INFORMATION SYSTEM ASSETS MANAGEMENT-CDAC

Information Security is being considered one of the paramount items by Governments due to recent rise of targeted attacks, focusing large number of critical infrastructures of many nations. Govt. of India has also started initiatives to ensure proper cyber security in its departments and organizations. In line with this, MeitY has already issued mandates to its affiliated organizations to implement an Information Security Management System (ISMS) based on ISO 27001. As an initial step, each organization shall develop a Cyber Crisis Management Plan (CCMP) and submit to CERT-IN. The purpose of this CCMP is to make each organization secure, vigilant and resilient. The CCMP for our organization is being developed and it shall outline the processes used by CDAC to respond to a critical cyber incident that would adversely affect the activities or reputation.

IT and digital assets constitute the major value of any organization. To be secure, these assets shall be prioritised with a view of what matters the most. Information security basically deals with Confidentiality, Integrity, Availability, Accountability and Assurance. Inventorying all sources of information and its prioritisation based on impact on security is one of the primary and critical tasks. These assets can be tangible or intangible and can exist in the form of information store, databases, hardware, software or network. The purpose of this exercise is to collect the list of critical assets of each group/department of CDAC centres from the perspective of business continuity of corresponding unit. The guidelines covering the identification of assets and its classification is provided in the following sections.

The activities to be completed as part of asset collection shall include

- Identify and document all assets along with its impact on business continuity. The details of asset shall include asset type, location, purchase cost and AMC/Warranty details
- Assignment of security label to each identified assets

GUIDELINES FOR ASSET IDENTIFICATION AND CLASSIFICATION:-

ASSET CLASSIFICATION BASED ON TYPE

- **Information Assets**: All information resources utilized in the course of organization's business. Example of information assets include database files, data files, operational and support procedures and archived information.
- **Software assets**: Assets including application software for implementing the business functions of CDAC and system software programs like OS, DBMS, development tools and software packages.
- **Physical assets**: Assets which are visible and tangible, such as computer equipment, network equipment, storage media, mobile devices etc.
- **Services**: Assets include the services run by CDAC, communication services used by CDAC etc.

ASSET OWNERSHIP

- **Asset Owner**: Functional head at GH/ SH(level) shall be identified as the owner of assets at respective division.
- **Asset Custodian**: Individual or entity who have been identified for management responsibility of the respective assets.
- **Asset User**: Individuals or entity who are using the asset in a routine way for business related tasks and are responsible for operational activities.

INFORMATION ASSET SECURITY CLASSIFICATION

Information assets can be classified based on the following guideline.

- **Confidential**: The loss or theft of this data can cause serious risk to the organization. This category of data is usually subject to regulation or controlled by contractual agreement.
- **Sensitive**: A level of relative value less than confidential but still important to protect. Losing the data will raise the risk to the organization, even if it is just reputational

damage. Strategy documents or interorganizational correspondence can be considered sensitive.

- **Private:** Usually compartmental data that might not do the organisation damage but must be kept private for other reasons.
- **Proprietary**: Data that is disclosed outside the Organisation on a limited basis or contains information that could reduce the Organisation's competitive advantage, such as the technical specifications of a new product.
- **Public**: This data, if lost, would have little or no impact on risk levels.

ASSET CLASSIFICATION BASED ON CRITICALITY

IT assets should be classified based on the criticality of assets with appropriate owners identified and designated. Criticality of assets could be determined by the impact on business continuity of CDAC on loss or non-availability of the assets identified. Categories of assets based on criticality are defined below.

- **Critical**: Asset loss or non-availability may cause disruption to the business functions of one or more CDAC centres.
- **High**: Asset loss or non-availability may cause disruption to one more groups or departments but not any centre as a whole.
- **Medium**: Loss or non-availability may cause disruption to one or more projects but not a group or department as a whole.
- **Low**: Loss or non-availability may cause disruption to one or more employees but not a project or team as a whole

Template for Asset List

The template to fill the asset list is provided as annexure I.

ANNEXURE – I

Asset List												
CDAC Centre:												
Group/Department												
Sl. No	Asset Name	Identifier	Owner	Custodian	User	Asset Type	Type Description	Purchase Cost	Location	Impact on Business Continuity	Security Classification	AMC/Warranty End Date
						Information				High	Confidential	
						Information				High	Confidential	
						Information				No Impact	Confidential	

(Separate excel template is provided to fill the asset details)

Signature of Project lead:

Name:

Date:

Signature of Group Head :

Name:

Date: