CONTROLLER GENERAL OF DEFENCE ACCOUNTS – EDP
ULAN BATAR ROAD, PALAM, DELHI CANTT – 110010
Phone : 011-25665761-63 Fax : 011-25675030
Website : http://cgda.nic.in
Email : cgdanewdelhi@nic.in

No Mech/EDP/810/Cyber Security Dated : 12 /10/2015

To
All PCsDA / CsDA /PCA (fys)

Subject : Cyber Security Measures.

This is regarding compliance of web 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.

Though detailed instructions regarding website security have already been issued, the importance of cyber security is once again reiterated. In view of the recent incidents following basis guide lines regarding cyber security are reproduced once again for strict compliance.

(i) Remove the database server containing sensitive information from public access. Data base server, Mail server and web server should be on separate machines.

(ii) No data should be in possession of third party like vender etc. take it's possession immediately.

(iii) Host the web site in NIC environment after securely designed web site and its audit by empanelled agency.

(iv) It is also requested to scrutinize the data available on the website and data base. Accordingly decision can be taken along with consultation of respective services and security agencies regarding uploading of sensitive / confidential data on website at database bench and necessary action taken thereafter.

(v) Use an account with restricted permissions in the database : Grant execute permissions only to selected stored procedures in the database to the used when database update/modification is to be done through web application.

(vi) Use an application firewall : Use application firewall to control input, output and / or access to the web application . eg. Mod-security for Apache Server.

(vii) In case the website is, interactive, multifactor authentication for login facility should be adopted like security questions and 'captcha'.

(viii) Client machine used for updating / uploading the website should be isolated from the LAN (Local Area Network).

(ix) Only dedicated machine is used for VPN access with IP binding and Mech binding got done by NIC. Any Internet Activity other than VPN access strictly prohibited on the client machine. A watch must be kept by higher authorities and zero tolerance policy to be adopted in this case.

(x) The client machine should be duly protected against any physical access by unauthorized person. Biometric access may be one of the options.

(xi) The machine should be duly protected against cyber attack by installing a good quality antivirus, adopting excellent password policies etc. Antivirus must be updated and machine scanned periodically. A mechanism to monitor weekly antivirus updated and scanning of the machine should be developed.

(xii) Virtual /onscreen keyboard for keying the password on client machine may be preferred. User accounts shall limited privileges. A user is responsible for activities carried out by the account assigned to him i.e. subject to monitoring for maintenance activities.

(xiii) In case the server is in LAN, its client machine should not be exposed to the Internet all.

(xiv) Unauthorized PLF file sharing software shall not be installed.

(xv) The WAN and internet must not be accessed from the same machine. A watch must be kept by higher authorities and zero tolerance policy to be adopted in this case.

(xvi) If multiple internets have bee provided in the same campus, stop it and distrubted network through single gateway protected by a good firewall should be enabled.

(xvii) Any incident or any doubt of cyber attack must be forwarded to CERT-In, and stop uploading.

(xviii) Copy if latest Security Audit report of all Websites within your jurisdiction may be forwarded to this office urgently.

Keeping in view the security aspects and data confidentially, it is requested to look into the matter personally. A compliance in this regard may please be conveyed within 15 days. CGDA is personally monitoring the website security issues.

Jt. CGDA(IT) has seen.

(VINAY KHANNA)
Sr ACGDA(IT)