



Govt. of India
Ministry of Finance
O/o Principal Chief Controller of Accounts
Central Board of Indirect Taxes & Customs
Coordination, Expenditure Section

1st Floor, AGCR Building, I.P. Estate, New Delhi-110002

E-Mail: expdr-coord@gov.in, PH: 011-23702282

F. No. Pr.CCA/CBIC/Coord.-Expdr./Circular- Instruction/Vol.I/2021-22/67 DTD.: 04/07/2022

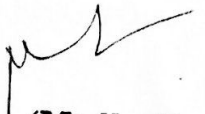
CIRCULAR

Subject :- Cyber Security Guidelines for Government Employees in Civil Accounts Organization- Reg.

Please find enclosed herewith O.M. No. I-67001/1/2021-Admin-CGA/106 dated 30.06.2022 issued by M/o Finance, DoE, O/o CGA, PFMS DIVISION, GIFMIS, New Delhi on the subject cited above.

All Zonal Heads of CBIC are therefore requested to bring the contents of the O.M. to the notice of all PAOs under their administrative control for information and strict Compliance.

This issues with the approval of Competent Authority.


(Madhu Rawat)
Sr. Accounts Officer

Encl: As Above

To:

- 1 DCA, CBIC North Zone, Jaipur
- 2 CA, CBIC East Zone, Kolkata
- 3 DCA, CBIC West Zone, Mumbai
- 4 DCA, CBIC South Zone, Chennai
5. IT Section (for uploading on website)

Copy for information to:-

- 1 Sr. PS to Pr. CCA (CBIC)
- 2 PS to CCA (CBIC)
- 3 PS to DCA(HQ), CBIC

93717/26
05/07/22

File No: 1-67001/1/2021-Admin-CGA/106
Government of India
Ministry of Finance, Department of Expenditure
Office of Controller General of Accounts
PFMS Division
GIFMIS

Mahalekha Niyantarak Bhawan
E-Block, GPO Complex,
INA, New Delhi – 110023.

Dated: 24/06/2022

OFFICE MEMORANDUM

Subject: Cyber Security Guidelines for Government Employees in Civil Accounts Organization.

This is with reference to the latest cyber security guidelines issued by NIC. In order to sensitize the government employees, contractual/outourced resources and build awareness, the following guidelines are required to be strictly adhered by the users in Civil Accounts Organization to ensure that systems remain more secure from probable cyber-attacks:

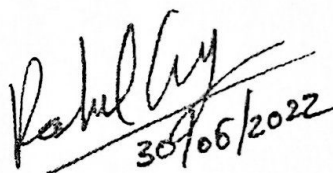
1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters. Don't use the same password in multiple services/websites/apps.
2. Change your passwords at least once in 45 days. Don't save your passwords in the browser or in any unprotected documents.
3. Don't write down any password, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: Sticky/post-it notes, plain paper pinned or posted on your table, etc.)
4. Use multi-factor authentication, wherever available.
5. Save your data and files on the secondary drive (ex: d:\) instead of system drive (Ex: c\ or root).
6. Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: Google drive, Dropbox, etc.).
7. Maintain an offline backup of your critical data.
8. Keep your Operating System and BIOS firmware updated with the latest updates/patches. Don't use obsolete or unsupported Operating Systems.
9. Install enterprise antivirus client offered by the government on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.
10. Configure NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) in your system's DNS Settings.
11. Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in your system's NTP Settings for time synchronization

12. Don't use any 3rd party DNS Service or NTP Service.
13. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).
14. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
15. Use authorized and licensed software only. Don't install or use any pirated software (ex: cracks, keygen, etc.).
16. Don't open any links or attachments contained in the emails sent by any unknown sender.
17. Ensure that proper security hardening is done on the systems.
18. When you leave your desk temporarily, always lock/log-off from your computer session.
19. When you leave office, ensure that your computer and printers are properly shutdown.
20. Keep your printer's software updated with the latest updates/patches.
21. Setup unique passcodes for shared printers.
22. Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.
23. Don't allow internet access to the printer.
24. Don't allow printer to store its print history.
25. Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centres.
26. Keep the GPS, Bluetooth, NFC and other sensors disabled on your computers and mobile phones. They may be enabled only when required.
27. Download Apps from official app stores of google (for android) and apple (for iOS).
28. Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user base, etc.
29. Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
30. While sending any important information or document over electronic medium, kindly encrypt the data before transmission. You can use a licensed encryption software or an Open PGP based encryption or add the files to a compressed zip and protect the zip with a password. The password for opening the protected files should be shared with the recipient through an alternative communication medium like SMS, Sandes, etc.
31. Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.
32. Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
33. Don't disclose any sensitive details on social media or 3rd party messaging apps.

34. Don't plug in any unauthorized external devices, including USB drives shared by any unknown person.
35. Don't use any unauthorized remote administration tools (ex: Teamviewer, Ammy admin, anydesk, etc.).
36. Don't use any unauthorized 3rd party video conferencing or collaboration tools for conducting sensitive internal meetings and discussions.
37. Don't use any external email services for official communication.
38. Don't jailbreak or root your mobile phone.
39. Don't use administrator account or any other account with administrative privilege for your regular work.
40. Don't use any external mobile App based scanner services (ex: Camscanner) for scanning internal government documents.
41. Don't use any external websites or cloud-based services for converting/compressing a government document (ex: word to pdf or file size compression).
42. Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.

All Principal CCAs/CCAs/CAs with independent charge are requested to bring the above guidelines to the attention of the users of Civil Accounts Organization in the Ministry/Department under their control.

This issues with the approval of competent authority.


30/06/2022
(Rahul Garg)
ACGA (GIFMIS)

To

All Pr. CCAs/CCAs/CAs with independent charge.

Copy to: - Sr. AO (GIFMIS) for uploading on website.