CONTROLLER GENERAL OF DEFENCE ACCOUNTS
IT & S, ULAN BATAR ROAD, PALAM, DELHI CANTT-10
Phone: 011-25665761-63 Fax:-011-25675030
E-mail : cgdanewdelhi@nic.in Website : www.cgda.nic.in

No. MECH/EDP/810/Cyber Security Dated:30.03.2016

To,

All the PCsDA/PIFAs/PCA(Fys)/CsDA/IFAs

Subject: Cyber/Network/Hardware Security measures.

This is regarding compliance of Cyber/Network/Hardware security instructions which lays down the security aspects to be adopted by the website administrators and other users. Below mentioned instructions are in continuation of letters dated 12/12/2011, 31/01/2012, 23/04/2015 and 18/05/2015.

2. Though detailed instructions regarding website, network and hardware security have already been issued, the importance of cyber security is once again reiterated. The following basic guide lines regarding Cyber/Network/Hardware security are reproduced once again for strict compliance.

I. Website Security measures

(i) The Website should be audited by CERT-In empanelled Auditors.

(ii) Security Audit of the website should be performed at an interval of Two Years.

(iii) Website will be hosted with NIC only.

(iv) The PC through which website is updated

 (a) should be detached from LAN.

 (b) should be kept in Server Room / Separate Room.

 (c) should have anti-virus installed.

 (d) should not store any Official Document/confidential data and once the data is uploaded on the website, it should be deleted.

 (e) USB port should be disabled.

 (f) password should be changed in a short interval.

 (g) Network cable should be unplugged after updating the website.

(h) Such PC should be used only for this purpose and any other internet activity must be restricted.

(v) The System should be kept in a separate room / Server Room and this room should have:

(a) Restricted Entry and entry Log Book be maintained.

(b) Must have Bio-metric base access to such PC.

(c) Monitoring facility through CCTV coverage. (Both Inside and Out Side)

(vi) SAOs / AOs / AAOs will be nominated for updating the website.

(vii) For Interactive websites login password should follow password policy with captcha / OTP / Bio-metric authentication.

(viii) Web server log analysis should be done at least once in month.

II. Network Security measures

(i) Internet and LAN/WAN connections should not be available on the same machine.

(ii) Each machine on LAN/WAN Network should be duly protected against any physical access by unauthorized person. A strong password may be used.

(iii) Each machine on LAN/WAN Network should be duly protected against virus/ malicious content by installing good quality antivirus. The antivirus must be updated & the machine should be scanned periodically.

(iv) Console Antivirus should be used on LAN connected PCs.

(v) Any pen drive/ USB data storage device should not be used on any machine on the WAN Network.

(vi) Office work/document/data etc should not be done/made available at internet connected PCs.

(vii) Internet/Public network should be accessed through a user account not as an administrator of the PC.

(viii) Telnet should be disabled on the internet connected PCs.

(ix) Ports that are not assigned to specific devices should be disabled, or set to a default guest network that cannot access the internal network. This prevents outside devices being able to jack in to your internal network from empty offices or unused cubicles. Unused open nodes of the LAN/WAN network must be disabled & closed.

(x) Password of any LAN/WAN application should not be saved at the login page.

(xi) To manage the network, it is better to create an IP based network for both LAN &WAN and allot fix IP for each user and Network design/architecture must be documented.

(xii) Any incident/ doubt of cyber attack on your network (both LAN & WAN) must be intimated to this HQrs & CERT-In immediately.

III. Hardware Security measures

(i) AMC of H/W peripherals should be done properly and periodically.

(ii) All the Server/PCs should be on UPS with 24x7 power backup facility.

(iii) Proper earthing should be available for all the H/W peripherals.

(iv) Antivirus should be installed on PCs/Servers and updated time to time.

(v) H/W peripherals should be secured from Physical damage/ Natural disaster.

(vi) Fire safety measures should be followed properly.

(vii) Blade Servers should be mounted in racks.

(viii) Servers should be put on first/upper floor & proper temperature should be maintained.

