F.No.N-24011/1/2022-CC
Government of India
Ministry of Finance
Department of Revenue

.....

New Delhi, dated 30, March, 2022

OFFICE MEMORANDUM

Subject: Guidelines/Best Practices to be followed while using office IT infrastructure such as computers, Wi-Fi, email, smart devices, USB devices, Internet browsing etc.

.....

In order to increase user understanding and sensitivity to threats and vulnerabilities and to spread awareness regarding the need to protect organization's and personal information, the following Guidelines/Best Practices are issued. All officers/staff of Department of Revenue are requested to follow these guidelines while using office IT infrastructure to minimize the threat of cyber attacks:

1. Internet connected computers should not be used for sensitive official documentation work.
2. Presence of programs not related to office work like Skype, Xbox Games, Telegram, Team Viewer etc., and presence of unnecessary apps like 'Whatsapp', 'Drop Box-41', 'Google Drive' etc., on many computers poses a serious security risk to all computers connected in the network. This should be avoided.
3. Usage of USB devices (pen drives & mobile phones) should be restricted as these are the major carriers of malware propagation,
4. Backup of data should be taken at regular intervals, to prevent loss of data.
5. Users should not install software not required for day to day office work.
6. Internet connected computers should be accessed with limited user account privileges.
7. All computers should be secured with three layer strong/complex (BIOS, Windows and Screensaver) passwords.
8. Common applications like MS Office, Acrobat Reader, flash players, etc. should be updated regularly so that these computers are not vulnerable to malware threats.
9. Usage of common USB devices for different networks may be avoided so as to ensure physical separation of different LANs & Internet Networks.
10. Latest/updated version of Antivirus should be installed in all the computers. It is preferable to use the centralized Antivirus system.
11. Always use genuine software and Operating Systems with latest security patches.
12. Remote access features should be restricted.
13. Auto-Play feature should remain disabled in all the computers.
14. Any unidentified security threat must be brought to the notice of system administrator by the user, rather than fixing problems by self means.
15. NIC mails:
    - Do not open emails or attachments from unknown email IDs.
    - Check for any shared folder under ***Preferences*** option in NIC mail. If any shared folder is found, disable it immediately.
    - Check ***Login History*** for account access details.
    - Don't save login credentials in browser and logout, once the session is over.
    - Enable ***Kavach*** on all NIC Email accounts.

2/-

Cyber Security: Best Practices

1. General Computer Usage:

- Use Account with limited privileges on systems and avoid accessing with administrator privileges for day-to-day usage.
- Backup of important files at regular intervals.
- Do not leave system unattended. Use systems screen locking functionality to protect against physical access, such as a screen saver that won't deactivate without a password, or just log out of everything so anyone that wants access has to log in again.
- Remove unnecessary programs or services from computer: Uninstall any software and services you do not need.
- Restrict remote access. If file sharing is not required in your day-to-day work, disable file and print sharing.
- Remove data securely: Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system.
- Scan all the files after you download whether from websites or links received from e-mails.
- Do not download unfamiliar software from the Internet.
- Supervise maintenance or rectification of faults in the system by service engineers.
- Use Defender Credential/Device Gurd on Windows 10 and Windows Server 2016 to enforce constrained language mode and application white-listing by leveraging advanced hardware features where supported.
- Prohibit any remote logon to the system (RDP, SMB, RPC) for local administrators and also prohibit a standard local administrator with an ID=500 which is vulnerable to pass-the-hash attack.
- Minimize and completely deny granting administrator privileges for users of local PCs, especially for users who work with external information systems.

2. General Internet Browsing:

- Be conscious of what you are clicking on/downloading. Download software from trusted source only.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Do not store official information/documents on Internet Cloud (iCloud, Google Drive, Dropbox etc.) or Internet connected computers.
- Make a habit of clearing history from the browser after each logout sessions.
- Delete Windows "Temp" and "Temporary Internet files" regularly.
- Avoid using services that require location information. Avoid posting of photos with GPS coordinates.
- Remember search engines track your search history and build profiles on you to serve you personalized results based on your search history.
- Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it.
- Be wary of free downloadable software – There are many sites that offer customized toolbars or other features that appeal to users, which are likely to have backdoors. Remember that things on the internet are rarely free. "Free" Screensavers, games, software etc. may generally contain Malware.

- Frequently check unusual folder locations for document (.doc, docx .xls, xlsx and .def) file extensions (in search options, select advanced search options, make sure you checked "Search System folder", "Search hidden files and folders" and "search subfolders").
- Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password.
- Be extremely careful with file sharing software. File sharing opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk serious legal consequences.

