# Cyber Security Guidelines for
# GOVERNMENT EMPLOYEES

CYBER SAFE BENGAL

*Presented by:*

## Cyber Security Centre of Excellence

Dept. of IT & Electronics | Government of West Bengal

https://cscoe.itewb.gov.in/

# PREFACE

In today's world, data is fuel that runs the world. Without data, decision making will get reduced to intelligent guess work. Hence, there is a tendency on the part of every application to collect as much user data as possible with ostensible purpose to improve the experience of the user.

However, this tendency to collect data has raised serious privacy concerns and in many cases have resulted in irreparable loss to users. Hence, understanding the role as a user what to share and what not to share; also, at the same time, understanding as government organization/employee how much data to collect, how to keep the collected data securely and who to allow use of this collected data are the natural questions which need elaborate and detailed explanations.

This document is a small yet decisive step in that direction which expands various advisories of Government of India published exclusively for government employees in a lucid manner and with examples so that the same can be easily understood and effectively implemented.

Cyber Security Centre of Excellence (CS-CoE) under this Department has been imparting On the Job Training (OJT) to Government employees across the State which especially targets to improve employee–understanding of cyber-security, data-privacy and information-security issues. Portal of the CS-CoE at https://cscoe.itewb.gov.in can be accessed for multifarious offerings on cyber-security.

I sincerely wish that every employee will be immensely benefitted by this handbook brought out under the active guidance of Shri Sanjay Kumar Das, Member-Secretary of the CS-CoE.

Sd/- (Rajeev Kumar)
Principal Secretary, IT&E Dept &
Chairman, CS-CoE Empowered Committee, West Bengal.

# DOs AND DON'Ts FOR GOVERNMENT EMPLOYEES

IT resources form the backbone of countless critical operations in a country's infrastructure, and given their interconnectedness, disruptions can have a cascading effect across sectors. An information technology failure at a power grid can lead to prolonged outages crippling other sectors like healthcare, banking services.

Critical Information Infrastructure (CII) means the IT resources that are essential for the smooth functioning of a country. The National Critical Information Infrastructure Protection Centre (NCIIPC) is the nodal agency for taking all measures to protect the nation's critical information infrastructure. It is mandated to guard CIIs from "unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction".

Government data means all data / information, document, media, or machine readable material regardless of its physical form, storage media or characteristics, that is created, collected, received, obtained, maintained, or disseminated by any Government entity in the course of official Government business.

**Ministry of Electronics & Information Technology (MeitY) has released Cyber Security Guidelines for Government Employees on 10th June 2022. All government employees, including temporary, contractual/outsourced resources are required to strictly adhere to the guidelines.**

All employees, contractual staff, consultants, partners, third party staff etc. working in Government offices or on Government projects must be cautious and careful to protect public data held by Govt organisations, ensure securing public ICT infrastructure and strictly abide by the security best practices.

## CYBER SECURITY DOs

### MeitY TIP 1

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

WB CS-CoE Explanation

- Include nonsensical unusual words only you would know.
- Use Passphrase Rather Than a Password.
- Avoid common patterns such as abc123, 12345678, 777, etc.
- Avoid easy-to-guess passwords such as nick names of self, friends, family members, pets, favourite player, birthday of anyone, birth year, etc.

## MeitY TIP 2

Change your passwords at least once in 45 days.

WB CS-CoE Explanation

- Don't reuse old passwords. Re-used passwords are easier to crack.
- Never disclose any password with anyone. Also, never disclose the style of your password (viz. **<name of your locality><special character><alpha numeric>** etc.). Because the styles are archived and used by password predicting applications.
- Change your password immediately if you suspect that it has been compromised.

## MeitY TIP 3

Use multi-factor authentication, wherever available.

WB CS-CoE Explanation

- Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) adds an extra layer of security. On top of your username and password, 2FA requires another piece of information to verify your login credential. When you have 2FA enabled, the site will text you a code (OTP) to enter after your password. The stolen password cannot be reused on its own unless supported by other factor. Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentication for account logins. When you activate MFA; the application would make you take image verification test, putting captcha, conforming code sent to other connected devices etc.

## MeitY TIP 4

Save your data and files on the secondary drive (d:\).

WB CS-CoE Explanation

- Keeping the C drive empty gives better performance.
- C drive stores the operating system (OS) and if the OS becomes corrupted, it would be more difficult to reinstall Windows without losing your data.
- As the recovery storage for the computer, it will help you get back your data in case anything goes wrong with your computer.

## MeitY TIP 5

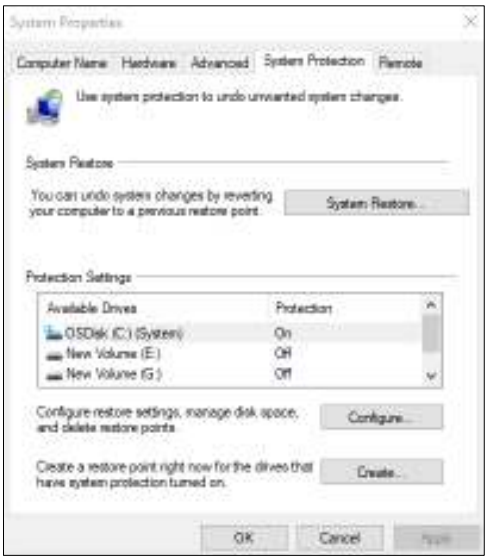
Maintain an offline backup of your critical data.

