

# **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](mailto:cgdanewdelhi@nic.in) Website : [www.cgda.nic.in](http://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

