



कर्मचारी राज्य बीमा निगम  
(श्रम एवं रोजगार मंत्रालय, भारत सरकार)  
Employees' State Insurance Corporation  
(Ministry of Labour & Employment, Govt. of India)



मुख्यालय/Headquarters  
पंचदीप भवन, सी. आई. जी. मार्ग, नई दिल्ली-110002  
Panchdeep Bhawan, C.I.G. Marg, New  
Delhi – 110002  
Website : <https://esic.gov.in>

Computer No.E 13105  
File No. I-17012/1/2022-ICT

Date : 26.02.2024

To

All Divisional Heads, ESIC HQ/ Insurance Commissioner (NTA)  
All Addl. Commissioner & Regional Director(s)/RDs/Joint Director(s)/Deputy  
Director(I/c)/SRO(I/c)  
All Dean(s)/Medical Superintendent(s)/  
All Director(s)/ Civil Surgeon(s)/ State Directorates  
All Sub-ordinate offices through their respective Regional Offices/Sub-Regional  
Offices/ State Directorate(s)

**Subject: Cyber Security Guidelines and Standard Operating Procedure**

Sir/Madam,

Please refer to this office letter of even No. dated 13/19.12.2022(Copy attached).  
Apart from above mentioned letter, Ministry of Labour and Employment, Govt. of India has  
issued Office Memorandum No. Z-20025/05/2023-IT Cell (Pt.A) dated 17.01.2024 on the  
subject-“Standard Operating Procedure (SoP) on Cyber Security for Government Employees  
– reg.” which, inter-alia, contains chapters on online video calls and conferencing, malware  
defence related, internet connection control honey trapping and social engineering (copy  
attached).

All heads of Accounting Units and heads of offices under their jurisdiction are  
requested to see to it for compliance and also circulate the enclosed SoP to all concerned for  
strict compliance.

**COMPLIANCE**

All ESIC/ESIS officers & officials, including temporary, contractual/outsourced  
resources are required to strictly adhere to the guidelines and Standard Operating Procedure,  
mentioned above. The above instructions are to be complied by the Regional  
Heads/Institution Heads, who shall be responsible for non-implementation of the same in the  
offices under their control. Any non-compliance shall be viewed seriously, and suitable action  
will be taken by the Chief Information Security Officer (CISO)/Department Heads.

Compliance report to above effect along with status report regarding all devices by all  
Regional Heads / Institution Heads is to be submitted immediately.

This issues with the approval of Director General.

Enclosure-As above.

Yours Sincerely

(R.K. Gautam)

Insurance Commissioner (ICT)

Z-20025/05/2023-IT CELL(Pt.A)  
Government of India  
Ministry of Labour and Employment  
IT Cell

Shram Shakti Bhawan, Rafi Marg  
New Delhi, Dated, the 17<sup>th</sup> January, 2024.

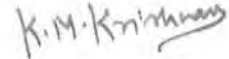
OFFICE MEMORANDUM

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

The undersigned is directed refer to the subject mentioned above and to forward herewith a copy of Standard Operating Procedure (SoP) on Cyber Security for Government Employees (copy enclosed) which, inter-alia, contains chapters on online video calls and conferencing, malware defence related, internet connection control, honey trapping and social engineering.

2. In this regard, all the Bureau Heads and all the Heads of subordinate offices/attached offices and organizations under the Ministry of Labour and Employment are requested to see it for compliance and also circulate the enclosed SoP to all concerned for strict compliance.

Encl. as above.



(K.M. Krishnan)

Under Secretary to the Government of India

Tele. No: 011-23473100

Email: km.krishnan@nic.in

To:

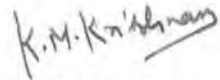
All Bureau Heads/ DG-ESIC/ CPFC/ CLC(C)/ DGMS/ DGFASLI/ DGLB/ DGLW/ DDG(E)/  
DG-VVGNLI/ DG-DTNBWED

Copy to:

1. Sh. Sanjay Kumar, HOD, NIC, Ministry of Labour and Employment

Copy for information to:

1. PPS to Secretary (L&E)
2. PPS to SLEA
3. PA to DS(AKS)



(K.M. Krishnan)

Under Secretary to the Government of India



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 resilience.



### **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/UseLogonCredential=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](mailto:incident@cert-in.org.in)) and NIC-CERT ([incident@nic-cert.nic.in](mailto: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:

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



7	<a href="https://security.nic.in/docs/Security_Policies_for_GOI/Password%20Management%20Guidelines.pdf">https://security.nic.in/docs/Security_Policies_for_GOI/Password%20Management%20Guidelines.pdf</a>	NIC Password Policy
8	<a href="https://guidelines.india.gov.in/">https://guidelines.india.gov.in/</a>	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.

\*\*\*\*\*





कंप्यूटर सं. E-13105

फाइल सं. 17012/1/2022-ICT

सेवा में,

दिनांक : 13.12.2022

19

सभी अपर आयुक्त एवं क्षेत्रीय निदेशक/ क्षेत्रीय निदेशक/प्रभारी उप निदेशक/प्रभारी उप क्षेत्रीय कार्यालय  
सभी संकायाध्यक्ष/चिकित्सा अधीक्षक  
सभी निदेशक/सिविल सर्जन/ राज्य निदेशालय  
सभी संबद्ध कार्यालयों को उनके संबंधित क्षेत्रीय कार्यालयों/ उप क्षेत्रीय कार्यालयों/राज्य निदेशालयों के माध्यम से

### विषय: साइबर सुरक्षा दिशानिर्देश

#### महोदय/महोदया,

सूचना और संचार प्रौद्योगिकी (आईसीटी) देशभर के सरकारी मंत्रालयों और विभागों में सर्वव्यापी हो गई है। जमीनी स्तर पर उपयुक्त साइबर सुरक्षा उपायों को अपनाने में कमी के कारण आईसीटी के बढ़ते अंगीकरण तथा प्रयोग में वृद्धि से सरकार के लिए साइबर हमले और खतरे बढ़ गए हैं। सरकारी कर्मचारियों, संविदात्मक/बहिःस्रोतन (आउटसोर्स) संसाधनों को संवेदनशील बनाने और साइबर सुरक्षा परिप्रेक्ष्य में, **क्या करें और क्या न करें**, के बारे में उनके बीच जागरूकता पैदा करने के लिए इन दिशानिर्देशों को संकलित किया गया है। देशभर के सभी क.रा.बी.निगम/क.रा.बी.योजना कार्यालयों में इन एक समान साइबर सुरक्षा दिशानिर्देशों का सख्ती से पालन करने से क.रा.बी.निगम की योजना गतिविधियों को पूरा करने के लिए उपयुक्त सुरक्षित वातावरण सुनिश्चित होगा।

