Asset Management Procedure

Ncell

Procedure

Approved Date:- 01/10/2019

Procedure Name DOCID: PR-IT-IS-02

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS-02 Asset Management Procedure v1.0**
Effective Date:	1st October, 2019
Document Author:	Information Security Team
Owner:	Information Security Team

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	01-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	15-10-2019
1	01-10-2019	Information Security Team	Ready for approval	Andy Chong	29-10-2019
2	08-21-2021	Information Security Team	6.1.5 Asset Disposal added 8.4.ii Label change: "Ncell Limited Proprietary" To "Ncell Proprietary"	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	28-09-2023	Information Security Team	Review period once every two years 6.1.1 Go live Process added, New clause 7.vii, 8.2 CIA rating changed to 1 – 15, 8.2.3 removed, 8.3 MCJ, CJ added Added Head of IT	Head of IT	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Review-Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	30-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

Table of Contents

1. Purpose

The purpose of this standard operating procedure is to describe a formal procedure to be followed for maintaining, handling and protecting all the assets of Ncell Pvt. Ltd. This SOP has been prepared to provide a step by step course of action for the following:

- Identifying and classifying the organisation assets.
- Compiling and maintaining the asset register in an appropriate format as specified in Annexure B1.
- Identifying the asset owners and custodians.
- Determining the confidentiality (C), integrity (I), and availability (A) ratings of assets.
- Understanding the responsibilities of Asset Owner, Custodian and User; and
- Appropriately classifying and reclassifying the information, be it in soft copy or hard copy.

2. Review and Updating

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

3. Scope

This scope of this SOP is all information assets covered as part of defined scope for Information Security Management System at Ncell Pvt. Ltd.

4. Definitions

i. **Information Asset**- Information asset is any piece of information that has got value to the organization. Information assets consist of information and the systems / facilities that are used to process the information.

ii. **Information security** - Preservation of confidentiality, integrity, and availability of information Asset; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

iii. **Threat** - This term defines an event (e.g., a tornado, theft, or computer virus infection), the occurrence of which could have an undesirable impact on the well-being of an asset.

iv. **Vulnerability** - This term characterizes the absence or weakness of a risk reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. For example, not having a fire suppression system could allow an otherwise minor, easily quenched fire to become a catastrophic fire.

v. **Risk** - The likelihood of a threat agent exploiting a given vulnerability thereby causing negative impact to an asset. A risk is the loss potential, or probability, that a threat will exploit a given vulnerability. For example, risk is loss of critical business data due to virus outbreak in the database server in absence of anti-virus software.

5. Responsibilities

Following are the responsibilities of the roles defined as part of asset management procedure:

5.1 Information Security Working Group Member

Where a unit/ department creates processes or uses an asset to support their business processes, an individual who facilities the preparation of asset register with respect to its unit/ department is an Information security working group member. Information Security working group member shall ensure the following:

i. Facilitates preparation of asset register with necessary details of assets and their criticality

ii. Facilitate review of asset register as per the defined frequency for its review.

5.2 Asset owner, custodian and user

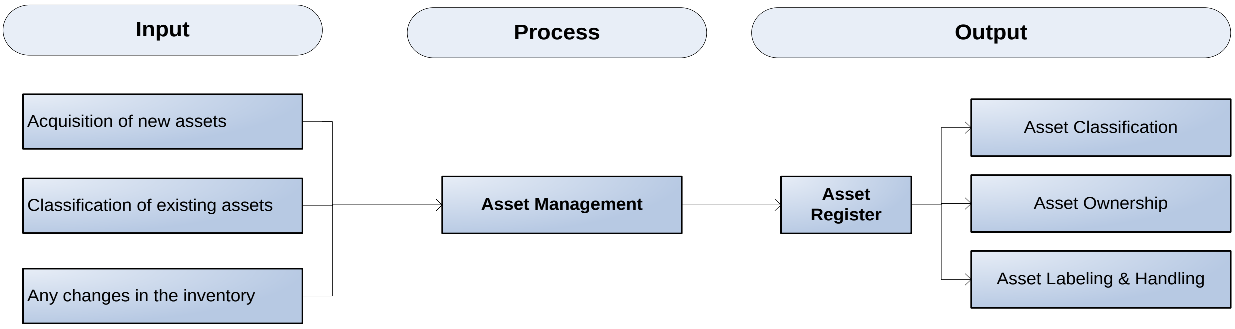
Refer Information Security Governance Procedure for responsibilities of asset owner, custodian and user.

