

# Information Classification Procedure

Ncell

Procedure

Approved Date:- 15/10/2019

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Procedure Name DOCID: PR-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

	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## Document Control

### i. Document Identification

<b>Document Title and Version:</b>	<b>PR-IT-IS-03-Information Classification Procedure</b>
Effective Date:	15 <sup>th</sup> October, 2019
Document Author:	Information Security Team
Owner:	CIO/Head of IT

### ii. Distribution List

All Ncell Employees
External Auditor (If Required)


### iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Ncell Employees and External Auditor (If required)

### iv. Digital Signature


CEO

CIO/Head Of IT

	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
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	15-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	20-10-2019
1	03-09-2020	Information Security Team	Revised. No changes	Andy Chong	12-09-2020
2	14-09-2021	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	10-10-2023	Information security Team	2. Review changed to once every two years. Added Head of IT	Head of IT	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
	Information Classification Procedure	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## Table of Contents

<b>Document Control</b> .....	2
<b>1. Purpose</b> .....	5
<b>2. Review and Updating</b> .....	5
<b>3. Scope</b> .....	5
<b>4. Asset/Information Classification</b> .....	5
<b>4.1 Confidentiality Classes</b> .....	5
<b>4.2 Scope of Confidentiality Classification Scheme</b> .....	6
<b>5. Responsibilities</b> .....	6
<b>5.1 Information Classification</b> .....	6
<b>5.2 Maintaining Classification Levels</b> .....	6
<b>6. Asset Labelling</b> .....	7
<b>7. Asset Handling</b> .....	7
<b>7.1 Information Assets</b> .....	7
<b>7.2 Paper Assets</b> .....	8
<b>7.3 Hardware Assets</b> .....	9
<b>8. Associated Documents</b> .....	9

	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## 1. Purpose

The purpose of this procedure is to standardize information classification system across Ncell and to ensure that the security level of information handling during the whole lifecycle of information corresponds to Ncell business needs, customer demands and expectations as well as to legal requirements.

This procedure will replace the existing confidentiality policy "Confidential Classification Guidelines" followed by Ncell.

## 2. Review and Updating

This Standard Operation Procedure to be reviewed once every two years and whenever significant changes occur in the organization.

## 3. Scope

This applies to all information processed by Ncell systems, people (all employees, managers, third party contractors).


## 4. Asset/Information Classification

Prioritised protection of information from unauthorised disclosure, modification and destruction is very important. Therefore, it becomes important to classify the information as per the uniform scheme classification scheme, approved by management.

### 4.1 Confidentiality Classes

Information assets shall be classified under one of the following four categories based on the sensitivity and criticality to Ncell:

- i. **PUBLIC:** 'PUBLIC' information is the type of information which has been declared as public knowledge and can be freely given to anyone without any possible damage to Ncell. The same must be approved for public use by the information owner. For example: products which are launched in market, Media releases etc.  
This information that may be disclosed to any person regardless of their affiliation with Ncell. Impact should be evaluated before classifying any document/email as public without identification or authentication. If information marking is desired, the words "Public" may be written or designated in the information in question by the information owner/custodian.
- ii. **INTERNAL:** 'INTERNAL' information is the type of information which can be freely shared among Ncell employees but has not been approved for general circulation outside the organization. This information is less critical, and its disclosure is not expected to impact seriously or adversely to the business, shareholders, business partners, employees, and customers e.g general corporate information, employee information, SOP, etc. Internal documents such as Information Security policy, procedures, processes, standards, and guidelines may be shared with third parties during RFP/ RFQ stage without signing of NDA. For all other documents shall not be shared without an NDA signed with third parties.  
Marking is at the discretion of the owner or custodian of the information. If information marking is desired, the words "Internal" may be written or designated in the information in question by the information owner/custodian. Other labels like "Ncell Limited Proprietary" may be used at the discretion of the individual department.
- iii. **CONFIDENTIAL:** 'CONFIDENTIAL' information is the type of information which is considered critical to Ncell's ongoing operations, and which can be shared internally in Ncell on a need-to-know basis only. If unauthorized people gain access to company's 'CONFIDENTIAL' information, this may lead to significant financial damage or significant loss of good reputation for Ncell or have considerable negative effects for certain customers. For example: Customer, Subscriber and Financial data. For business purpose, the confidential documents may be shared with third parties only after signing of a Non-Disclosure Agreement.
- iv. **Restricted:** 'Restricted' information refers to highly sensitive internal documents which should be protected very closely and securely e.g., business plan, roll out plan, marketing plan and other

	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

information integral to the success of Ncell. If unauthorized user gain access to company's 'Restricted information this may lead to very serious financial damage or loss of good reputation for Ncell or several catastrophic adverse effects on Ncell operation, asset, or individuals. Password protection/or classification as Restricted for email and document attached is mandatory. For example: Business Plans, Business Strategies etc.