#### साइबर सुरक्षा क्या करें

- 1) बड़े अक्षरों, छोटे अक्षरों, संख्याओं और विशेष वर्णों के संयोजन का उपयोग करते हुए 10 कैरेक्टर की न्यूनतम लंबाई वाले जटिल पासवर्ड का प्रयोग करें।
- 2) अनुमान लगाने में मुश्किल पासवर्ड या पासफ्रेज़ (passphrase) का प्रयोग करें।
- 3) 45 दिनों में कम से कम एक बार अपना पासवर्ड बदलें।
- 4) हमेशा ऐसे कंप्यूटर से पासवर्ड बदलें जो वायरस/मैलवेयर(malware) से मुक्त हो।
- 5) जहां भी उपलब्ध हो, बहु-स्तरीय प्रमाणीकरण का उपयोग करें।
- 6) अपने डाटा और फाइलों को सेकेंडरी ड्राइव (उदाहरण : D:\) में सेव करें।
- 7) अपने महत्वपूर्ण डाटा का ऑफलाइन बैकअप बनाए रखें। महत्वपूर्ण डाटा का नियमित बैकअप मानकों के अनुसार किया जाना है।
- 8) अपने ऑपरेटिंग सिस्टम और बीआईओएस फर्मवेयर को नवीनतम अपडेट/पैच के साथ अपडेट रखें।
- 9) सरकार द्वारा पेश किए गए इंटरप्राइज़ एंटीवायरस क्लाइंट को अपने आधिकारिक डेस्कटॉप/लैपटॉप पर इंस्टॉल करें। सुनिश्चित करें कि एंटीवायरस क्लाइंट नवीनतम वायरस डेफिनेशन, सिग्नेचर और पैच के साथ अद्यतित है।
- 10) उस मशीन को एंटी-वायरस के नवीनतम पैच(patch) के साथ स्कैन करें, जिस पर आप अपने मेल का प्रयोग कर रहे हैं और नवीनतम पैच के साथ उनके ओएस को भी अपडेट करवाएं।
- 11) क.रा.बी.निगम प्रॉक्सी(proxy) सेटिंग्स को proxy.esic.in और पोर्ट(Port)3128 में कॉन्फिगर(configure) करें।
- 12) समय तुल्यकालन (Time Synchronization) के लिए अपने सिस्टम की एनटीपी सेटिंग्स में एनआईसी की एनटीपी सेवा (samay1.nic.in, samay2.nic.in) को कॉन्फिगर करें।



- 13) अधिकृत तथा लाइसेंस प्राप्त सॉफ्टवेयर का ही उपयोग करें और सिस्टम में संस्थापित/उपलब्ध होने पर किसी भी की लॉग (Key log) सॉफ्टवेयर को हटा दें।
- 14) सुरक्षा खतरों तथा वायरस के लिए कार्यस्थल में उपयोग किए जाने वाले सिस्टम/कंप्यूटर/लैपटॉप को नियमित रूप से अवश्य स्कैन किया जाना चाहिए।
- 15) यह सुनिश्चित किया जाए कि सिस्टम पर उचित सुरक्षा दृढीकरण (Hardening) किया जाता है।
- 16) जब आप अस्थायी रूप से अपना डेस्क छोड़ते हैं, तो अपने कंप्यूटर सेशन में हमेशा लॉक/उससे लॉग ऑफ करें। उपयोग न होने पर अपने कंप्यूटर, लैपटॉप तथा मोबाइल फोन को लॉक करें। यह डेटा को अनधिकृत पहुंच तथा उपयोग से बचाता है।
- 17) जब आप कार्यालय से जाएं तो यह सुनिश्चित करें कि आपका कंप्यूटर तथा प्रिंटर ठीक से शट डाउन (shutdown) हो।
- 18) अपने प्रिंटर से सॉफ्टवेयर को नवीनतम अपडेट/पेच के साथ अपडेट रखें।
- 19) साझा प्रिंटर के लिए अद्वितीय(unique) पासकोड सेटअप करें।
- 20) डाटा केंद्रों में स्थित किसी सूचना प्रौद्योगिकी परिसंपत्ति को अलग से जोड़ने हेतु हार्डवेयर वर्चुअल प्राइवेट नेटवर्क (VPN) टोकन का उपयोग करें।
- 21) अपने कंप्यूटरों तथा मोबाइल फोन पर जीपीएस, ब्लूटूथ, एनएफसी तथा अन्य सेंसर को बंद रखें। इन्हें तब ही इनेबल किया जाए जब उनकी जरूरत हो।
- 22) गूगल (एंड्रॉइड के लिए) तथा ऐप्पल (आइओएस के लिए) के आधिकारिक ऐप स्टोर से आधिकारिक ऐप डाउनलोड करें।
- 23) वायरलेस संचार स्वाभाविक रूप से असुरक्षित होते हैं। सुरक्षा प्रोटोकॉल तथा चयनात्मक पहुंच नियंत्रण भूमिका तथा उत्तरदायित्वों के आधार पर सुनिश्चित किया जाना चाहिए।
- 24) नियमित कार्य के लिए अपने कंप्यूटर/लैपटॉप तक पहुंच के लिए एक मानक प्रयोक्ता (नॉन-एडमिनिस्ट्रेटर) अकाउंट का उपयोग करें।
- 25) इलेक्ट्रॉनिक माध्यम से कोई महत्वपूर्ण सूचना अथवा दस्तावेज भेजते समय कृपया प्रेषण से पहले डाटा को एन्क्रिप्ट करें। आप लाइसेंस प्राप्त एन्क्रिप्शन सॉफ्टवेयर का उपयोग अथवा एक ओपन पीजीपी आधारित एन्क्रिप्शन या फाइलों को एक कंप्रेस्ड जिप पर जोड़कर उस जिप को पासवर्ड से सुरक्षित रखें। संरक्षित फाइलों को खोलने का पासवर्ड वैकल्पिक संचार माध्यम जैसे एसएमएस, संदेश आदि के माध्यम से प्राप्तकर्ता के साथ साझा किया जाना चाहिए।
- 26) कोई भी संक्षिप्त शॉर्टनड यूनिफार्म रिसोर्स लोकेटर (URLs) जैसे (tinyurl.com/ab534/) खोलते समय सावधानी बरतें। कई मालवेयर तथा फिशिंग साइटें यूआरएल शार्टनर सर्विसेस का दुरुपयोग करती हैं।
- 27) एसएमएस अथवा सोशल मीडिया आदि के माध्यम से साझा किए गए लिंक जहां लिंक से पहले ऑफर/छूट हैं अथवा किसी भी वर्तमान मामले के संबंध में ब्योरे उपलब्ध कराने का दावा करते हैं, उन्हें खोलते समय सावधानी बरतें। ऐसे लिंक फिशिंग(phishing)/मालवेयर(malware) वेबपेज का कारण बनते हैं जोकि आपके डिवाइस को संक्रमित कर सकते हैं।
- 28) संदिग्ध ईमेल अथवा सुरक्षा से जुड़ी किसी घटना की सूचना तुरंत [incident@cert-in.org.in](mailto:incident@cert-in.org.in), [incident@nic-cert.nic.in](mailto:incident@nic-cert.nic.in) को तथा अपने अधिकारी/प्रभागाध्यक्ष को तुरंत दें।
- 29) एनआइसी-सीईआरटी (<https://nic-cert.nic.in/advisories.jsp> ) तथा सीईआरटी-आइएन (<https://www.cert-in.org.in>) द्वारा प्रकाशित सुरक्षा सलाह का पालन करें।
- 30) हमेशा यह सुनिश्चित करें कि "रिमेम्बर पासवर्ड" विकल्प कहीं भी अर्थात् ब्राउजर में अथवा आइएमएपी/पीओपी मेल क्लायंट अर्थात् आउटलुक, थंडरबर्ड, सीमॉन्की, विन्डोज मेल आदि में कन्फिगर न किया जाए।
- 31) कार्यस्थल पर उपयोग किए जाने वाले प्रत्येक सिस्टम/कंप्यूटर/लैपटॉप को पासवर्ड से सुरक्षित किया जाना चाहिए।
- 32) ईमेल एक्सेस करने के लिए सभी को टू फैक्टर ऑथेंटिकेशन (जैसे कवच) का इस्तेमाल करना चाहिए। मेल आईडी का पासवर्ड किसी के साथ साझा नहीं करना चाहिए ।



