Controller General of Defence Accounts
Ulan Batar Road Palam Delhi Cantt–11 0010
IFA WING

CIRCULAR NO. 07 of 2011

No. IFA/9 **Dated: 02 .06.11**

To

All PIFAs/IFAs

Subject: Implementation of Cyber Security Policies for Govt of India

1. It has been intimated by EDP Sec of HQrs office vide circular No MECH/EDP/810/Cyber Security dated 02.05.2011 that National Informatics Centre has prepared the Cyber Security Policy providing instructions on secure and acceptable cyber resources in all the Ministry/Departments. A soft copy of Standard Operation Procedure for cyber Security policies is available on CGDA WAN (ftp://10.48.152.109) in folder Cyber Security.

2. The Standard Operating Procedures may be provided to all the Sub offices under your Administrative Control. Sub offices may be asked to train their staff about the self explanatory instructions/procedures of Standard Operating Procedure.

4. Asset Management Procedure detailed in Standard Procedure may be followed for keeping Hardware and Software asset register.

5. A feedback with reference to the implementation of the policy in your organization may be furnished to Jt CGDA (IT) EDP Centre of HQrs office,

6. Please acknowledge receipt.

Sd/-
(T Kabilan)
Sr.ACGDA(IFA)

Copy to

EDP Centre	For information please

T. Kabilan 2/6.
(T Kabilan)
Sr.ACGDA(IFA)

Controller General of Defence Accounts
Ulan Batar Road Palam Delhi Cantt–11 0010
IFA WING

CIRCULAR NO. 07 of 2011

No. IFA/9 **Dated: 02 .06.11**

To

All PIFAs/IFAs

Subject: Implementation of Cyber Security Policies for Govt of India

1. It has been intimated by EDP Sec of HQrs office vide circular No MECH/EDP/810/Cyber Security dated 02.05.2011 that National Informatics Centre has prepared the Cyber Security Policy providing instructions on secure and acceptable cyber resources in all the Ministry/Departments. A soft copy of Standard Operation Procedure for cyber Security policies is available on CGDA WAN (ftp://10.48.152.109) in folder Cyber Security.

2. The Standard Operating Procedures may be provided to all the Sub offices under your Administrative Control. Sub offices may be asked to train their staff about the self explanatory instructions/procedures of Standard Operating Procedure.

4. Asset Management Procedure detailed in Standard Procedure may be followed for keeping Hardware and Software asset register.

5. A feedback with reference to the implementation of the policy in your organization may be furnished to Jt CGDA (IT) EDP Centre of HQrs office,

6. Please acknowledge receipt.

(T Kabilan)
Sr.ACGDA(IFA)

Copy to

EDP Centre	For information please

(T Kabilan)
Sr.ACGDA(IFA)

Name of the Document		Asset Management Procedure	
Classification	Restricted	Audience	Client System Administrator, Network Administrator and Network Security Administrator
Version	2.0	Date of last change	10th Sept, 2010

ASSET MANAGEMENT PROCEDURE

1. Introduction

An asset is a hardware or software which is of value / importance to a Ministry / Department. Therefore it is essential to maintain a proper record of each asset.

Assets, if not maintained properly, might be stolen or misused.

This document provides necessary steps for maintaining the record of cyber resources.

2. Asset Register

Asset Register should be maintained which includes the following information about an asset:

2.1. **Asset ID:** A unique asset identification number assigned to each asset for easy and quick identification. *(refer: Asset Management Guidelines)*

2.2. **Asset Name**[1]: Name given for identification of Asset based on its functionality.

2.3. **Asset Details**: Details about the asset such as IP Address, MAC Address, Hostname, Software license number, etc.

2.3.1. **IP address:** Logical address allocated to the client systems, network devices and network security devices by the System Administrator or Network Administrator.

2.3.2. **MAC address:** MAC address (Media Access Control address) is a unique identifier assigned to network adapters or network interface cards by the manufacturer for identification.

2.3.3. **Hostname:** A hostname is a unique name by which a system / network devices / network security devices connected on the network can be identified.

2.3.4. **Serial No. / License:** In case of hardware provide serial number and for software provide license key.

2.4. **Asset Type**: There are two types of assets as follows:

2.4.1. **Hardware:** Physical devices which are required / used to support operations. For example – client systems, routers, firewalls, printers, etc.

[1] Asset Name: 'Payroll Server' could be a name of the asset which is used for processing the salary of employees. In case there are more than one asset providing the same functionality, asset name should be suffixed by a number like Payroll Server 1, Payroll Server 2 and so on.

2.4.2. **Software:** Software which is used to support / facilitate operations of Ministry / Department. For example – Operating Software, Application Software, Development tools and Utilities.

2.5. **Physical Location**: Physical location and details where the asset is located.

2.6. **Owner**: User who is assigned the asset for the operations of Ministry / Department.

Asset information should be captured using *Asset Register Template* (Attached in the Annexure).

3. Procedure

Asset Management procedure is a bottom-up approach, which collects asset information for every Ministry / Department in each location. The role of each person is defined below:

3.1. **For Network devices / Network Security devices**

3.1.1. **Network Administrator / Network Security Administrator**

3.1.1.1. Collect and maintain asset information using *Asset Register Template*.

3.1.1.2. Forward the asset information to Information Security Officer and National Security Operation Centre.

3.1.2. **National Security Operations Centre**

3.1.2.1. Maintain the consolidated Asset information from all locations.

3.2. **For Client Systems, Software, Peripheral devices and other Accessories**

3.2.1. **System Administrator**

3.2.1.1. Collect and maintain asset information using *Asset Register Template*.

3.2.1.2. Forward the asset information to the respective Information Security Officer, Network Administrator and Network Security Administrator.

3.2.2. **Information Security Officer**

3.2.2.1. Review and maintain the Asset information received from System Administrator, Network Administrator and Network Security Administrator

3.2.2.2. Forward the consolidated Asset Information to the Chief Information Security Officer of respective Ministry / Department at a frequency defined in the *Asset Management Guidelines*.

3.2.3. **Chief Information Security Officer**

3.2.3.1. Maintain the consolidated Asset information from all locations.

4. Annexure

Annexure	Template Name
Asset Register Template	Asset Register.xls

5. References

5.1. Security Policy for System Administrator

5.2. Security Policy for Department

5.3. Security Policy for Network connected to Internet

5.4. Asset Management Guidelines

Asset Register

Document Information

Document Title	Asset Register
Date	
Classification	Restricted
Document Type	

Document History

Date	Version	Author	Comments/Changes

S.No	Asset ID	Asset Name	Asset Details				Asset Type	Asset Location	Department / Ministry	Asset Owner	Remarks
			IP Address	MAC Address	Host Name	Serial No. / License					
1	1234	Laptop					Hardware	North Block	ABC	User	