SECRET

No. 22001/09/2023-CP
Government of India
Ministry of Home Affairs
Cyber and Information Security Division
(CPC Desk)

Date: 08.01.2024
North Block, New Delhi

OFFICE MEMORANDUM

Subject: Standard Operating Procedure (SoP) on Cyber Security for Government Employees.

The undersigned is directed to refer to DGsP/ IGsP Conference, 2022, inter-alia recommending formulation of Standard Operating Procedure (SoP) on Cyber Security for Government Employees. Guidelines on Information Security Practices for Government Entities were issued by CERT-In on 30.06.2023 and are available on their website. Those guidelines inter-alia contain security practices pertaining to data security, secure cloud services, social media security, vulnerability and patch management and security auditing guidelines. Those guidelines have an annexure pertaining to guidelines for Central Government CISOs and Employees.

It is to inform that the National Information Security Policy and Guidelines (NISPG) last circulated by MHA in 2019 is also being revised and is expected to take some time for finalization. During the finalization of the NISPG, the guidelines issued by CERT-In dated 30.06.2023 and the Standard Operating Procedure (SoP) on Cyber Security of Government Employees (copy enclosed) along with similar guidelines available on the subject are proposed to be subsumed into NISPG.

As an interim measure, Standard Operating Procedure (SoP) on Cyber Security for Government Employees (copy enclosed) which inter-alia also contains chapters on online video calls and conferencing, malware defence related, internet connection control, honey trapping and social engineering is being issued with the request that the same may be circulated to all concerned for strict compliance.

Encl: a.a

(Mahendra Vikram Singh)
Under Secretary (CPC)
Telefax:011-23093662
Email: mv.singh@nic.in

To

Secretary-All Ministries/ Departments of Government of India

Copy to:

Director, Intelligence Bureau, North Block, New Delhi.

SECRET

No.-22001/09/2023-CP
Government of India
Ministry of Home Affairs
Cyber and Information Security Division
(CPC Desk)

E-85-349545 7/24

12:40 Pm 78 11/1/24

Date: 08.01.2024
North Block, New Delhi

OFFICE MEMORANDUM

Subject: Standard Operating Procedure (SoP) on Cyber Security for Government Employees.

The undersigned is directed to refer to DGsP/ IGsP Conference, 2022, inter-alia recommending formulation of Standard Operating Procedure (SoP) on Cyber Security for Government Employees. Guidelines on Information Security Practices for Government Entities were issued by CERT-In on 30.06.2023 and are available on their website. Those guidelines inter-alia contain security practices pertaining to data security, secure cloud services, social media security, vulnerability and patch management and security auditing guidelines. Those guidelines have an annexure pertaining to guidelines for Central Government CISOs and Employees.

It is to inform that the National Information Security Policy and Guidelines (NISPG) last circulated by MHA in 2019 is also being revised and is expected to take some time for finalization. During the finalization of the NISPG, the guidelines issued by CERT-In dated 30.06.2023 and the Standard Operating Procedure (SoP) on Cyber Security of Government Employees (copy enclosed) along with similar guidelines available on the subject are proposed to be subsumed into NISPG.

As an interim measure, Standard Operating Procedure (SoP) on Cyber Security for Government Employees (copy enclosed) which inter-alia also contains chapters on online video calls and conferencing, malware defence related, internet connection control, honey trapping and social engineering is being issued with the request that the same may be circulated to all concerned for strict compliance.

Encl: a.a

for JS | CISO

JS (Adv)

12/1

(Mahendra Vikram Singh)
Under Secretary (CPC)
Telefax:011-23093662
Email: mv.singh@nic.in

To

Secretary-All Ministries/ Departments of Government of India

Copy to:

Director, Intelligence Bureau, North Block, New Delhi.

SOP ON CYBER SECURITY FOR GOVERNMENT EMPLOYEES

1. SCOPE AND TARGET AUDIENCE

The following guidelines shall be followed in full letter and spirit by all government employees, including outsourced/contractual/temporary employees, who are working for government Ministry/Department/Organisations.

2. DESKTOP/LAPTOP/THIN-CLIENT/WORKSTATION AND PRINTER SECURITY AT OFFICE/ INTRANET LAN

2.1. Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.

2.2. Set three tier passwords i.e. BIOS Password, Windows and screensaver password. Enable screen lock out and log off settings after certain inactivity time.

2.3. Ensure that the Operating System and BIOS firmware are updated with the latest updates/patches.

2.4. Set Operating System updates to auto-updated from a trusted source.

2.5. Ensure that the Antivirus clients installed on systems/devices are updated with the latest virus definitions, signatures and patches. Perform full antivirus scan of entire system on regular interval after updating its signatures.

