Government of India
Department of Atomic Energy
Computer and Information Security Advisory Group (CISAG)

Date: 14/05/2020

GUIDELINES FOR WORK FROM HOME

1. Computer and Internet security

1.1. Preferably use a dedicated computer or laptop with licensed operating system for office work. Ensure that the OS of the computer/ laptop is up to date with latest patches, by enabling auto update feature.

1.2. Use antivirus with latest updates for protecting your computer from malwares. If you notice slowness of computer then run full computer scan. Make it a habit of running full computer scan at least once in a day.

1.3. Ensure that auto-update feature of the anti-virus software is enabled so as to update virus signatures automatically from the service providers, as and when an update of signature or virus engine is available.

1.4. Create a dedicated login for office work and do not share its password with anyone.

1.5. Install and use software obtained/downloaded only from trusted sources.

1.6. Use only licensed software for doing office work.

1.7. Use complex password on home Wi-Fi network and broadband router and share the password(s) with only trusted people.

1.8. Ensure that network firewall is enabled on the broadband router.

1.9. Do not register official email address with Internet hosted services/applications.

1.10. Refrain from opening attachments from un-trusted sources when you are not expecting them.

1.11. Ensure that you have logged out from all applications like webmail and any other service provided by department after the work is over.

1.12. Close all office work related windows, applications, files and documents when not in use.

1.13. Be suspicious of emails appear to be coming from very senior officers or other unexpected sources. Open them only after you are sure about the origin of email by checking ‘from address’ rather than only the sender's name. Doubly cross check for mails received with from address of Director/Chairman. Open them only after you are sure about origin of such emails.

1.14. Do not send/provide official email account and password information to anyone and ensure that the password of the official email account is not the same as that of any other account of you on Internet.

1.15. Turn off the computer when not in use.

1.16. Get the PC maintenance done only by trusted vendor/firm.

1.17. Wi-fi/ any other network on the computer/ laptop, may be enabled only when it is required.

1.18. Do not provide access of your computer/ laptop remotely through commercial services such as teamviewer / anydesk etc.

2. Document Security

2.1. Exchange documents always through official means such as external webmail facility provided by department.
2.2. It is advised to keep official documents only in external storage such as Pen Drive, USB Hard Disk (do not keep any official document on home PC) and connect this device to PC only during official work.
2.3. Protect documents with password while exchanging them via email
2.4. Do not share passwords of documents with others not party to the document.
2.5. Always store the password protected documents in the same form on desktop/ laptop/removable drive .
2.6. Do not share documents with secret and top-secret classification via email.
2.7. Keep the official documents in the PC to minimum by deleting old/unnecessary documents.
2.8. While deleting documents, ensure that they are flushed out even from Trash folder.
2.9. Do not sync/backup official documents in any Internet based cloud storage or email systems. Note that these days Microsoft enables cloud drive named “onedrive” by default on all PCs. Hence do not use Microsoft email accounts for login to your computer.
2.10. Do not share documents with external parties without the explicit instructions from superiors.
2.11. Always use encrypted channels such as “https” while sharing documents with others on Internet.
2.12. Avoid use of smartphone like devices for any official document storage/transactions.
2.13. If possible external storage containing official documents may be encrypted using bitlocker.
2.14. Whatsapp like messengers/ other file sharing platforms may be avoided for sharing official documents.
2.15. Webex, Zoom like web conferencing software may be avoided for official meetings. Conference calls directly from phone may be used for this purpose.
2.16. Do not use any online antivirus scanner for document scanning.
2.17. Do not use any online tools for format conversion or for any reason.

3. General Notes

Be aware that COVID-19 pandemic is being used by cyber criminals with an aim to scam people out of their money, data and to gain access to their systems. While working from home you should:

- Exercise critical thinking and vigilance when you receive phone calls, messages and emails.
- Exercise caution in opening messages, attachments, or clicking on links from unknown senders.
- Be wary of any requests for personal details, passwords or bank details, particularly if the message conveys a sense of urgency.
- If in any doubt of the communicator's identity, delay any immediate action. Re-establish communication later using contact methods that you have sourced yourself.