- 33) उपयोगकर्ताओं को हर सप्ताह सुरक्षा संबंधी खतरों और ऐसी घटनाओं को रोकने के तरीके के बारे में शिक्षित करें। मानक दिशानिर्देश, मानक प्रचालन प्रक्रियाओं (एसओपी) और प्रोटोकॉल सभी को परिचालित किए जाने चाहिए।
- 34) यदि सिस्टम किसी वायरस/मैलवेयर/फिशिंग सॉफ्टवेयर से संक्रमित पाया जाता है तो,
  - क. सभी उपयोगकर्ताओं (डेस्कटॉप और मोबाइल क्लाइंट दोनों) के लिए कवच में आईएमएपी (IMAP) सेवा को डिस्पैबल करें।
  - ख. संक्रमित कंप्यूटरों को एलएएन (LAN)/इंटरनेट से तुरंत डिस्कनेक्ट कर दें।
  - ग. डाटा फाइलों का बैकअप लेने के बाद संक्रमित कंप्यूटरों की हार्ड डिस्क को फॉर्मेट किया जा सकता है;
  - घ. ऑपरेटिंग सिस्टम और एप्लिकेशन को संक्रमण मुक्त और अपडेटेड सॉफ्टवेयर से फिर से इंस्टॉल किया जाना चाहिए।
  - ङ. बैकअप डेटा को पुनर्स्थापित (रीस्टोर) करने से पहले वायरस के लिए स्कैन किया जाना चाहिए।
  - च. सहकर्मियों और अन्य कर्मचारियों को सुरक्षा नीति और संबंधित जानकारी के बारे में शिक्षित करें।

### साइबर सुरक्षा में वर्जित

- 1) एक से अधिक सेवाओं/वेबसाइटों/ऐप्स में एक ही पासवर्ड का उपयोग न करें।
- 2) पासवर्ड किसी से साझा न करें। पासवर्ड दूसरों के साथ साझा नहीं किया जाना चाहिए, चाहे आप उन्हें जानते हों या नहीं। अपने पासवर्ड या पासफ्रेज़ को गोपनीय रखें। आप अपनी निजी जानकारी(credential) से जुड़ी सभी गतिविधियों के लिए ज़िम्मेदार हैं।
- 3) अपने पासवर्ड को ब्राउजर या किसी असुरक्षित दस्तावेज में सेव न करें।
- 4) किसी भी असुरक्षित सामग्री पर कोई भी पासवर्ड, आईपी एड्रेस, नेटवर्क डायग्राम या अन्य संवेदनशील जानकारी न लिखें (उदाहरण के लिए : पताका (स्टिकी)/पोस्ट-इट नोट्स, पिन किया हुआ या आपकी टेबल पर पोस्ट किया गया सादा कागज, आदि)
- 5) अपने डेटा और फाइलों को सिस्टम ड्राइव (जैसे : c:\ or root) पर सेव न करें।
- 6) किसी भी गैर-सरकारी क्लाउड सेवा (जैसे : Google ड्राइव, ड्रॉपबॉक्स, आदि) पर किसी भी आंतरिक/प्रतिबंधित/गोपनीय सरकारी डाटा या फाइलों को अपलोड या सेव न करें।
- 7) अप्रचलित या असमर्थित ऑपरेटिंग सिस्टम का उपयोग न करें।
- 8) कार्यालयी कंप्यूटर/लैपटॉप और किसी अन्य डिवाइस को निजी नेटवर्क (मोबाइल हॉटस्पॉट) से न जोड़ें।
- 9) कार्यालयी कंप्यूटर, सिस्टम या लैपटॉप से किसी को भी आधिकारिक प्रयोजनों के लिए संचार हेतु किसी भी निजी मेल आईडी का उपयोग नहीं करना चाहिए। सभी अधिकारियों को gov.in (nic.in), आदि के साथ समाप्त होने वाली कार्यालयी ई-मेल आईडी का उपयोग करना चाहिए।
- 10) कार्यालयी सिस्टम पर निजी काम न करें।
- 11) क.रा.बीमा प्रबंधन की अनुमति के बिना पोर्टेबल डिवाइस जैसे पेन ड्राइव आदि को प्लग इन न करें। जैसे ही आप उन्हें कंप्यूटर में प्लग करते हैं, इन उपकरणों को कोड के साथ संक्रमण किया जा सकता है।
- 12) कार्यालयी सिस्टम पर किसी अन्य साइट (जो कार्यालयी आवश्यकता से संबंधित न हो) को कनेक्ट न करें।
- 13) किसी तृतीय पक्ष (थर्ड पार्टी) डीएनएस (DNS) सेवा या एनटीपी (NTP) सेवा का उपयोग न करें।
- 14) किसी तीसरे पक्ष की पहचान छिपाने वाली सेवाओं का इस्तेमाल न करें (उदाहरण : नोर्ड वीपीएन, एक्सप्रेस वीपीएन, टोर, प्रॉक्सी, आदि)।
- 15) किसी भी तृतीय पक्ष (थर्ड पार्टी) टूलबार (जैसे : डाउनलोड मैनेजर, weather टूल बार, askme टूल बार आदि) का इस्तेमाल न करें।
- 16) किसी भी चोरी के (पायरेटेड) सॉफ्टवेयर को संस्थापित या उपयोग न करें (जैसे : क्रैक, keygen, आदि)।
- 17) अज्ञात प्रेषक द्वारा भेजे गए ईमेल में निहित कोई भी लिंक या अटैचमेंट न खोलें ।
- 18) प्रणाली पासवर्ड अथवा प्रिंटर पासकोड अथवा वाई-फाई पासवर्ड किसी भी अनधिकृत व्यक्तियों से साझा न करें।