2.6. Only Applications/software's, which are part of the allowed list, authorized by CISO, shall be used; any application/software which is not part of the authorized list approved by CISO, shall not be used. No software should be downloaded/installed from internet without the permission of CISO. Computer systems must have genuine Windows OS license and applications. The activation-key must be recorded and kept for OS license activation in case system is formatted due to unavoidable situation. No unwanted applications or data must be stored or installed on the system.

2.7. Always lock/log off from the desktop when not in use.

2.8. Shutdown the desktop before leaving the office.

2.9. Keep printer's software updated with the latest updates/patches.

2.10. Setup unique pass codes for shared printers.

2.11. Internet access to the printer should not be allowed.

2.12. Printer to be configured to disallow storing of print history.

2.13. Enable Desktop Firewall for controlling information access.

2.14. Keep the GPS, Bluetooth, Wi-fi, NFC and other sensors disabled on the desktops/laptops. They may be enabled only when required.

2.15. Use a Hardware VPN Token for connecting to any IT Assets located in Data Centre.

2.16. Do not write passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on users table etc.).

2.17. Do not use any external mobile App based scanner services (ex: Cam scanner etc) for scanning internal government documents.

2.18. Do not use personal laptops/tablets/mobiles/fitbits or any other electronic gadgets in office LAN.

2.19 User must ensure that the pc/laptop/workstation in intranet must not be connected to any external Network by any means, wired or wireless, under any circumstance.

2.20 Remove pirated /unsupported Operating systems and other software/applications that are not part of the authorized list of software.

2.21 Ensure that systems are shut down after office hours.

2.22 Keep regular backup of critical data.

2.23 Remove/delete applications which are not in use.

2.24 User shall never share hard disk or folders with anyone, by default. However, whenever necessary, only the required folders shall be shared with the specific user for a specific period of time. A proper record needs to be maintained for any such sharing with the period of sharing clearly mentioned.

2.25 Maintain Air gap between intranet and internet systems as per organization's existing information security policies as well the baseline security guidelines of the overarching Ministry to ensure cyber resilence.

3. PASSWORD MANAGEMENT

3.1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.

3.2. Change passwords at least once in 30 days.

3.3. Use Multi-Factor Authentication, wherever available.

3.4. Don't use the same password in multiple services/websites/apps.

3.5. Don't save passwords in the browser or in any unprotected documents.

3.6. Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persons.

3.7 Common password such as admin@123, Password, admin or which contain words such as unit name, room no, telephone, mobile or other things which is generally known to other colleagues must be avoided.

4. INTERNET BROWSING SECURITY

4.1. While accessing Government applications/services, email services or banking/payment related services or any other important application/services, always use Private Browsing/Incognito Mode in your browser.

4.2. While accessing sites where user login is required, always type the site's domain name/URL, manually on the browser's address bar, rather than clicking on any link.

4.3. Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.

4.4. Don't store any usernames and passwords on the internet browser.

4.5. Don't store any payment related information on the internet browser.

4.6. Don't use any 3rd party anonymization services (3rd party VPN, Tor, Proxies etc). Avoid using unauthorized VPN services and remote desktop tools like Anydesk and Teamviewer.

4.7. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.

4.8. Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software).

4.9. Don't use your official systems for installing or playing any Games.

4.10. Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortening services. Such links may lead to a phishing/malware webpage, which could compromise the device.

4.11 Cache and History should be deleted regularly from the browsers after every usage on internet connected systems.

4.12 Do not leave any official document on internet connected computers.

4.13 Enable genuine ad-blocker to protect from malvertising.

4.14 Ensure the genuineness of SSL/TLS website while performing online transactions.

5. MOBILE SECURITY

5.1. Ensure that the mobile operating system is updated with the latest available updates/patches.

5.2. Don't root or jailbreak your mobile device. Rooting or Jail breaking process disables many in-built security protections and could leave your device vulnerable to security threats.

5.3. Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.

5.4. Download Apps from official app stores of Google (for android) and apple (for iOS). Do not install apps from untrusted sources unless you are sure about the source of the app.

5.5. Before downloading an App, check the developer & popularity of the app and read the user reviews.

5.6. Observe caution before downloading any apps which has a bad reputation or less user base etc.

5.7. While participating in any sensitive discussions switch-off the mobile phone or leave the mobile in a secured area outside the discussion room.

5.8. Don't accept any unknown request for Bluetooth pairing or file sharing.

5.9. Before installing an App, carefully read and understand the device permissions required by the App along with the purpose of each permission.

5.10. In case of any disparity between the permissions requested and the functionality provided by an app, users to be advised not to install the App (Ex: A calculator app requesting GPS and Bluetooth permission).

5.11. Note down the unique 15-digit IMEI number of the mobile device and keep it offline. It can be useful for reporting in case of physical loss of mobile device.