5.3 CIO/Head of IT/CTO

Will be accountable for implementation of this procedure.

6. Asset Management Overview

Ncell shall adhere to the following guidelines, to ensure that each asset in their respective unit has a defined and identified owner, custodian and user.



Input
Process
Output
Acquisition of new assets
Classification of existing assets
Any changes in the inventory
Asset Management
Asset Register
Asset Classification
Asset Ownership
Asset Labeling & Handling

Figure 1: Asset Management Process Overview

6.1 Inputs required for asset management.

6.1.1 Acquisition of New Assets

Any new information asset acquired by Ncell will act as an Input to the process for labelling and classification of assets, updating in asset inventory, and assignment of an owner, custodian, and user to the asset. Project Go live Procedure[1] needs to be followed for any new asset before processing Ncell data.

6.1.2 Labeling and Classification of existing Assets

In order to ensure that the correct controls are applied to the information assets of the organisation, a system of protective labelling will be used so that all employees and third parties (where applicable) are aware of how that information must be managed. This labelling of assets will follow the guidelines defined in Ncell Information Classification Guidelines.

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 classification scheme, approved by management.

6.1.3 Owner, Custodian and User for the Assets

Identify key people/roles that require the use of, or are responsible for the ownership, maintenance, safeguarding of assets.

6.1.4 Asset Inventory Update

Any additions or updates to the current asset register should be appropriately captured.

6.1.5 Asset Disposal

The need for disposal may be triggered by the following scenarios –

- When asset is on longer required to be help for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held.
- When the asset is redundant and hence no longer in use
- When the asset has exceeded its warranty/ retention period; and/or

[1] Project GoLive Procedure

- When the asset has malfunctioned and cannot be repaired

6.2 Outputs Generated from Asset Management

6.2.1 Asset Register

As an output of the process, Ncell will have an updated Information Asset Register (IAR) which is an inventory of information assets owned by Ncell. For each identified asset, Individuals or entities will be identified who will be responsible for classification and ownership of assets. Additionally, the custodians for daily maintenance/ implementing controls/update of assets will also be identified. To ensure safeguarding of information from unauthorized disclosure, modification and destruction, Asset registers will also classify assets as per the classification defined and approved by management for each asset.

The asset register shall be reviewed and updated annually or whenever significant changes occur to the asset.

7. Guiding Principles

i. It is mandatory to have an asset owner for each asset. Asset owner shall be an Ncell employee or a Unit Head.
ii. Asset owner can optionally appoint an asset custodian. If an asset custodian is not appointed, owner shall carry out responsibilities of the asset custodian. Asset custodian shall also be an Ncell employee or a unit.
iii. All OSS tools (including client-based tools) shall be owned by the OSS team.
iv. All generic client-based Software (e.g., MS office) shall be owned by the ESPP team, as applicable.
v. Services/systems with availability rating 5.0 need to have site level redundancy. For such services/. systems, asset custodians must comply to the other business continuity requirements; and
vi. Assets with classification rating as 'Secret' should have a criticality rating of 'Catastrophic'.
vii. Minimum Baseline Security Standard (MBSS) assessment for assets which processes Ncell data will be done annually on a sampling basis. Sample shall be taken from Minimum Crown Jewel / Crown Jewel.

8. Asset Management Process

S.N.	Activity	Responsibility	Documents Required	Processing Time
1	Provide asset management procedure to all unit/ department heads and Information Security working group members nominated from each unit/ department	Information Security Team	Asset Management Procedure	NA
2	Provide asset register template to all unit/ department heads	Information Security Team	Asset Register Template	NA
3	Identify all the assets used by each unit	Unit Head	NA	NA
4	Identify the 'Asset Owner' for each identified asset	Unit Head	NA	NA
5	Collect the asset information from each asset owner and consolidate in unit asset register	Unit Head	NA	NA
6	Identify the 'Asset Custodian' and 'Asset User'	Asset Owner	NA	NA
7	Use the Asset Register template given in Annexure A and fill-up the template with necessary information about asset, i.e., Asset Type, Asset Location	Asset Owner	NA	NA

8	Assign CIA Rating to each asset as per the Annexure A	Asset Owner	NA	NA
10	Classify all assets as per *Section 8.4*	Asset Owner	NA	NA

8.1 Asset Type

An asset register of Ncell's assets shall be maintained as per Asset Register Template provided in Annexure. Respective unit heads are responsible to maintain the same in their unit.