- 19) प्रिंटर के लिए इंटरनेट एक्सेस की अनुमति प्रदान न करें।
- 20) प्रिंटर को अपनी प्रिंट हिस्ट्री स्टोर करने की अनुमति प्रदान न करें।
- 21) सामाजिक मीडिया अथवा तृतीय पक्ष मैसेजिंग ऐप्स पर संवेदनशील ब्योरे का खुलासा न करें।
- 22) किसी अपरिचित व्यक्ति द्वारा साझा यूएसवी ड्राइव सहित किसी भी अनधिकृत बाह्य उपकरणों पर प्लग-इन न करें।
- 23) किसी भी अनधिकृत दूरवर्ती प्रशासनिक टूल्स (उदाहरण : टीमव्यूवर, एम्मि एडमिन, ऐनीडेस्क आदि) का प्रयोग न करें।
- 24) संवेदनशील आंतरिक बैठकों और चर्चाओं के संचालन के लिए किसी भी अनधिकृत तृतीय पक्ष वीडियो कॉन्फ्रेंसिंग का प्रयोग न करें।
- 25) कार्यालयी संप्रेषण के लिए किसी भी बाह्य ई-मेल सेवाओं का प्रयोग न करें।
- 26) असत्यापित अथवा अविश्वस्त लिंक अथवा वेबसाइटों को किसी भी समय एक्सेस न करें।
- 27) अपने मोबाइल फोन को जेलब्रेक अथवा रूट न करें।
- 28) अपने नियमित कार्य के लिए एडमिनिस्ट्रेटर अकाउंट विशेषाधिकार अथवा प्रशासनिक प्राधिकार वाले किसी अन्य अकाउंट का प्रयोग न करें।
- 29) आंतरिक सरकारी दस्तावेज स्कैन करने के लिए स्कैनर सेवा (उदाहरण कैमस्कैनर) आधारित किसी भी बाह्य मोबाइल ऐप को प्रयोग न करें।
- 30) सरकारी दस्तावेज परिवर्तित/कंप्रेस (उदाहरण : word से pdf अथवा फाइल आकार compression) करने के लिए किसी भी बाह्य वेबसाइटों अथवा cloud आधारित सेवाओं का प्रयोग न करें।
- 31) किसी भी संवेदनशील सूचना को अनधिकृत अथवा अपरिचित व्यक्ति के साथ टेलीफोन अथवा किसी माध्यम से साझा न करें।
- 32) सार्वजनिक वाई-फाई हॉटस्पॉट का प्रयोग करने से बचें।
- 33) जब भी वायरलेस अथवा ब्लूटूथ प्रयोग न किया जा रहा हो, उन्हें चालू न रखें। यह केवल तभी करें जब इसका प्रयोग करने की योजना हो और इसे केवल सुरक्षित वातावरण में ही प्रयोग करें।
- 34) इंटरनेट/इंटरनेट सेवाओं से जुड़ने के लिए एसडीडब्ल्यूएन(SDWAN) उपकरणों की उपेक्षा (बाईपास)(Bypass) न करें और किसी भी स्थल से एसडीडब्ल्यूएन(SDWAN) उपकरण की उपेक्षा (बाईपास)(ByePass) करने पर प्रशासनिक कार्रवाई की जाएगी।

## अनुपालन

अस्थायी संविदात्मक/बाह्यस्रोतन संसाधनों सहित सभी क.रा.बी.निगम/क.रा.बी.योजना कर्मचारियों को उपर्युक्त दिशानिर्देशों का सख्ती से पालन करना आवश्यक है। क्षेत्रीय प्रमुखों/ संस्था अध्यक्षों द्वारा उपर्युक्त अनुदेशों का अनुपालन सूचना प्रौद्योगिकी संसाधनों/वार्षिक रख-रखाव संविदा अभिकरण (AMC एजेंसी) की सहायता से तुरंत किया जाना है। वे अपनी नियंत्रणाधीन संस्थाओं में इन दिशा-निर्देशों के समुचित कार्यान्वयन के लिए उत्तरदायी होंगे और इन दिशा-निर्देशों के पालन न होने के कारण साइबर अटैक के किसी भी मामले को गंभीरता से लिया जाएगा और सक्षम प्राधिकारी द्वारा उचित कार्रवाई की जाएगी।

सभी क्षेत्रीय प्रमुखों/संस्था प्रमुखों द्वारा सभी उपकरणों के लिए एंटीवायरस सॉफ्टवेयर स्थापना की स्थिति सहित एक अनुपालन रिपोर्ट तुरंत प्रस्तुत की जाएगी।

यह महानिदेशक के अनुमोदन से जारी किया जा रहा है।

भवदीय  
मोना वर्मा

(डॉ. मोना वर्मा)

उप चिकित्सा आयुक्त(सू.सं.प्रौ.)





कर्मचारी राज्य बीमा निगम  
(श्रम एवं रोजगार मंत्रालय, भारत सरकार)  
Employees' State Insurance Corporation  
(Ministry of Labour & Employment, Govt. of India)



मुख्यालय/Headquarters  
पंचदीप भवन, सी. आई. जी. मार्ग, नई दिल्ली-110002  
Panchdeep Bhawan, C.I.G. Marg, New Delhi – 110002  
Website : <https://esic.nic.in> / [www.esic.in](http://www.esic.in)

सत्यमेव जयते

Computer No.E 13105  
File N 17012/1/2022-ICT  
To

Date : 13.12.2022

All Addl. Commissioner & Regional Director(s)/RDs/Deputy Director(I/c)/ SROi/c  
All Dean(s)/Medical Superintendent(s)/  
All Director(s)/ Civil Surgeon(s)/ State Directorates  
All Sub-ordinate offices through their respective Regional Offices/Sub-Regional  
Offices/ State Directorate(s)

**Subject: Cyber Security Guidelines**

Sir/Madam,

Information and communication technologies (ICT) have become ubiquitous amongst government ministries and departments across the country. The increasing adoption and use of ICT has increased the cyber-attacks and threat perception to government, due to lack of adoption of proper cyber security measures on the ground. In order to sensitize the government employees, contractual /outsourced resources and build awareness amongst them on **DO'S and DON'TS** on cyber-security perspective, these guidelines have been compiled. Strict adherence of these uniform cyber security guidelines in all ESIC/ESIS offices across the country will ensure a proper secured environment for ESIC to carry out the Scheme activities.

