No. 18-59/2021-CERT-T
Department of Telecommunications
(Security Assurance – II Wing)

R. No. 1417, Sanchar Bhawan, New Delhi
Dated: 05.05.2021
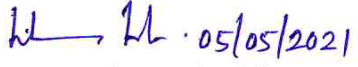
Office Memorandum

Subject: Information Security Best Practices.

The undersigned is directed to enclose a copy of Information Security Best Practices prepared by Department of Telecommunications and to be followed by the officials under the control of DoT and its PSUs.

2.   This is for kind information and necessary action.

Enclosure: As above.

(signature) · 05/05/2021

(Jitendra Kumar Joshi)
Director (CERT-T)
Tel: 011-23725122

To,

1. DG (Telecom) / CGCA.
2. Administrator, USOF/ Sr. DDG, TEC/ Sr. DDG, NTIPRIT/ Sr. DDG, NCCS/ DG, NICF/ Sr. DDG (BW)/ Wireless Advisor.
3. CVO/ DDG (AS)/ DDG (DS)/ DDG (CS)/ DDG(IR)/ DDG(SA)/ DDG (SPPI)/ DDG (Satellite)/ DDG (Pers.)/ DDG (NT)/ DDG (Estt.)/ DDG (Training)/ DDG (Skill Development)/ DDG (PG)/ DDG (PHP)/ DDG (SU)/ DDG (SR)/ DDG (FIPP)/ DDG (LFA)/ JS(T)/ JS(A)/ DDG (C&A)/ DDG (BB)/ JA (Fin.)/ JA (Tech.).
4. CMD, BSNL/ CMD, MTNL/ CMD, TCIL/ ED, C-DOT.
5. Heads of all field offices of DoT.

Copy to:
1. PSO to Secretary (T)
2. Sr. PPS/ PPS to Member (S), Member (T), Member (F)
3. Sr. PPS/ PPS to Additional Secretary (T)
4. Sr. PPS/ PPS to Advisor (O), Advisor (T), Advisor (F)
5. DDG (IT), with request to upload the O.M. on the Department's website in "What's new" and also in "Circulars" sub-head "Security".

INFORMATION SECURITY BEST PRACTICES

Department of Telecommunications
(Security Assurance Wing)

Table of Contents:

1. Introduction:

Department of Telecommunications, Security Assurance Wing has prepared this document to disseminate Information Security Best Practices for the benefit of Officials/Officers working in DoT and the PSUs associated.

This should not be considered as an exhaustive list of prescription for Information Security but basic minimum precautions to be taken. Each organization may 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 strictly be carried out only in a standalone computer which is not connected to internet.

2.2   Computers should be protected from virus/ worms using Antivirus software permitted for use by the organization.

2.3   Make sure that operating system, application and software patches including anti-virus software are up to date; and auto updates are turned on in computer. Use of outdated operating system, application, software and anti-virus shall be avoided.

2.4 Don't leave the computer unattended.

2.5 Always lock the computer before leaving workplace to prevent unauthorized access. The computer can be locked by pressing 'ctrl + alt + del' and choosing 'lock this computer' or 'window button+ L'.

2.6 Enable password-protected screen saver with a timeout period of 5 minutes to ensure that computers that were left unsecured can be protected.

2.7 Be careful of what is plugged into the computer. Malware can spread through infected USB drives, external hard drives, and even smart phones.

2.8 Use non-administrator account privileges for login to the computer and avoid accessing the computer with administrator privileges for day-to-day usage.

2.9 Treat sensitive data very carefully and use encryption to securely encode sensitive information.

2.10 Backup important files at regular intervals to avoid unexpected loss.

2.11 Remove unnecessary programs or services from computer which are not required for day to day operation.

2.12   Do not give remote access, file and print sharing option to other computers. Remote access or screen sharing options shall be disabled.

2.13   Do not use file sharing software such as torrents etc. as file sharing opens computer to the risks of malicious files and attacks.

2.14   Avoid entering sensitive information onto a public computer like cyber cafe, library computers etc.

2.15   After storing or downloading any personal information on computers in cyber café or library computers, make sure to delete all the documents permanently before leaving the computer. By pressing Shift and Delete button together may delete documents. This makes it difficult to recover deleted files.

2.16   Remove files or data that is no longer needed to prevent unauthorized access to such data. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from system. File shredder software should be used to delete sensitive files on computers.

3. General Internet Browsing:

Following precautions are to be taken while browsing on Internet:

3.1 Always be careful when clicking on links or downloading. If it is 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 system administrator/ department.

3.3 Always use updated web browser for browsing internet. Running an outdated web browser may contain security vulnerabilities and risk of computer getting compromised increases.

3.4 Do not store/share any sensitive information on any device that is connected to the Internet.

3.5 The "Save password" option prompted by the browser should not be selected if a pop-up window appears after entering information on the login screen. Don't save account information, such as passwords or credit card information in web browsers.

3.6 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 browser address bar to verify that a site is secure.

3.7 Use web browser which has been permitted by Organization.

3.8 Make a habit of clearing history from the browser after each session. Following are the settings in various browsers to automatically clear the history at the end of browser session:

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.

- In the next window that opens, under Cookies, enable the option that says "**Keep local data only until quitting the 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.

- 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." Click **OK**.

Microsoft Edge

- Select Setting from menu at upper right corner.

- Open Privacy, Search, and Services from left menu.

- Click on Choose what to clear every time you close the browser

- Enable all options on next page.

3.9   No classified information of government can be stored on private cloud services (Google drive, Dropbox, iCloud etc.,) and one can be 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.

