



सत्यमेव जयते

भारत सरकार Government of India
रक्षा मंत्रालय Ministry of Defence
रक्षा लेखा महानियंत्रक
Controller General of Defence Accounts
उलान बटार रोड़, पालम, दिल्ली छावनी-110010
Ulan Batar Road, Palam, Delhi Cantt – 110010
Phone : 011-25665761-63, Fax : 011-25675030
E-Mail : cgdanewdelhi@nic.in



No. Mech/EDP/148/Website/Vol-IV

Dated: 18/05/2015

To,

All PCsDA/CsDA/PIFA/
IFA/PCA(Fys)/CFA(Fys)

Subject: Cyber Security Measures.

Reference :- Hqr office letter no. Mech/EDP/148/Website/Gen. dated: 23/04/2015

The counter measures for strengthening the cyber security of the website and IT environment in offices have been issued time to time by the various security and Government Agencies like NIC and CERT-In. This office has also issued certain security measures vide letter quoted under reference. For further strengthening the IT environment, following recommendations may also be implemented, wherever applicable.

- i. Website should be hosted in NIC environment.
- ii. Data base server, Mail server and Web server should be on separate machines.
- iii. In case the website is interactive, multifactor authentication for login facility should be adopted like security questions and '*captcha*'.
- iv. Client machine used for updating/uploading the website should be isolated from the LAN (Local Area Network).
- v. Any Internet Activity other than VPN access should be strictly prohibited on Client machine.
- vi. The machine should be duly protected against any physical access by unauthorised person. Biometric access may be one of the options.

(2)

- vii. The machine should be duly protected against cyber attack by installing a good quality antivirus, adopting excellent password policies etc. Antivirus must be updated & machine scanned periodically. Virtual/onscreen keyboard for keying in the password on client machine may be preferred.
- viii. In case the server is in LAN, the client machine should not be exposed to the Internet at all.
- ix. Logs of web servers should be taken and analysed for any cyber attack/misuse.
- x. Any incident or any doubt of cyber attack must be forwarded to CERT-In, Army cyber security group including this HQrs office.

Jt CGDA (IT) has approved this.



(Vinay Khanna)
Sr. ACGDA (IT)