution must be able to:

- i. passively monitor the network traffic,
- ii. recognize the correct data streams to capture,
- iii. assemble the collected packets,
- iv. reconstruct the files carried in the data stream,
- v. perform the same analysis that is done on the data at rest to determine whether any portion of the file contents is restricted by its rule set.
- vi. read the contents within the packet's payload.
- vii. alert and optionally block the data flows in real or near real time when a rule is violated.
- viii. Additionally, the tool should also:
 - a. quarantine or encrypt the data in question based on the rule set.
 - b. decrypt the data prior to its inspection and re-encrypt the data once completed.

Ncell	Ncell	Classification: Internal
	Data Loss Prevention 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

3.3 Data in Use

Ncell shall ensure that the DLP solution is able to:

- monitor data movements while the data is being used at the endpoint. E.g. Printing, Removable Devices etc.
- enforce rules as defined in the endpoint policy to limit the movement of data.

4. DLP Solution Capabilities

Ncell shall ensure that the DLP solution is capable of the following:

- Policy Creation and management – the solution should have predefined policies addressing applicable local laws and regulations. E.g. of these can be EU GDPR, PCI DSS etc. It should also allow creation of custom policies to comply with locally applicable laws and regulations.
- Directory services integration - Integration with directory services should allow the DLP console to map a network address to a named end user.
- Backup and restore – the solution should allow Backup and restore features for preservation of policies and other configuration settings.
- Reporting - A reporting function may be internal or may leverage external reporting tools.

5. DLP Program

Ncell shall employ the following approach while developing a DLP program:

5.1 Assessment

Ncell should conduct assessment with the following objectives:

- The assessment should consider what data the organization wants to protect.
- The security risk based on the current and future security architecture.
- The total cost, and value-added benefits of introducing DLP.
- An objective cost-benefit analysis valuing the cost of data loss, total cost of implementation and management, and potential benefits provides the value proposition for a DLP solution.
- A DLP value proposition and go/no-go decision should be based on an objective risk-based assessment and analysis, considering current and future business direction.

5.2 Data Classification

Ncell must ensure that the data is classified as mentioned in organization's Information Classification Procedure

5.3 Regulatory and Privacy Compliance

Ncell shall ensure that DLP solution is complying with locally applicable regulatory and privacy policies and standards.

5.4 Monitoring and Incident Handling

Ncell shall ensure monitoring of DLP alerts and should log incidents in case of a suspicious data breach. Incident management process should be followed during and post raising the data leakage incidents. For detailed information, please refer organization's security incident management procedure.

Ncell shall ensure timely closure of incidents by following the escalation matrix defined in organization's information security incident management procedure.

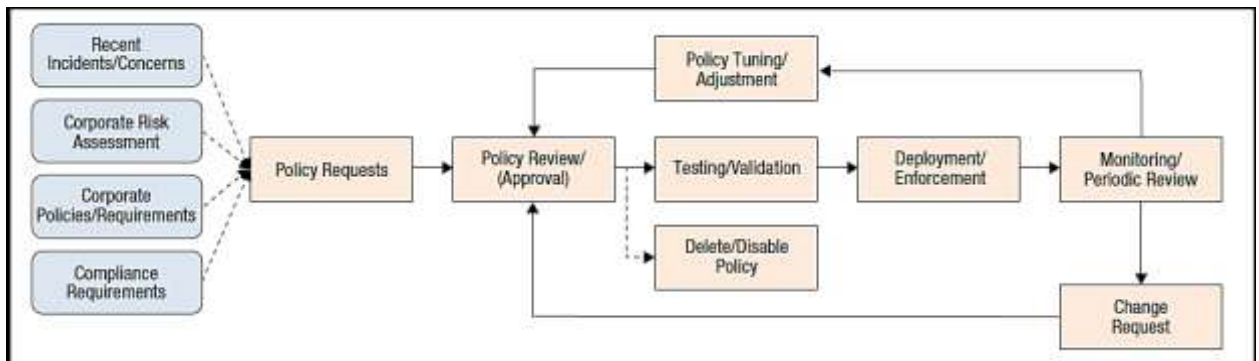
5.5 Training and Awareness

Ncell shall ensure that relevant stakeholders are trained and awareness programs are run for benefit of the users.

5.6 DLP Policy management Process

Ncell should follow the below mentioned workflow while creating DLP Policies

Ncell	Ncell	Classification: Internal
	Data Loss Prevention 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



5.7 Analysis and Reporting

Ncell shall identify metrics for meaningful analysis and report the same every week. The report should include

- Summary of Weekly Incidents and their Status
- Top Data Loss Incidents by Communication Channel.
- Top Data Loss Incidents by Severity.

5.8 Agent Compliance

Ncell shall maintain 95% compliance status of the agents installed on Ncell's endpoints.

5.9 Health Status

Health checks should be performed daily on the DLP tool. Checks should include the following

- Storage Percentage
- Memory Utilization
- CPU Utilization

6. Backup, Recovery and Archiving

DLP tool and Database should be backed up daily and should follow organization's backup guidelines.

7. Governance and Compliance

- Exception management process shall be followed to raise the exception for this procedure.
- Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

8. Associated Documents

- Information Security Policy
- Security Incident Management Procedure