3. Malware Defense:

- Always set automatic updates for Operating System, Anti-Virus and Applications. (My Computer -> properties -> automatic updates -> select Automatic and time).
- Enable hidden file & system file view to find any unusual or hidden files. (My Computer -> tools -> folder options -> view -> select enabled with "Show hidden files and folders" option and disable 'Hide protected operating system files").
- Turn off auto play (Start -> Run -> type gpedit.msc ->Computer Configurations -> Administrative Templates -> Windows Components -> Select "AutoPlay Policies" -> Double Click at "Turn off Auto Play" -> Select Enabled -> Set "Turn off Auto Play on:" to " All drives" and Click OK).
- Configure the following parameter in the registry PCs running Windows 8 (and up) and all the servers using Windows 2012, to prohibit storing unencrypted passwords in RAM (which are usually leveraged by Mimikatz) HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/ SecurityProviders/WDigest/UseLogon Credential=0.
- Type: dir %temp%in "run" and delete all entries after opening any suspicious attachments.
- Type cmd in run and type netstat -na. Checkout Foreign Established connections and IP addresses. Check the IP address for its ownership.
- Type "msconfig" in "run" and check for any unusual executable running automatically.
- Check Network icon (for packets received and sent)/ ADSL lights for data in non-browsing mode. Check data usage pattern in Mobile. If the outgoing is unusually high, then it is very likely that the system is compromised.
- Type "ipconfig/displaydns" in command prompt and look out for any URLs which you have not accessed recently.
- Always be cautious while opening attachments even from the known sources. Try to use non-native applications for opening attachments. Example: For word document use, WordPad to open the attachment.
- When in doubt, better to format the Internet connected computer rather than doing some "patch works".
- Prohibit any remote logon to the system (RDP, SMB, RPC) for local administrators.
- Enforce application whitelisting/Software Restriction Policies on all endpoint workstations. This will prevent malware droppers or unauthorized software from gaining execution on endpoints. Leverage Group Policy/ Applocker to strict enforcing of applications running from %appdata%, %tmp%, %temp%, %localappdata%, %programdata%.

- Isolate hosts in the same VLAN, so that one workstation would not be able to gain access to another one on network levels L2/L3, and could access shared network segments (printers, servers, etc.).
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Disable or prevent ActiveX controls in Microsoft Office Word Document from running without prompting. Click Office Button->Word Options->Trust center->Trust Center Settings->ActiveX Settings.
- Disable Macros in Microsoft office documents (doc/docx, xis/xisx,ppt/pptx and mdb/accdb), by default, Microsoft products come with VBS Macro disable. Office Button->Word Options->Trust center->Trust Center Settings->Macros Settings.
- Disable Java Scripts or similar scripting functions in Adobe Acrobat Reader for PDF files.
- Configure built in "File Protection Setting" feature in Microsoft Office 2010: Office Button->Word Options->Trust Center->Trust Center settings->.
- Configure built in feature for "Protected View" settings in Microsoft Office 2010 to open the Microsoft Office word documents in Protected view:Office Button-> Word Options->Trust Center->Trust Center Settings->Protected View.
- Check for unrecognized tasks being registered in task scheduler using "Schtasks/Query/FO LIST/V" from command prompt.

4. USB storage device (Pen Drive/External Hard Disk etc.):

- Use only official USB storage devices for official work.
- Records of USB storage devices should be maintained.
- Damaged/faulty Removable Storage Media (RISM) should never be handed over to outsiders/manufacturer for repair.
- Sensitive information should be stored on removable media only when required in the cases of assigned duties.
- All media must be stored in a safe, secure environment.
- All media must be handled with care and it must be ensured that it is not kept near magnetic material and not exposed to extreme heat or pollution.
- The computers should be enabled with "Show hidden file and folders" option and "Hide protected operating system files" should be disabled to view hidden malicious files in USB storage devices.
- Make sure there is no hidden file and folders present in the Media.
- Autorun/Autoplay feature should be disabled in all the computers.
- Avoid Baiting. (Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer). Do not use any electronic storage device unless you know its origin is legitimate and safe.
- Scan all electronic media for Malware before use.

5. Password:

- Passwords must be changed at regular intervals.
- Always use different passwords for different accounts.
- Do not share passwords with anyone.