Asset owner shall be responsible for complete protection of assets ensuring they are secure against all kinds of physical, environmental and/ or logical threats. Assets are classified into seven types: Information, paper, people, physical, services and software, as detailed below:

i. **Information Asset:** This would include Data files (including important data in local desktops/laptops), Customer Data, Subscriber Data, System documentation, User documentation, Training materials, Operational / Support procedures, Continuity plans, Archived information, etc.
ii. **Physical Asset:** This would include Computer equipment (processors, monitors, laptops, modems, printers etc.), Communication equipment (Network devices, Hardware elements of MSC, BSC, OCS, IT systems, VAS Systems etc.) etc.
iii. **Paper:** Information in physical hard copy form, which is used / required / generated during operations and is used to manage business processes. E.g., Bill of material, Contracts, Agreements, Invoices, Manuals.
iv. **Software Asset:** This would include Application software, System software, Development tools & Utilities. Software licenses, Software elements of MSC, BSC, OCS, IT systems, VAS Systems etc.
v. **Services:** Services/Infrastructure which is necessary to ensure smooth operation of Ncell. This would include general utility services such as Power, Lighting, Air Conditioning, any third-party outsourced service from service providers, internal services from support departments like HR, Administration and other departments etc.
vi. **Site:** This would include the building of operation for the organization
vii. **People:** This would include personnel required to support and run business processes

8.2 Asset Criticality Rating

Based on the sensitivity of the asset, each asset must be rated on Confidentiality, Integrity and Availability parameters on a scale of 1-15, i.e., 1 being minimum impact and 15 being maximum.

8.2.1 Confidentiality Rating

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Confidentiality is used in the context of how sensitive the information to untimely disclosure is or to unauthorized individuals.

i. Ensuring confidentiality to data/information gives an assurance that information is shared only among authorized persons of Ncell. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data, etc.
ii. Based on the sensitivity of the asset, confidentiality characteristic of an asset must be rated on a scale of 1-5, i.e., 1 being minimum impact and 5 being maximum impact.

8.2.2 Integrity Rating

Integrity refers to the completeness and accuracy of information assets. Integrity is lost if unauthorized changes are made to the data or IT/ Network system by either intentional or accidental acts. If integrity of data is not restored back, continued use of contaminated data would result in inaccuracy, fraud or erroneous decisions.

i. If the integrity of asset is compromised, the impact on the organization needs to be understood/ estimated by asset owner.

ii. Based on the sensitivity of the asset, integrity characteristic of an asset has to be rated on a scale of 1-5, i.e., 1 being minimum impact and 5 being maximum impact.

8.2.3 Availability Rating

Availability indicates how soon the information asset is required, in case the same is lost. If the asset is not available, the impact on the organization needs to be understood/ estimated by asset owner.

i. Based on the sensitivity of the asset, availability attribute of an asset has to be rated on a scale of 1-5, 1 being minimum impact and 5 being maximum impact. The availability characteristic will depend on the downtime that can be afforded for the asset.