5.12. Use auto lock to automatically lock the phone or keypad lock, protected by pass code/ security patterns, to restrict access to your mobile phone.

5.13. Use the feature of Mobile Tracking which automatically sends messages to two preselected phone numbers of your choice which could help if the mobile phone is lost/ stolen.

5.14. Take regular offline backup of your phone and external/internal memory card.

5.15. Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates.

5.16. 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 latest news. Such links may lead to a phishing/malware webpage/app, which could compromise your device.

5.17. Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.

5.18. Disable automatic downloads in your phone.

5.19. Always keep an updated antivirus security solution installed.

6. EMAIL SECURITY

6.1. Ensure that Kavach Multi-Factor Authentication is configured on the NIC Email Account.

6.2. Download Kavach app from valid mobile app stores only. Do not download from any other website.

6.3. Do not share the email password or Kavach OTP with any unauthorized persons.

6.4. Don't use any unauthorized/external email services for official communication.

6.5. Don't click/open any link or attachment contained in mails sent by unknown sender. Ensure the authenticity of the sender before opening the attachment in the email. Check for headers of original mail to check the authenticity.

6.6. Regularly review the past login activities on NIC's Email service by clicking on the "login history" tab. If any discrepancy is observed in the login history, then the same should be immediately reported to CERT-In and NIC-CERT.

6.7. Use PGP or digital certificate to encrypt e-mails that contains important information

6.8. Be cautious while opening emails with attachments and hyperlinks on Gov/Nic email. Observe extra caution with documents containing macros while downloading attachments, always select the "disable macros" option and ensure that protected mode is enabled on your office productivity applications like MS Office.

6.9 Be aware of current social engineering attacks and do not install any files in computer systems based on the directions over phone/mobile, wherein the caller would be pretending to be someone very important government official and insisting on urgency to download the files sent over email.

7. REMOVABLE MEDIA SECURITY

7.1 Perform a low format of the removable media before the first-time usage.

7.2 Perform a secure wipe to delete the contents of the removable media.

7.3 Scan the removable media with Antivirus software before accessing.

7.4 Secure the files/folders on the removable media by encryption.

7.5 Always protect your documents with strong password.

7.6 Don't plug-in the removable media on any unauthorized devices.

7.7 Disable auto-run functionality of the removable media while plug-in on the computer system.

7.8 Do not use removable disk in unsecured systems.

8. SOCIAL MEDIA SECURITY

8.1. Limit and control the use/exposure of personal information while accessing social media and networking sites.

8.2. Always check the authenticity of the person before accepting a request as friend/contact.

8.3. Use Multi-Factor authentication to secure the social media accounts.

8.4. Do not click on the links or files sent by any unknown contact/user.

8.5. Do not publish or post or share any internal government documents or information on social media.

8.6. Do not publish or post or share any unverified information through social media.

8.7. Do not share the @gov.in/@nic.in email address on any social media platform.

8.8. Do not share any official documents through messaging apps like WhatsApp, Telegram, Signal etc. It is recommended to use NIC's Sandes App instead of any 3rd party messaging app, for official communication.

8.9 Avoid to share private information such as home address, private pictures, phone number, Aadhaar Number or any other private or official information publicly on social media.

8.10 Review the social media privacy settings to ensure the level of security to personnel networking profile.

8.11 Avoid to click on Ads that promise free money, prizes or discounts.

9. ONLINE VIDEO CALLS AND CONFERENCING

9.1 Enable the password authentication to enter in the meeting room.

9.2 Enable waiting room feature in video conferencing software.

9.3 Lock meeting once all the participants have joined.

9.4 Turn off the screen sharing functionality and remote monitoring features.

9.5 Be careful about clicking on links and opening documents.

9.6 Be careful what you show in the background.

9.7 Be careful what is on your screen before using the screen sharing function.

9.8 Turn off anything that gives the app too many permissions.

10. MALWARE DEFENSE RELATED

10.1 Always set automatic updates for Operating System, Anti-Virus and Applications as envisaged in earlier points.

10.2 Configure web browser to block pop-ups, disable unnecessary plugins and enable secure browsing features.

10.3 Enable hidden file & system file view to find any unusual or hidden files.

10.4 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").

10.5 Configure the following parameter in the registry of PCs running Windows 8 (and above) 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/UseLogonCredent ial=0

10.6 Type %temp% in "Windows Run" and delete all entries after opening any suspicious attachments.

10.7 Open Command Prompt and type netstat –na. Checkout Foreign established connection with IP addresses and its ownership.

10.8 Type "msconfig" in "Windows Run" and check for any unusual executable running automatically.

10.9 Check Network adapter for data/packets received and sent. If the outgoing / sent is unusually high, then it is very likely that the system is compromised.