- Passwords should never be written down or stored online without encryption.
- Do not reveal a password in email, chat or other electronic communication.
- Do not reveal a password on questionnaires or security forms.
- Always decline the use of the "Remember Password" feature of applications.
- All users should be aware of how to select strong passwords.
- Strong passwords contain combination of lower case characters, upper case characters, numbers, special characters (e.g. @#$%()_+/) etc.
- Contain at least thirteen alphanumeric characters (except in the case of BIOS, if the same is not possible).
- Weak passwords have the following characteristics:
  - The password contains less than thirteen characters.
  - The password is a word found in a dictionary (English or foreign).
  - The password is a common usage word such as: Names of family, pets, friends, colleagues, movie, novel, comic characters etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like acai, qwerty, asdfg, zxcvb etc.
- Password history should be enforced wherever possible to ensure that the users are forced to select different passwords with a user account.
- Maximum password age should be configured to enforce the period of time (90 days) that a password can be used before the system forces the user to change it.
- Always use different passwords for different accounts.

6. Social Engineering:

- Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email.
- Some emails entice the recipient into opening an attachment that activates a virus or malicious program into your computer.
- Be suspicious of unsolicited phone calls, visits or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

- Take advantage of any anti-phishing features offered by your email client and web browser.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

7. Best Practices for Mobile Phones/Tabs:

- Do not store any classified/sensitive data (text/video/photograph) in the device.
- Before downloading any App, same should be checked for its reputation/review. Read vendor privacy policies before downloading apps and app permission should be reviewed closely.
- Disable installing of third party apps from unknown sources.
- Disable background data for apps.
- Avoid use of wallet aggregator apps, which stores/links other e-wallets and bank apps.
- Auto start, data usage for each App and App permission should be controlled through the security features available (depends on OS and make of the phone).
- Review the default privacy settings of smart phone apps or services and, if needed, change the settings; e.g., settings about whether or not to attach location data to images, to social network posts, etc.
- Relevant anti-virus software should be installed in the smart device and same be updated regularly.
- Turn off GPS location services when not needed.
- Turn off/remove the apps which are not needed.
- When device is idle, it should get locked and require a password/pin or swipe pattern. Set the device to lock in relatively short time.
- Take back-up of data (contacts, personal photos etc.) on external media.
- Do not reply or click on link on SMS or messages or photos sent by strangers.
- Be cautious with public Wi-Fi. Many smartphone users use free Wi-Fi hotspots to access data (and keep their phone plan costs down). There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.

8. Work From Home (WFH) environment:

- Only approved users and devices by the head of the organization should be allowed.
- The organizations must ensure provision of accessing personal computer/devices of employees is done in a standardized and secure manner.
- Appropriate device configuration must be maintained and security capability must be deployed, to prevent remote access of data from outside the organization's boundary by allowing only approved devices based on the unique parameters (MAC ID, IP etc.) of the device.
- Two factor authentications should be implemented on different communication channels (like SMS for OTP and user name and password through secure protocol over the Internet).

9. Video Conferencing – Securing the VC Cameras:

VC cameras, which are not protected with any password or having weak password could be exploited to eavesdrop into the ongoing video conferencing, monitor calls, read call logs, CDR's of VC, intrude/interrupt ongoing calls etc. The vulnerability could be further exploited through remote maintenance module to switch on the camera and monitor activities. To prevent such attacks:

- Set a strong password to manage the VC camera.
- Disable administration interfaces from remote access.
- Disable use of default accounts/passwords.
- Check periodically to detect any misconfigurations or missing patches.

For secure use of commercial VC solutions for discussions between Governments and parent partner organizations:

- A separate system may be designated by the organization. Such system should not store any classified or sensitive information.
- The background for the meeting should be chosen in such a manner (like plain wall, curtains or background option of the VC application) no sensitive documents/surroundings are visible during VC.
- Wherever possible, an isolated Internet connection should be preferred for such VCs. Logical isolation may also be considered for VC systems so that other internal systems are not exposed to the VC network.

10. Email security practices:

- Not to open/reply email links (hyperlinks/web links/URLs mentioned in the body of such mails) claiming to offer anti-spyware software. The links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
- Scan mail attachments before downloading/opening.
- Use two factor authentication wherever possible.
- Use different email accounts for personal and professional purposes.
- Periodically check last log-in activity for any unauthorized access.
- Change passwords of all their online accounts (emails and others) from another secure computer, if any suspicious activities like email access from foreign IP addresses, etc. are noticed.

(Dinesh Bouddh)
Director (NC/CC)

To

All Officers/Officials of Department of Revenue (HQ/CBDT/CBIC).