#### **CYBER SECURITY DO'S**

- 1) Use complex passwords with a minimum length of 10 characters, using a combination of capital letters, small letters, numbers and special characters.
- 2) Do use hard-to-guess passwords or passphrases.
- 3) Change your passwords at least once in 45 days.
- 4) Always change the password from a computer which is Virus/malware free.
- 5) Use multi-factor authentication, wherever available.
- 6) Save your data and files on the secondary drive (ex: d:\).
- 7) Maintain an offline backup of your critical data. Regular backups of important data is to be done as per standards.
- 8) Keep your Operating System and BIOS firmware updated with the latest updates/patches.
- 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) Get the machine scanned with latest patches of Anti-Virus on which you are accessing your mail and also get their OS updated with the latest patches.
- 11) Configure ESIC Proxy settings to proxy.esic.in and Port 3128
- 12) Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in your system's NTP Settings for time synchronization.



- 13) Use authorized and licensed software only and remove any key logger software, if installed/available in system.
- 14) The system/computer/laptop used in workplace must be scanned regularly for security threats and Viruses.
- 15) Ensure that proper security hardening is done on systems.
- 16) When you leave your desk temporarily, always lock/log-off from your computer session. Do lock your computer, Laptops and mobile phone when not in use. This protects data from unauthorized access and use.
- 17) When you leave office, ensure that your computer and printers are properly shutdown.
- 18) Keep your printer's software updated with the latest updates/patches.
- 19) Setup unique passcodes for shared printers.
- 20) Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centres.
- 21) Keep the GPS, Bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.
- 22) Download official Apps from official app stores of google (for android) and apple (for iOS).
- 23) Wireless communication is inherently insecure. Security protocols and selective access control must be ensured based on roles and responsibilities.
- 24) Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
- 25) 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.
- 26) Observe caution while opening any shortened uniform resource locator (URLs) (ex: [tinyurl.com/ab534/](http://tinyurl.com/ab534/)). Many malwares and phishing sites abuse URL shortener services.
- 27) 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.
- 28) Report suspicious emails or any security incident to [incident@cert-in.org.in](mailto:incident@cert-in.org.in), [incident@nic-cert.nic.in](mailto:incident@nic-cert.nic.in) and to your authority/head of division immediately.
- 29) Adhere to the security advisories published by NIC-CERT (<https://nic-cert.nic.in/advisories.jsp>) and CERT-In (<https://www.cert-in.org.in>).
- 30) Always ensure that the "REMEMBER PASSWORD" option isn't configured anywhere *i.e.* in the browser or in IMAP/POP mail client *i.e.* Outlook, Thunderbird, seamonkey, Windows Mail etc.
- 31) Every system/computer/laptop used in workplace environment must be password protected.



- 32) Two factor authentication (such as Kavach) must be used to access emails by all. Password for Mail ID must not be shared with anyone.
- 33) Educate users every week for Security related threats and how to prevent such incidences. Standard guidelines, SOPs and protocols must be circulated to all.
- 34) If system is found to be infected with any virus/malware/phishing software,
  - a) Disable IMAP service in Kavach for all users (both in desktop and mobile client).
  - b) Disconnect the infected computers from LAN/Internet immediately.
  - c) Hard disks of the infected computers may be formatted after taking backup of data files;
  - d) Operating systems and applications should be re-installed from clean and updated software;
  - e) Backup data should be scanned for virus before restoring it;
  - f) Educate colleagues and other staff about security policy and related information(s).

### **CYBER SECURITY DON'TS**

- 1) Don't use the same password in multiple services/websites/apps.
- 2) Don't share the password with anyone. The password must not be shared with others, whether you know them or not. Do keep your passwords or passphrases confidential. You are responsible for all activities associated with your credentials.
- 3) Don't save your passwords in the browser or in any unprotected documents.
- 4) Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (eg.: sticky/post-it notes, plain paper pinned or posted on your table, etc.)
- 5) Don't save your data and files on the system drive (eg.: c:\ or root).
- 6) Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (eg.: Google Drive, Dropbox, etc.).
- 7) Don't use obsolete or unsupported Operating Systems.
- 8) Don't connect official computer/laptop and any other device with private network (Mobile Hotspot)
- 9) Nobody should use any private mail ID for communications for official purposes, from official Computers, systems or Laptops. All officials must use official e Mail IDs ending with gov.in (nic.in), etc.
- 10) Don't use personal work on official systems.
- 11) Don't plug in portable devices such as pen drive, etc., without permission from ESI management. These devices may be compromised with code just waiting to launch as soon as you plug them into a computer.
- 12) Don't connect any other site (unrelated to official requirement) on official system.
- 13) Don't use any 3rd party DNS Service or NTP Service.
- 14) Don't use any 3rd party anonymization services (eg.: Nord VPN, Express VPN, Tor, Proxies, etc.).
- 15) Don't use any 3rd party toolbars (eg.: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
- 16) Don't install or use any pirated software (eg.: cracks, keygen, etc.).
- 17) Don't open any links or attachments contained in the emails sent by any unknown sender.

- 18) Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.
- 19) Don't allow internet access to the printer.
- 20) Don't allow printer to store its print history.
- 21) Don't disclose any sensitive details on social media or 3rd party messaging apps.
- 22) Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person
- 23) Don't use any unauthorized remote administration tools (eg.: TeamViewer, Ammy admin, Anydesk, etc.)
- 24) Don't use any unauthorized 3rd party video conferencing or collaboration tools for conducting sensitive internal meetings and discussions.
- 25) Don't use any external email services for official communication.
- 26) No unverified or untrusted links or websites must be accessed at any time.
- 27) Don't jailbreak or root your mobile phone.
- 28) Don't use administrator account or any other account with administrative privilege for your regular work.
- 29) Don't use any external mobile App based scanner services (eg.: CamScanner) for scanning internal government documents.
- 30) Don't use any external websites or cloud-based services for converting/compressing a government document (ex: word to pdf or file size compression)
- 31) Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.
- 32) Avoid using public Wi-Fi hotspots.
- 33) Don't leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment
- 34) **Don't Bye pass SDWAN Devices to connect internet/intranet services and any location bye-passing SDWAN Device would attract administrative action.**

## COMPLIANCE

All ESIC/ESIS employees, including temporary, contractual/outsourced resources are required to strictly adhere the guidelines mentioned above. The above instructions are to be complied with the help of IT Resources / AMC Agency by the Regional Heads/Institution Heads immediately. They shall be responsible for proper implementation of these guidelines in the institutions under their control and any cases of cyber-attacks due to non-adherence of these guidelines shall be viewed seriously and suitable action will be taken by the competent authority.