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 clicking 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 prevent any nuisance web ads or malware embedded in ads from appearing on screen.

Following are the setting to turn on popup blocker configure 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

- 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 please 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 transaction. Accessing government email on such computers has a high risk of causing information breach.

3.15 If it is required 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 device such as smartphone or tablet or computer. The consequences for victims of these unauthorized 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 commonly used passwords enable intruders to easily gain access and control a device. Following practices may be considered while setting up and managing a password,

4.1   Create strong password with a minimum length of ideally 10 characters and comprising of combination of alphabets (both lower case and upper case), numbers and special characters.

4.2   All passwords (e.g., email, computer, etc. passwords) should be changed periodically at least once every three months. Don't reuse old passwords.

4.3   Passwords should not be stored in readable form in computers, notebook, and notice board or in any other location where unauthorized persons might discover or use them.

4.4   Treat passwords as sensitive information and do not share them with anyone.

4.5   Always use different passwords for every log-in account. Using same password for more than one account risks multiple exposures if one of the passwords is hacked.

4.6   If it is necessary to communicate passwords, such as password for a password protected file which are sent as an attachment through email. Such passwords should be communicated through a different channel such as phone call or SMS.

4.7   Always decline the use of the "Remember Password" feature wherever it is prompted by the applications.

4.8   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.

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

- A secure password not only consist of letters, it must also use numbers, special characters and caps. One suggested way to replace letters with numbers and special characters, so an "e" will become "€", an "o" turns into a "0" and "t" is written as "+". This way, the simple term "Network" changes to the substantially harder word "**N€+w0rk**".

- Password length matters, the longer the password, the harder it is to crack.

- Think of a sentence, and selecting the first letters of each word of that sentence in a row will get a complex password and easy to remember as well.

  For example, sentence like this, "This 20 page long document contains best practices for information security!" would produce the following password: "**T20pldcbpfis!**" It is long, contains numbers, special characters, caps and letters, and it is 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 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 defences, 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 practices may be considered while dealing with Removable storage media:

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

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.

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, if they contain official information.

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.

5.9 In order to minimize physical risk, loss, theft or data 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 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.

6. Email Communication:

Following practices may be considered in regards to email communication:

6.1 Use only Government provided email address for official communications (e.g. NIC email).

6.2 Designation based email address with "nic.in" or "gov.in" domain shall be used for official purposes instead of personal name based email in order to avoid official communications getting stored in personal email. This will also enhance security of official information.

6.3 While relieving from the post, the official email account shall be handed over to the successor or surrendered.

6.4 System administrator may deploy appropriate controls to restrict use of personal email address for any official communications.

6.5 Avoid downloading email attachments or clicking on suspicious links received in emails from unknown or untrusted sources.

6.6 Classified information shall not be communicated via emails. In case of emergent requirements to do so, the approval of competent authority should be obtained.

6.7 Avoid accessing official email accounts from public Wi-Fi connections.

6.8 Auto save of password for email accounts should not be enabled.

6.9 Logout from mail accounts after work is done.

6.10 User should type the complete URL in the browser instead of clicking links received in an email.

6.11 Do not open / forward / reply to any suspicious e-mails.

6.12 Be cautious on tiny or shortened URL's (appears like http://tiny.cc/ba1j5yyyy etc.) and don't click on it as it may take to a malware infected website.

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

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

7.5   Turn off 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 Govt. 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:

8.1   Access social media on any official device (computer, mobile etc.).

8.2   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 that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email. Following practices may be considered to avoid social engineering attacks:

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

9.2 Avoid sharing of OTPs/ passwords/ card number or other vital information to anyone. Sharing such information may cause serious implications, i.e. financial fraud, personal data theft etc.

9.3 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 them to carry out more significant crime. Therefore, 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 to that fake site, they're essentially handing over their login credentials and giving the crook access to their bank accounts.

9.4 **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.

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.

9.5 **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.

9.6 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 or

www.npa-gov.in against the actual name www.npa.gov.in.

9.7   It is safer to type a URL into 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 wrong click on it.

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

9.9   If an email is received 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.

9.10 Immediately change any passwords those might have revealed to anyone. If same passwords are used for multiple resources, make sure to change it for each account, and do not use that password in the future.

10. Digital Signature:

A digital signature is a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic.

Authentic means that the creator of the document is known and it has not been altered in any way since that person created it. While handling official communications online following practices may be considered:

10.1 Files should be signed digitally. The digital signature should be validated by user itself.

10.2 Digital signature should not be saved on computer. Rather, it should be stored in removable flash drive.

10.3 The digital signature flash drive or password should not be shared with anyone.

10.4 Don't attempt wrong password for digital signature otherwise same may get blocked after certain numbers of wrong attempts.

10.5 Be aware of the expiration date of your electronic/ digital certificate.

11. Glossary Terms:

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, spreadsheet, text file, etc.) is authentic. Authentic means that the creator of the document is known and it has not been altered in any way since that person created it.
DNS	The domain name system (DNS) is the way internet domain names are located and translated into internet protocol addresses.
Encryption	Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.

GPS	The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information.
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection.
IM	Instant Messaging is a type of communications service that enables to create a kind of private chat room with another individual in order to communicate in real time over the Internet.
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 viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to a computer which gives malicious users/programs access the 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 the computer and damage/alter 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 Certified	Wi-Fi certified is a program for testing 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.

- Due care has been taken while preparing this booklet. If any suggestion for improvement(s) is felt, same may be shared at dircert-dot@gov.in.