#### **4.2 Scope of Confidentiality Classification Scheme**

The classification scheme applies to all information in different formats e.g. to:

- i. Information in physical form (e.g. contracts, meeting minutes, business plans, product designs, employment contracts and other printed documents and information on paper).
- ii. Information in electronic form (e.g. files created by workplace tools; Word, Excel, and PowerPoint etc. documents)
- iii. Electronic communications (e.g. messages sent via e-mail, instant messaging and online collaboration).
- iv. Spoken information (e.g. information disclosed in a phone conversation or during other discussions)

### **5. Responsibilities**

#### **5.1 Information Classification**

- i. Information owner is responsible for classifying information.
- ii. information owner is usually the person who has;
  - a. Created the information, or .
  - b. received it first (from a third party outside Ncell), or .
  - c. has the right to decide on how the information is processed and used.
- iii. information ownership may also be appointed to a person regarding certain information category or type. The appointment will be decided by the person who created the information as well as the one who has the right to decide on how the information is processed/used, together with Security officer. information owner is also responsible for reviewing classifications periodically, if applicable for the information in question, and always when changes are made to the information.

#### **5.2 Maintaining Classification Levels**

All Ncell employees and third parties who work with confidential and classified Ncell information are responsible for following the guidelines below as per the classification level:

- i. to maintain privacy of the confidential information accessed by them and to prevent from unauthorized disclosure.
- ii. to respect requirements of orders, instructions and dispositions related to confidentiality of commercial/office secret.
- iii. to report to manager/director as appropriate when outsider tries to obtain confidential information.
- iv. to maintain commercial/office secret of the company's partners with whom the company collaborates whether Non-Disclosure Agreement is entered into.
- v. to bar from using confidential data for practicing an activity which may be competitor for the company and may prejudice it.
- vi. to protect notebooks, drafts, drawings, disks containing confidential information

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

## 6. Asset Labelling

In order to ensure that the correct controls are applied to the information assets of the organization, a system of protective marking will be used so that all employees and third parties are aware of how that information must be managed. Labelling of assets will only be applicable for Paper, Information and Hardware assets.

Asset Type	Restricted	Confidential	Internal	Public
<b>Information – Word document/ Power Point</b>	Will be marked automatically while selecting sensitivity.	Will be marked automatically while selecting sensitivity.	Will be marked automatically while selecting sensitivity.	Will be marked automatically while selecting sensitivity.
<b>Information – Excel document</b>	Will be marked automatically while selecting sensitivity.	Will be marked automatically while selecting sensitivity.	Will be marked automatically while selecting sensitivity.	Will be marked automatically while selecting sensitivity.
<b>Paper assets</b>	Marked as “Secret” or “Restricted” at the bottom of each page	Marked as “Confidential” at the bottom of each page	Marked as “Internal” at the bottom of each page	Marking not mandatory. All unlabeled documents shall be assumed to be Public.
<b>Hardware assets</b>	All hardware fixed assets shall be tagged by the Asset Management Unit within a month of their on-boarding. The tagging shall be performed location-wise, basis the asset numbers generated from asset inventory tool corresponding to the asset serial number. The tagging shall be reviewed as per Ncell policy			

## 7. Asset Handling

For each security classification level, a set of controls must be in place to ensure that Information, Paper and Hardware assets, are handled appropriately and protected at all times. The following sections sets out the main procedural components of these controls.