A compliance report along with status on antivirus software installation on all devices by all Regional Heads / Institution Heads is to be submitted immediately.

This issues with the approval of the Director General

Yours Sincerely

(Dr.Mona Varma)  
Dy.Medical Commissioner(ICT)



# INFORMATION SECURITY BEST PRACTICES



## MINISTRY OF HOME AFFAIRS



## INFORMATION SECURITY BEST PRACTICES

### Table of Contents

<b>1. Introduction</b> .....	3
<b>2. General Computer Usage</b> .....	3
<b>3. General Internet Browsing</b> .....	5
<b>4. Password Management</b> .....	9
<b>5. Removable Information Storage Media</b> .....	12
<b>6. Email Communication</b> .....	15
<b>7. Home Wi-Fi Network</b> .....	16
<b>8. Avoiding Social Engineering Attacks</b> .....	17
<b>9. Glossary</b> .....	20



## **INFORMATION SECURITY BEST PRACTICES**

### **1. Introduction**

Ministry of Home Affairs, Cyber & Information Security (CIS) Division has prepared this document to disseminate Information Security best practices for the benefit of Government Officials/Officers.

This should not be considered as an exhaustive list of prescription for Information Security but basic minimum precautions to be taken. Each organization should identify additional measures for information security in accordance with their use scenarios, sensitivity of data, business continuity and other relevant factors.

### **2. General Computer Usage**

Following are some of the best practices for computer use on day to day basis:

- 2.1 All classified work should be strictly carried out only in a standalone computer which is not connected to the internet.
- 2.2 Create strong passwords for login by using a combination of letters, numbers, and special characters with minimum of 10 characters.
- 2.3 Computers should be protected from virus/worms using an Antivirus software permitted for use by your organization.
- 2.4 Make sure your operating system, application and software patches including anti-virus software are up to date; and auto updates are turned on in your computer.
- 2.5 Don't leave the computer unattended with sensitive information on the screen.

## **INFORMATION SECURITY BEST PRACTICES**

- 2.6 Always lock your computer before leaving workplace to prevent unauthorized access. A user can lock computer by pressing „ctrl +alt+del“ and choosing „lock this computer“ or “window button+ L”.
- 2.7 Enable a password-protected screen saver with a timeout period of 2 minutes to ensure that computers that were left unsecured will be protected.
- 2.8 Be careful of what you plug in to your computer. Malware can spread through infected USB drives, external hard drives, and even smart phones.
- 2.9 Use non-administrator account privileges for login to the computer and avoid accessing with administrator privileges for day-to-day usage.
- 2.10 Treat sensitive data very carefully and use encryption to securely encode sensitive information.
- 2.11 Backup your important files at regular intervals to avoid unexpected loss.
- 2.12 Remove unnecessary programs or services from computer which are not required for day to day operation.
- 2.13 Do not give remote access, file and print sharing option to other computers.
- 2.14 Do not use file sharing softwares as file sharing opens your computer to the risk of malicious files and attacks.
- 2.15 Avoid entering sensitive information onto a public computer like cyber cafe, library computers etc.,



## **INFORMATION SECURITY BEST PRACTICES**

- 2.16 If you store or download any personal information on computers in cyber café, make sure you delete permanently all the documents after you are done with your work. You may press Shift and Delete button together to make it difficult to recover deleted files.
- 2.17 Remove files or data you no longer need to prevent unauthorized access to such data. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system. File shredder software should be used to delete sensitive files on computers.
- 2.18 Ensure to use un-interrupted power supply to computers through UPS or other backup sources.
- 2.19 Do not plug the computer directly to the wall outlet as power surges may damage computer. Instead use a genuine surge protector to plug a computer.
- 2.20 The systems should be placed in a room which is dust free and has a good ventilation to avoid overheating of CPU.

### **3. General Internet Browsing**

Following are some of the best practices to keep in mind when browsing on Internet:

- 3.1. Always be careful when clicking on links or downloading. If it's unexpected or suspicious for any reason, don't click on it.
- 3.2. Do not download any type of files/software from any source other than those allowed by your system administrator/department.
- 3.3. Use web browser which has been permitted by your Organization.

## INFORMATION SECURITY BEST PRACTICES

- 3.4. Always use updated web browser for browsing. If you run a web browser that is out of date, it may contain security vulnerabilities and you risk having your computer compromised. Depending on the security exploit, your personal information (including emails, banking details, online transactions, photos and other sensitive information) could be stolen or destroyed.
- 3.5. Do not store/ share any sensitive information on any device that is connected to the Internet.
- 3.6. The "Save password" option prompted by the browser should not be selected if a window appears after entering information on the login screen, asking you to do so. Don't save account information, such as passwords or credit card information in web browsers, especially on those PCs which are shared with other users.
- 3.7. Look for HTTPS sign in the browser address bar. The "s" in "https" stands for secure, meaning that the website is employing SSL encryption. Check for an "https:" with a green padlock icon in your browser address bar to verify that a site is secure.
- 3.8. Make a habit of clearing history from the browser after each logout session. Following are the settings in various browsers to automatically clear the history on each browser session ends:

### Chrome

- Click on the menu icon in the upper right corner and select **Settings**> Show **advanced settings**...>**Privacy** and then tap the **Content settings** button.



## INFORMATION SECURITY BEST PRACTICES

- In the next window that opens, under Cookies, enable the option that says "**Keep local data only until you quit your browser.**"
- Press **Done** at the bottom of the window.

### Firefox

- Click on the menu icon in the upper right corner and select **Options**. Then in the window that opens, click on the **Privacy** tab.
- Under **History**, click the drop down menu next to "Firefox will:" and select Use **custom settings for history**.
- Check the option **Clear History when Firefox** closes.
- Once you're done click **OK**.

### Internet Explorer

- Click **settings** icon in the upper-right corner of the browser and select **Internet Options**.
- Open the **General Tab** in the window that appears.
- Under the **Browsing History** section, check the box next to "**Delete browser history on exit.**" Once you're done click **OK**.

3.9. No classified information of government can be stored on private cloud services (Google drive, Dropbox, iCloud etc.) and doing so may make you liable for penal action, in case of data leakage.

3.10. When on tour, avoid using services that require location information, unless it is necessary for discharge of office duties.