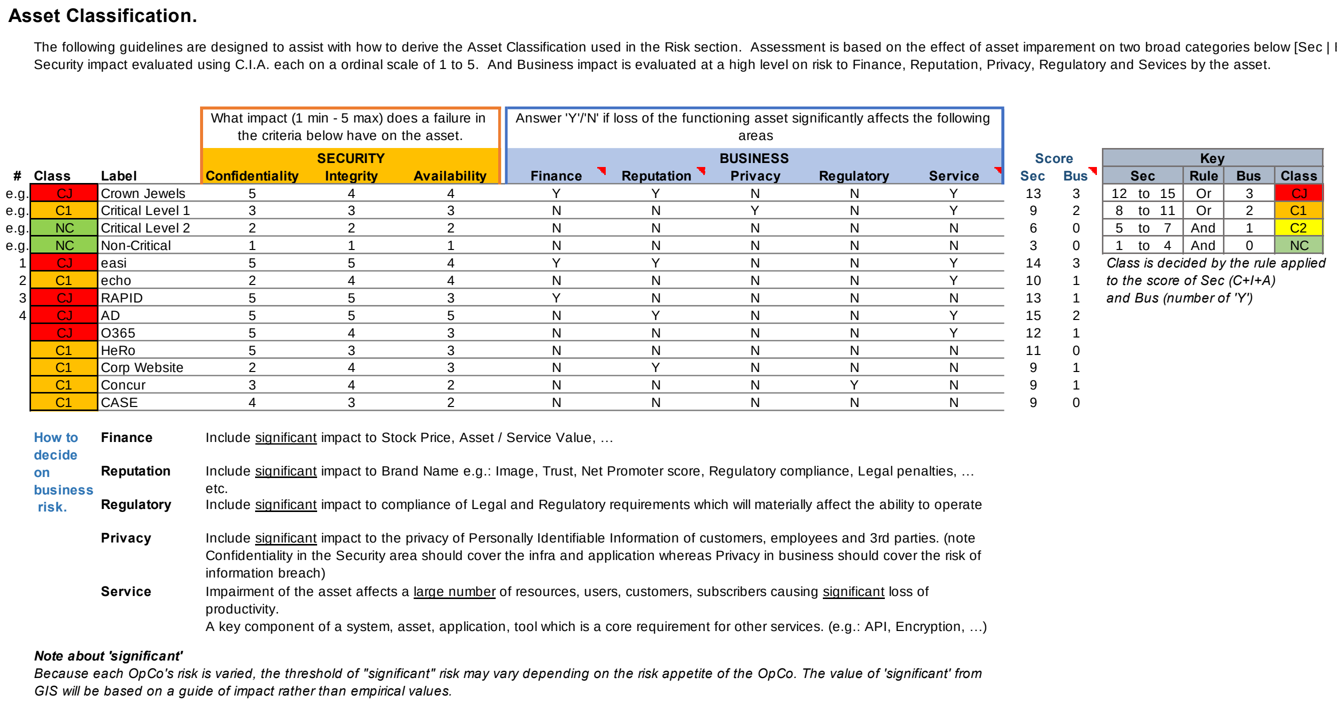
Below guidelines can be followed for determining confidentiality, Integrity and availability rating of asset:

Impact	1-Insignificant	2-Minor	3-Moderate	4-Major	5-Catastrophic
Disruption to Service:					
Localised**	• < 1 hour	• 1 hour – 3 hours	• 3 hours – 10 hours	• 10 hours – 48 hours	• > 48 hours
Regional**	• 0 – 15 min	• 15 min – 1 hour	• 1 hour – 3 hours	• 3 hours – 10 hours	• > 10 hours
Nationwide**	• Nil	• 0 – 15 min	• 15 min – 1 hour	• 1 hour – 3 hours	• > 3 hours
Injuries	• Nil	• Minor injury	• Minor injury	• Extensive bodily injuries / permanent disability	• Extensive bodily injuries / permanent disability requiring hospitalisation
		• Minor treatment (first aid)	• Requires outpatient treatment	• Hospitalisation required	• Death
Financial*	• < 1% variance against targets / budget financial indicators	• 1% < 5% variance against targets / budget financial indicators **or** • (222k to <22m) BDT	• 5% < 10% variance against targets/budget financial indicators **or** • (>=22m to <111m) BDT	• 10% < 15% variance against targets /budget financial indicators **or** • (>=111 m to <222 m) BDT	• >= 15% variance against targets / budget financial indicators **or** • (>=222 m) BDT

Reputation	• Customer complaints generally restricted to hotline / emails	• Customer complaints generally restricted to hotline / emails	• Customer complaints include negative posts online (e.g., blogs, twitter, etc.)	• Widespread negative publicity online (e.g., blogs, twitter, YouTube etc.) • Corporate image significantly affected	• Widespread negative publicity online (e.g., blogs, twitter, YouTube etc.)
	• Estimated time to restore reputation: 1 week	• Estimated time to restore reputation: 3 months	• Estimated time to restore reputation: 1 year	• Estimated time to restore reputation: 1 year < 3 years	• Long-standing reputation damage • Criminal prosecutions • Political intervention
Media Attention	• None	• Media enquires only	• One-off newspaper article / radio / television / online mention	• Sustained media attention for > 3 days	• Sustained media attention for > 5 days
Legal and Regulatory	• Litigation or non-compliance issues that has no litigation consequences. • Issuance of advice letter	• Minor non compliances or breaches of contract, Act, regulations, consent conditions • Issuance of reprimand/ warning letter	• Breach of regulatory or contractual obligations is widespread. • Litigation and increased scrutiny from regulators. • Multiple issuances of reprimand/ warning letters	• Major breach of contract, act, regulations, or consent conditions • Expected to attract regulatory attention. • Investigation, prosecution and / or possibility of action taken against specific member(s) of the senior management team.	• Serious breach of contract or legislation • Potential for litigation including class actions. • Future approvals / registration / licensing in jeopardy • Possibility of criminal action involving a felony against senior enterprise management or Ncell

8.3 Critical Assets

Criticality of assets will be defined as per the criteria in the picture below:



Asset Classification.