### 7.1 Information Assets

Asset Type	Secret/Restricted	Confidential	Internal	Unclassified
<b>Emailing</b>	Select Sensitivity while sending email.	Select Sensitivity while sending email.	Select Sensitivity while sending email.	Select Sensitivity as “Public” while sending email.
<b>Authorization and access privileges</b>	Information owner to authorize specific individual users; Authorization granted on a need-to-know basis to deliver services or carry out job functions.	Information owner to authorize a user/group; Authorization granted on a need-to-know basis to deliver services or carry out job functions.	No authorization required except for modification Widely available within Ncell to all users.	No authorization required Widely available within Ncell to all users.
<b>Authentication</b>	User IDs and Passwords should be used for authentication before providing access.	User IDs and Passwords should be used for authentication before providing access.	Authentication at domain level.	None.
<b>Availability</b>	To be stored on file server.	To be stored on file server.	To be stored on file server.	No special requirements.
<b>Storage on removable media</b>	Encrypted files on storage media.	Encryption is optional. Based on	No specific requirements.	No encryption required.



<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

		project requirements.		
<b>Transmission</b>	Encrypted communications.	Encrypted communications.	Internal information may be sent in the clear over unencrypted connections.	No special requirements.
<b>Reproduction/ Duplication</b>	Copy only when necessary and when access to original is highly impractical.	Copy only when necessary and when access to original is highly impractical.	No restrictions but copies to be destroyed immediately after use.	No special requirements.
<b>Disposal</b>	Disposal should be done as per "Media Handling Procedure"	Disposal should be done as per "Media Handling Procedure"	Disposal should be done as per "Media Handling Procedure"	Disposal should be done as per "Media Handling Procedure"

## 7.2 Paper Assets

Asset Type	Secret	Confidential	Internal	Unclassified
<b>Authorization and access privileges</b>	Information owner to authorize specific individual users.	Information owner to authorize a user/group.	No authorization required except for modification Widely available within Ncell to all users.	No authorization required Widely available within Ncell to all users.
<b>Availability</b>	Scan and store electronic copy on file server.	Scan and store electronic copy on file server.	Scan and store electronic copy on file server.	No special requirements.
<b>Storage</b>	Locked when not in use in areas under surveillance and restricted to authorized individual persons;	Locked when not in use and restricted to authorized individual persons.	Master copy should be secured against destruction.	No encryption required.
<b>Transport / Transmission</b>	Mail, courier, or transport in properly labelled secure packaging using reputable companies that employ secure conditions.	Physical transmission allowed as per permission of owner; Transmission through reliable courier agencies; Classification marking on external envelope; and Receiver should provide the confirmation of receipt of information to information owner.	Physical transmission allowed as per permission of owner; and Transmission through reliable courier agencies.	No special requirements.
<b>Disposal</b>	Shred the data.	Shred the data.	Shred or tear all documents and files, or place in secure receptacle for future shredding.	No special requirements.

<b>Ncell</b>	<b>Ncell</b>	Classification: Internal
	<b>Information Classification Procedure</b>	Owner: CIO/Head of IT
		Effective Date: 15-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

### 7.3 Hardware Assets

Asset Type	Secret	Confidential	Internal	Unclassified
<b>Authorization and access privileges</b>	To authorize specific individual users.	Asset owner to authorize a user/group.	No authorization required except for modification Widely available within Ncell to all users.	No authorization required Widely available within Ncell to all users.
<b>Availability</b>	Redundancy required.	Redundancy required.	No special requirements.	No special requirements.
<b>Storage</b>	Stored under access control mechanism and continuous surveillance.	Stored under access control mechanism and continuous surveillance.	Stored under lock and key.	No special requirements.
<b>Transport / Transmission</b>	Transport in properly labelled, secure and manufacturer specified packaging using reputable companies that employ secure conditions	Transport allowed as per permission of owner; Transmission through reliable transport agencies; Classification marking on external packaging; and Receiver should provide the confirmation of receipt of asset to asset owner.	Transport allowed as per permission of owner; and Transmission through reliable transport agencies.	No special requirements.
<b>Disposal</b>	Disposal should be done as per Media Handling Procedure depending upon type of hardware asset.	Disposal should be done as per Media Handling Procedure depending upon type of hardware asset.	Disposal should be done as per Media Handling Procedure depending upon type of hardware asset.	Disposal should be done as per Media Handling Procedure depending upon type of hardware asset.

### 8. Associated Documents

- i. Asset Management Procedure
- ii. Media Handling Procedure
- iii. Information Security Policy