## INFORMATION SECURITY BEST PRACTICES

- 3.11. While browsing, some pop-ups may appear with option of close button. These may be fake and may actually try to install spyware when you click on it. Beware of such pop-ups and avoid clicking on it.
- 3.12. Popup blocker option should be kept **turned ON** in the browser and may be selectively allowed for trusted sites, if required. Doing so will help prevent any nuisance web ads or malware embedded in ads from appearing on screen. Following are the settings to turn on popup blocker configuration in various browsers:

### Firefox

- Select **Tools** from the Mozilla Firefox taskbar
- Select **Options** from the drop-down menu
- Select **Content** from the Options dialog box
- To enable all pop-ups, check the **Block pop-up windows** radio button
- Click **Close**

### Chrome

- Click on the **Menu**
- Click on **Settings**
- Scroll to **Privacy**, Click on **Content Settings**
- Scroll to **Pop-Ups**
- **Uncheck** Allow All Sites to show Pop-Ups



## INFORMATION SECURITY BEST PRACTICES

- Click **OK**

### Internet Explorer

- Click **Tools** menu
- Click **Internet Options**
- Click **Privacy** tab
- Under Pop-up Blocker, Check **Turn on Pop-up Blocker**
- Click **OK**

- 3.13. Remember that things on the internet are rarely free. “Free” Screensavers etc., often contain malware. So be aware of such online free offers.
- 3.14. Avoid using public computers and public Wi-Fi connections to access and carryout any financial or sensitive transactions. Accessing government email on such computers has a risk of causing information breach.
- 3.15. If your job requires you to access certain information systems in a secure way, it is advisable to use security controls such as MPLS link, VPN over internet etc., for such access.

## 4. Password Management

Unauthorized access is a major problem for anyone who uses a computer or devices such as smartphones or tablets. The consequences for victims of these break-ins can include the loss of valuable data such as classified information, personal data etc. One of the most common ways that hackers break into computers is by guessing passwords. Simple and

## **INFORMATION SECURITY BEST PRACTICES**

commonly used passwords enable intruders to easily gain access and control a computing device.

Following are some of the best practices to consider while setting up and managing a password,

- 4.1. Create strong password with a minimum length of ideally 10 characters and comprising of mix of alphabets, numbers and characters.
- 4.2. All passwords (e.g., email, computer, etc.) should be changed periodically at least once every three months.
- 4.3. Don't reuse old passwords.
- 4.4. Passwords should not be stored in readable form in computers, notebook, notice board or in any other location where unauthorized persons might discover or use them.
- 4.5. Treat passwords as sensitive information and do not share it with anyone.
- 4.6. Always use different passwords for every log-in accounts you have. Using the same password for more than one account risks multiple exposures if one site you use is hacked.
- 4.7. If your work requires you to communicate passwords, such as while sending password for an encrypted file sent as an attachment through email it must be communicated through a different channel such as over a phone call or SMS.
- 4.8. Always decline the use of the "Remember Password" feature wherever it is prompted by the applications.



## INFORMATION SECURITY BEST PRACTICES

4.9. Remember weak passwords have the following characteristics:

- The password contains less than 10 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 / Comics 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 123456, aaaaa, qwerty, asdfg, zxcvb, etc.

4.10. Some suggested way to construct a strong password are as follows,

- A secure password not only consist of letters, must also use numbers, special characters and caps. One suggested way to replace letters with numbers and special characters, so an “i” will become “!”, an “o” turns into a “0” and “s” is written as “\$”. This way, the simple term “Microsoft” changes to the substantially harder word “**MIcr0\$oft**”.
- Password length matters, the longer the password, the harder it is to crack.
- Think of a sentence and select the first letters of each word in a row will get a complex password and easy to remember as well.

## INFORMATION SECURITY BEST PRACTICES

For example, sentence like this, “My Name is Dinesh Anandan and I was born on 1 January 1986!” would produce the following password: “**MNiDAalwbo1J1986!**”. It’s long, contains numbers, special characters, caps and letters, and it’s easy to remember and won’t be in dictionary.

### 5. Removable Information Storage Media

One of today’s biggest security concern is the use of removable storage devices (USB devices such as pen drives, CD-RW, DVD-RW, Blu-ray discs, Media cards etc.,) in their networks. The amount of data that can be quickly copied to removable storage devices is increasing every day. While these devices can significantly boost productivity, they can also cause dangerously high risks in data security and control policies.

External removable portable storage devices allow users to bypass perimeter defenses, including firewalls and email server anti-malware, and potentially introduce malware into the office network. Since the malware enters the network from an internal device, it may go undetected until significant damage is caused to the network. Removable storage devices also facilitate easy pilferage of sensitive information from an organization’s premises. This information might include classified information.

Following are some of the best practices to be considered while dealing with Removable storage media:

- 5.1. Auto run/ Auto play feature must be disabled for all removable media.



## INFORMATION SECURITY BEST PRACTICES

- 5.2. The classified data should be encrypted before copying into the removable storage media designated to store classified information.
- 5.3. Classified information should be stored only on organization allocated removable storage media for work purpose.
- 5.4. The computers should be enabled with “Show hidden file and folders” option to view hidden malicious files in USB storage devices.

Steps to enable hidden file & system file view to find any unusual or hidden files in computer are as follows:

### Windows 10

- In the search box on the taskbar, type **folder**, and then select **Show hidden files and folders** from the search results.
- Under **Advanced settings**, select **Show hidden files, folders, and drives**, and then select **OK**.

### Windows 8.1

- Go to **Search**.
- Then type **folder** in the search box, then select **Folder Options** from the search results.
- Select the **View** tab.
- Under **Advanced settings**, select **Show hidden files, folders, and drives**, and then select **OK**.

### Windows 7

- Select the Start button, then select **Control Panel -> Appearance and Personalization**.

## INFORMATION SECURITY BEST PRACTICES

- Select **Folder Options**, then select the **View** tab.

- 5.5. It is advisable to scan all removable media with anti-virus software before use.
- 5.6. Removable media like USB's, CDs etc., must not be left unattended.
- 5.7. Technical controls may be implemented to restrict use of portable storage media drives outside of the Government network.
- 5.8. Removable media should not be taken out of office unless permitted by the competent authority in your office.
- 5.9. In order to minimize physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.
- 5.10. In case of damage or malfunction of device, the same should be returned to the designated authority in your office for repair/replacement. Never ever handover such devices to outsiders or other vendors for repair as it might have classified information.
- 5.11. If the USB device is no longer a functional requirement after issuance, then the same should be returned to the issuing authority.
- 5.12. The contents of removable media must be removed/erased after the official purpose has been served.