The following guidelines are designed to assist with how to derive the Asset Classification used in the Risk section. Assessment is based on the effect of asset imparement on two broad categories below [Sec | I
Security impact evaluated using C.I.A. each on a ordinal scale of 1 to 5. And Business impact is evaluated at a high level on risk to Finance, Reputation, Privacy, Regulatory and Sevices by the asset.

			What impact (1 min - 5 max) does a failure in the criteria below have on the asset.			Answer 'Y'/'N' if loss of the functioning asset significantly affects the following areas						
			SECURITY			BUSINESS					Score	
#	Class	Label	Confidentiality	Integrity	Availability	Finance	Reputation	Privacy	Regulatory	Service	Sec	Bus
e.g.	CJ	Crown Jewels	5	4	4	Y	Y	N	N	Y	13	3
e.g.	C1	Critical Level 1	3	3	3	N	N	Y	N	Y	9	2
e.g.	NC	Critical Level 2	2	2	2	N	N	N	N	N	6	0
e.g.	NC	Non-Critical	1	1	1	N	N	N	N	N	3	0
1	CJ	easi	5	5	4	Y	Y	N	N	Y	14	3
2	C1	echo	2	4	4	N	N	N	N	Y	10	1
3	CJ	RAPID	5	5	3	Y	N	N	N	N	13	1
4	CJ	AD	5	5	5	N	Y	N	N	Y	15	2
	CJ	O365	5	4	3	N	N	N	N	Y	12	1
	C1	HeRo	5	3	3	N	N	N	N	N	11	0
	C1	Corp Website	2	4	3	N	Y	N	N	N	9	1
	C1	Concur	3	4	2	N	N	N	Y	N	9	1
	C1	CASE	4	3	2	N	N	N	N	N	9	0

Key					
Sec			Rule	Bus	Class
12	to	15	Or	3	CJ
8	to	11	Or	2	C1
5	to	7	And	1	C2
1	to	4	And	0	NC

Class is decided by the rule applied to the score of Sec (C+I+A) and Bus (number of 'Y')

How to decide on business risk.		
	Finance	Include significant impact to Stock Price, Asset / Service Value, …
	Reputation	Include significant impact to Brand Name e.g.: Image, Trust, Net Promoter score, Regulatory compliance, Legal penalties, … etc.
	Regulatory	Include significant impact to compliance of Legal and Regulatory requirements which will materially affect the ability to operate
	Privacy	Include significant impact to the privacy of Personally Identifiable Information of customers, employees and 3rd parties. (note Confidentiality in the Security area should cover the infra and application whereas Privacy in business should cover the risk of information breach)
	Service	Impairment of the asset affects a large number of resources, users, customers, subscribers causing significant loss of productivity. A key component of a system, asset, application, tool which is a core requirement for other services. (e.g.: API, Encryption, …)

Note about 'significant'
Because each OpCo's risk is varied, the threshold of "significant" risk may vary depending on the risk appetite of the OpCo. The value of 'significant' from GIS will be based on a guide of impact rather than empirical values.

8.4 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.

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 has to be approved for public use by the information owner. For example: products which are launched in market, Media releases etc.
 Marking is at the discretion of the owner or custodian of the information. 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 the business seriously or adversely, 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 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.

Marking for assets which are identified as ‘Confidential’ shall be mandatory. The word "Confidential" may be written or designated in a conspicuous place on or in the information in question by the information owner/custodian.

iv. **SECRET:** ‘SECRET’ 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 information integral to the success of Ncell. If unauthorized user gain access to company’s ‘SECRET’ information this may lead to very serious financial damage or loss of good reputation for Ncell or may have very serious negative effects for certain. For example: Business Plans, Business Strategies etc. Marking for assets which are identified as ‘Secret’ shall be mandatory. The word "Secret" may be written or designated in a conspicuous place on or in the information in question by the information owner/custodian.