10.10 Type "ipconfig /displaydns" in command prompt and look out for any URLs which you have not accessed recently.

10.11 Always be cautious while opening attachments even from the known sources. Try to use non-native applications for opening attachments (as an example, use WordPad to open a word document).

10.12 When in doubt, better to format the Internet connected computer instead of performing some "patch works".

10.13 Prohibit any remote logon to the system (RDP, SMB, RPC) for local administrators.

10.14 Check regularly if any unusual applications running from %appdata%, %tmp%, %temp%, %localappdata%, %programdata% directories.

10.15 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.)

10.16 Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources as well as addresses and block these before receiving and downloading messages.

10.17 Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

10.18 Disable or prevent ActiveX controls in Microsoft Office Word Document from running without prompting.

10.19 Disable Macros in Microsoft office documents (doc/docx, xls/xlsx, ppt/pptx and mdb/accdb). By default, Microsoft products come with VBS Macro disabled.

10.20 Disable Java Scripts or similar scripting functions in Adobe Acrobat Reader for PDF files.

10.21 Configure built in "File Protection Setting" feature in Microsoft Office.

10.22 Configure built in feature for "Protected View" settings in Microsoft Office to open the Microsoft Office word documents in protected view.

10.23 Check for unrecognized tasks being registered in task scheduler using "Schtasks /Query /FO LIST /V" from command prompt.

10.24 Use Tools that can analyze for malicious code execution.

10.25 Avoid internet access through administrator account. Instead, use a limited user account, which limits the impact of malware that tries to gain administrative access.

11. INTERNET CONNECTION CONTROL

11.1 Enable strong and latest secure encryption in Wireless networks.

11.2 Change default credentials for wireless admin console and network.

11.3 Update wireless router firmware regularly.

11.4 Turn off remote management functionalities like WPS and Universal Plug and Play (UPnP).

11.5 Enable MAC address filtering and MAC binding to keep unauthorized devices away from wireless network.

11.6 Avoid to connect personal devices to unsecured network such as public unprotected network.

11.7 Avoid submitting sensitive information when using public Wi-Fi.

11.8 Keep wireless network down, when not in use.

12. HONEY TRAPPING AND SOCIAL ENGINEERING

12.1 Be vigilant of suspicious/unsolicited communications by unknown individuals. Be particularly wary of individuals who seem to be overly interested in personal/professional life, or who ask for sensitive information. Whenever an unknown individuals tries to contact an officer through whatsapp, telegram, facebook, linkedin or any other social media app/website, Government Official should immediately inform his superior officers. The beginning signs of these interactions may be such as, liking every posts, commenting/complementing on near every posts.

12.2 Any content (post, picture, blog, profile info etc) posted on social media should not reveal any sensitive information like Rank/Department/Unit/Current Project/Uniform/Tour Plans etc. in the backdrop.

12.3 Clicking/opening on advertisements or any downloadable content shared by the unknown, should be avoided, as it may lead to installing of malware on the systems.

12.4 Steer away from unknown dating sites and don't trust generous offers.

12.5 Don't meet any unknown or little known person in any shady or lonely places like hotel rooms etc.

12.6 Do not engage in video calls from unknown numbers in social media platforms like whatsapp, facebook, telegram, signal etc.

13. SECURITY ADVISORY AND INCIDENT REPORTING

13.1 Adhere to the NISPG Guidelines and other Security Advisories published from time to time by CERT-In, MHA, NCIIPC, MeiTY and other important government organisations.

13.2 Report any cyber security incident, including suspicious mails and phishing mails immediately to CISO or Tech/IT team of your organisations for further escalation to CERT-In (incident@cert-in.org.in) and NIC-CERT (incident@nic-cert.nic.in).

14. CYBER SECURITY RESOURCES

The following resources may be referred for more details regarding the cyber security related notifications/information published by Government of India:

S N	Resource URL	Description
1	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in	Security Tools & Best Practices
5	https://infosecawareness.in/	Security Awareness materials
6	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips

7	https://security.nic.in/docs/Security_Policies_for_GOI/Password%20Management%20Guidelines.pdf	NIC Password Policy
8	https://guidelines.india.gov.in/	Guidelines for Indian Government Websites

15. COMPLIANCE

15.1 All government employees, including temporary, contractual/outsourced resources are required to strictly adhere to the guidelines mentioned in this document in full letter and spirit. Any non-compliance may be acted upon by the respective CISOs/Ministry/Department heads.

15.2 CISOs or Tech/IT Head need to ensure that these guidelines are adhered upon by all the employees. Sensitization cum training sessions should be conducted by CISOs or Tech/IT Heads explaining the salient features of this SOP. These sessions should be regular feature and cover all the employees within the Ministry/Department/Organization from top to bottom level.

15.3 CISOs or Tech/IT heads should regularly conduct security audits to ensure cyber hygiene.

*****