(ix) Access Control system should be managed for Server room.

(x) Annual Stock Taking should be done as per Stock Taking guidelines.

(xi) Preventive maintenance should be done on regular interval.

3. It is also requested to provide the information attached at Annexure- 'A' to Hqrs office in respect of the offices under your jurisdiction by 15.04.2016 through mail at cgdanewdelhi@nic.in or CGDA Mail Server at hqedp@cgdamail.org.

Jt.CGDA(IT) has approved.

(A K Wani)
Sr. ACGDA (IT)

Annexure – 'A'

(Annexure to the letter No. MECH/EDP/810/Cyber Security dated 30.03.2016)

Name of Office: ________________________

(i) **Website Security measures**

Sl No	Particulars	Yes	No	Remarks
1.	Whether Security Audit of the Website Performed by CERT-In Auditors? (If Yes please attach certificate else provide reasons?)			
2.	Whether Security Audit performed at an interval of Two Years?			
3.	Is your website interactive?			
5.	Whether the website is hosted on NIC? (if No Provide details)			
6.	Whether VPN connected PC is attached in LAN?			
7.	Is VPN connected PC protected with password?			
8.	Whether password of VPN connected PC is changed periodically (Every 15 days)?			
9	Is any official data is available on VPN connected System?			
10.	Is Anti-virus installed on VPN connected System?			
11.	Is VPN Connected PC placed in Server Room/ Separate Room?			
12.	Whether no. of Persons is restricted for updating the website? (No. of persons)			
13.	Whether Log book is maintained for Updating the Website?			
14.	Is CCTV Camera installed outside / Inside of the Server Room / Separate Room?			

15	Is any Bio-metric device installed to open/access the Server Room?			
16.	Whether Pen Drive/any USB drive is used to carry the data for uploading the website?			
17.	Whether CD / DVD is used to carry the data for uploading the website?			
18.	Whether data or any confidential doc is deleted from such PC after uploading on the website?			
19.	Whether Log files of the web server is analyzed? (if Yes Who perform the log analysis)			

(ii) **Network Security measures:**

S. No.	Particular	Yes	No	Remarks
1.	Whether Internet & WAN connection is available on the same machine?			
2.	Whether internet has been made available on any machine on the LAN?			
3.	Whether each machine on LAN/WAN network is password protected?			
4.	Whether Antivirus is installed on each machine on the network and updated time to time?			
5.	Whether console Antivirus is installed on LAN/WAN network connected PCs.			
6.	Whether Firewall/ any other H/w or S/w is used for the network security?			
7.	Whether Internet is used on the PCs containing official data/work/documents etc?			
8.	Whether USB data storage device i.e. pen drive etc is used on any machine on the network?			
9.	Whether Unused open nodes are closed/disabled in the LAN/WAN network?			

10.	Whether maintaining a network hardware list that includes device name and type, location, serial number, service tag, and responsible person name?			
11.	Whether IP based network is available for both LAN &WAN and allotted fix IP for each user?			
12.	Whether telnet & USB are disabled?			
13.	Whether any incident/ doubt occurred regarding network security?			

(iii) **Hardware Security measures**

S. No.	Particular	Yes	No	Remarks
1.	Whether AMC of H/W peripherals exist?			
2.	Whether all the Servers/PCs are on UPS with 24x7 power backup?			
3.	Whether proper earthing is available for all the H/W peripherals?			
4.	Whether Antivirus is installed on PCs/Servers and updated time to time?			
5.	Whether the H/W peripherals are secured from Physical damage/ Natural disaster?			
6.	Whether fire safety measures are taken/followed?			
7.	Whether Blade Servers are mounted in racks?			
8.	Whether Servers & Router are on first/upper floor?			
9.	Whether Back up of data on Servers/PCs is taken on daily basis as required?			
10.	Whether Access Control system is managed for Server room?			
11.	Whether Annual Stock Taking is being done as per Stock Taking guidelines?			

ACDA/DCDA (IT&S)