9. IT Asset Lifecycle

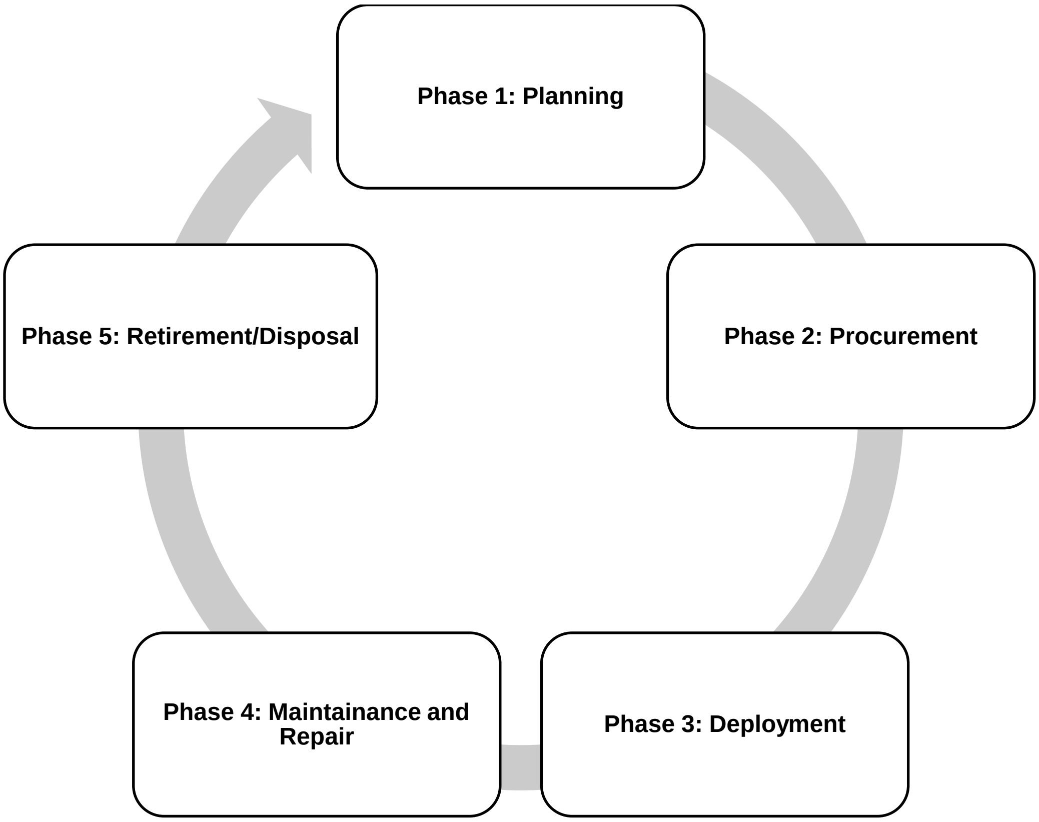

Phase 1: Planning
Phase 2: Procurement
Phase 3: Deployment
Phase 4: Maintainance and Repair
Phase 5: Retirement/Disposal

Figure 2: IT Asset Lifecycle

9.1 IT Asset Lifecycle Phases

i. **Planning:** During this phase, requirement gathering is performed and an estimation of the IT assets required is assessed.

ii. **Procurement**: Post finalization of required IT assets, the assets are procured and purchased as per the requirements and plan.

iii. **Deployment**: After procurement of IT assets, the assets are tested and deployed in the required environment.

iv. **Maintenance & Repair:** Periodic maintenance and required repair activities are carried out to ensure optimum life of the IT asset.

v. **Retirement/Disposal:**

a. After end of asset lifecycle, the asset is written off by the procurement team in the SAP database.
b. The asset is then sanitized by the ESPP team for removal of any information that it may contain with the Information Security Officer’s sign off.
c. Post sign-off, the IT asset is sent to the Warehouse team for further processing/disposal.
d. For end of life of laptops, the laptop is formatted and sanitized by the ESPP team and handed over to the user after approval and sign-off from the Procurement Team.
e. For more information on disposal methods, please refer Ncell’s Media Handling Procedure.

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. IT Asset Management Procedure
iii. Media Handling Procedure
iv. System Development Lifecycle Procedure
v. Project Go-Live Procedure