## INFORMATION SECURITY BEST PRACTICES

### 6. Email Communication

Following are some of the best practices in regards to email communication:

- 6.1. Use only Government provided email address for official communications (e.g. nicemail).
- 6.2. System administrator may deploy appropriate controls to restrict use of personal email address for any official communications.
- 6.3. Avoid downloading email attachments or clicking on suspicious links received in emails from unknown or untrusted sources.
- 6.4. Classified information be not communicated via emails. In case of emergent requirements to do so, the approval of competent authority should be obtained.
- 6.5. Avoid accessing official email accounts from public Wi-Fi connections.
- 6.6. Auto save of password for email accounts should not be enabled.
- 6.7. Logout from mail accounts after your work is done.
- 6.8. User should type the complete URL in the browser instead of clicking links received in an email.
- 6.9. Do not open / forward / reply to any suspicious e-mails.
- 6.10. Be cautious on tiny or shortened URL"s (appears like <http://tiny.cc/ba1j5y>) and don"t click on it as it may take you to a malware infected website.



## INFORMATION SECURITY BEST PRACTICES

- 6.11. Do not open attachment having extension such as EXE, DLL, VBS, SHS, PIF, SCR. Typical example., .txt.exe, .doc.exe

### **7. Home Wi-Fi Network**

With the mass explosion of Laptops, Smart Phones and Tablets, pervasive wireless connectivity is widely used an option for connecting to the Internet. Insecure wireless configuration can provide an easy open door for malicious threat actors. Government officials may use their home Wi-Fi network to do office work and in order to secure their home Wi-Fi network, following are some of the best practices:

- 7.1. Turn on WPA2 or higher encryption feature in wireless routers.
- 7.2. Change the default network device name, also known as its service set identifier or "SSID." When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. It is advisable to have SSID name which does not disclose your identity in any manner.
- 7.3. Change the network device default password. Unauthorized users may be familiar with the default passwords, so it is important to change the router device's password.
- 7.4. Consider using the Media Access Control, or "MAC," address filter in your wireless router. Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept

## **INFORMATION SECURITY BEST PRACTICES**

connections only from devices with MAC addresses that the router will recognize. To create another obstacle to unauthorized access, consider activating your wireless router's MAC address filter to include your devices only.

- 7.5. Turn off your wireless router when not needed for any extended period of time.
- 7.6. Update the firmware of wireless devices regularly as it will reduce the number of security loop holes in the device.
- 7.7. Disable remote management feature in routers to protect against unauthorized access.

### **8. Use of Social Media by Government Officers/Officials:**

All personnel including employees, contractual staff, consultants, partners, third party staff etc., who manage, operate or support information systems, facilities, communication networks; and information created, accessed, stored and processed by or on behalf of the Government of India, unless authorized to do so, shall not:

- a. Access social media on any official device (computer, mobile etc.).
- b. Disclose official information on social media or social networking portals or applications.

### **9. Avoiding Social Engineering Attacks**

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing

## INFORMATION SECURITY BEST PRACTICES

that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email. Following are some of the best practices should follow to avoid social engineering attacks:

8.1. Be careful to unsolicited phone calls, visits, or email messages from individuals asking about personal or other Government information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

8.2. **Phishing** is one of common type of social engineering scam. The hacker typically sends an email or text to the target, seeking information that might help with a more significant crime. So do not reveal personal, sensitive or financial information in email or messages, and do not respond to such emails.

For example, a hacker might send emails that appear to come from a source trusted by the victim. That source might be a bank for instance, asking email recipients to click on a link to log in to their accounts. Those who click on the link, though, are taken to a fake website that, like the email, appears to be legitimate. If they log in at that fake site, they're essentially handing over their login credentials and giving the crook access to their bank accounts.

8.3. **Vishing** is the voice version of phishing. "V" stands for voice, but otherwise, the scam attempt is the same. The hacker uses the phone to trick a victim into handing over valuable information. So don't reveal any sensitive information over phone calls.



## INFORMATION SECURITY BEST PRACTICES

For example, a hacker might call an officer, posing as a Government officer. The hacker might prevail upon the victim to provide login credentials or other information that could be used to target the Organization.

- 8.4. **Quid pro quo** scam is another type of social engineering attack that involves an exchange like I give you this, and you give me that. Hackers make the victim believe as a fair exchange, but that's far from the case, as the cheat always comes out on top.

For example, a hacker may call a target, pretending to be an IT support technician. The victim might hand over the login credentials to their computer, thinking they're receiving technical support in return. Instead, the hacker can now take control of the victim's computer, loading it with malware or, perhaps, stealing personal information from the computer to commit identity theft.

- 8.5. Be cautious of 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). In general, all government websites have gov.in or nic.in at the end of their names. For example, a malicious website may have name as [www.npagov.in](http://www.npagov.in) or [www.npa-gov.in](http://www.npa-gov.in) against the actual name [www.npa.gov.in](http://www.npa.gov.in)

- 8.6. It's safer to type a URL into your browser instead of clicking on a link. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

- 8.7. Hacker wants you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let the urgency influence your careful review.

## INFORMATION SECURITY BEST PRACTICES

- 8.8. If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam and do not respond and delete such emails.
- 8.9. Immediately change any passwords you might have revealed to anyone. 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.

## 10. Glossary

Term	Definition
DDoS	A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
Digital Signature	A digital signature is a way to ensure that an electronic document (e-mail,

## INFORMATION SECURITY BEST PRACTICES

	<p>spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.</p>
DNS	<p>The domain name system (DNS) is the way internet domain names are located and translated into internet protocol addresses.</p>
Encryption	<p>Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.</p>
GPS	<p>The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information.</p>
HTTPS	<p>Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection.</p>
IM	<p>Instant Messaging a type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet.</p>



### INFORMATION SECURITY BEST PRACTICES

IoT	Internet of Things (IoT) is an ecosystem of connected objects that are accessible through the internet.
Malware	Malware is short for malicious software and used as a single term to refer to virus, spy ware, worm etc.
SMS	SMS is a text messaging service component of most telephone, internet, and mobile-device systems.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network attached devices for conditions that warrant administrative attention.
SSH	Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two computers.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LAN to which a client wants to attach.
Trojan	A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike

### INFORMATION SECURITY BEST PRACTICES

	viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.
URL	A Uniform Resource Locator (URL), colloquially termed a web address is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.
USB	A Universal Serial Bus (USB) is a common interface that enables communication between devices and a host controller such as a personal computer.
Virus	Virus is a program written to enter to your computer and damage/alter your files/data and replicate themselves.
VPN	A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
Wi-Fi	Wi-Fi certified is a program for testing

## INFORMATION SECURITY BEST PRACTICES

Certified	products to the 802.11 industry standards for interoperability, security, easy installation, and reliability.
Worms	Worms are malicious programs that make copies of themselves again and again on the local drive, network shares, etc.

### NOTE:

- In case of any doubt, *National Information Security Policy & Guidelines* (NISPG) issued by Ministry of Home Affairs may be referred to.
- Due care has been taken while preparing this booklet. If any suggestion for improvement(s) is felt, same may be shared at [cyberdost@mha.gov.in](mailto:cyberdost@mha.gov.in).

(version 1.0)