WB CS-CoE Explanation

An incident cannot affect all backups simultaneously. Keeping an offline backup is beneficial for easy recovery of data in case of any ransomware attack.

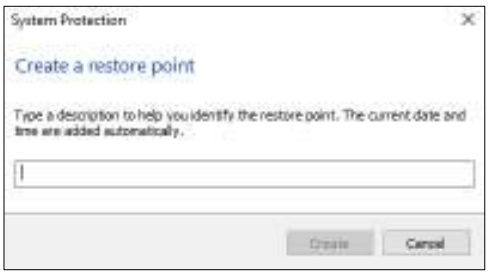
**Backup (External)** – makes a spare copy of data or a disk on an external storage device.

**Restore Point (Internal)** – is a backup copy of important Windows operating system (OS) files and settings that can be used to recover the system to an earlier point of time in the event of system failure or instability.




Create a system restore point:

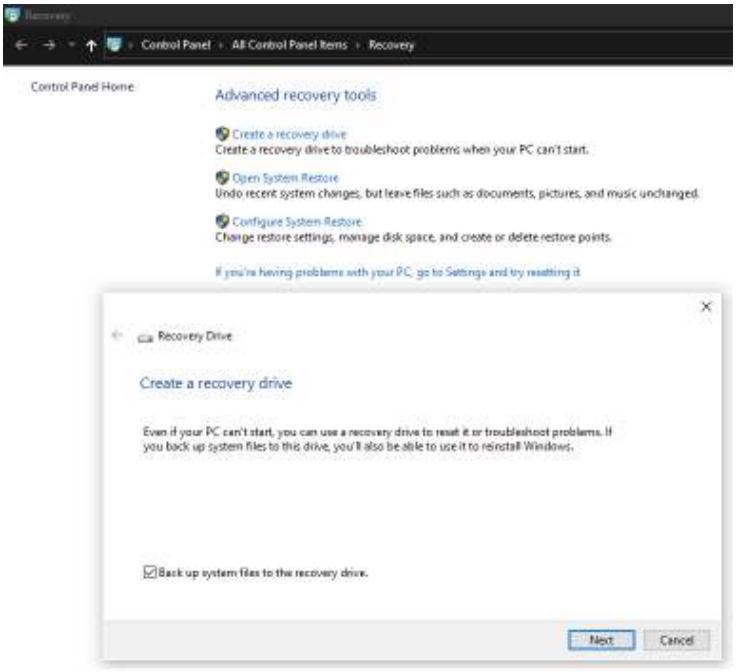
- In the search box on the taskbar, type Create a restore point, and select it from the list of results.
- On the System Protection tab in System Properties, select Create.
- Type a description for the restore point, and then select Create > OK.




**Recovery Drive (External)** – A Recovery Drive lets you boot your system and easily access a number of recovery and troubleshooting tools to revive a failing Windows system.

To create a recovery drive in Windows:

- In the search box on the taskbar, search for Create a recovery drive and then select it. You might be asked to enter an admin password or confirm your choice.
- When the tool opens, make sure Back up system files to the recovery drive is selected and then select Next.
- Connect a USB drive to your PC, select it, and then select Next.
- Select Create. Many files need to be copied to the recovery drive, so this might take a while.




Recovery drive isn't a system image. It doesn't contain your personal files, settings, or programs.

## MeitY TIP 6

Keep your Operating System and BIOS firmware updated with the latest updates/patches.

WB CS-CoE Explanation

As and when software manufacturer find bugs in their software and OS, they also fix them by releasing regular updates which patch and mitigate vulnerabilities. Run software and app updates as soon as they're available. Keeping IT systems up-to-date helps protect organizational assets.

- Update spam filters with latest spam mail contents. These filters use a number of techniques to classify phishing emails, and reject email with forged addresses.
- Do Consistently Update and Patch Your Network Devices.
- Ensure that regular cyber-security knowledge updates are received by all employees.
- Check popular update listing sites and digital magazines

## MeitY TIP 7

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.

WB CS-CoE Explanation

- Always use device specific licensed Anti-virus and run virus scan on regular basis.
- Never go for installing free Anti-virus software available in the internet.
- Always scan all removable media with antivirus
- Keep the anti-virus software updated.

## MeitY TIP 8

Configure NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) in your system's DNS Settings.

## MeitY TIP 9

Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in your system's NTP Settings for time synchronization.

## MeitY TIP 10

Use authorized and licensed software only.

WB CS-CoE Explanation

- Always use genuine software and operating system.
- Do not download and install pirated software from random sites from the Internet. Many of them are malware ridden.

## MeitY TIP 11

Ensure that proper security hardening is done on the systems.

## MeitY TIP 12

When you leave your desk temporarily, always lock/log-off from your computer session.

WB CS-CoE Explanation

- Don't leave computer unattended with sensitive information on screen. Make sure to always lock your computer screen with "windows + L" or "Ctrl+Alt+Del"
- A good idea to use Screensavers with timeout period of maximum 5 minutes.
- You can send the PC to sleep mode automatically after certain time it is left idle.

## MeitY TIP 13

When you leave office, ensure that your computer and printers are properly shutdown.

## MeitY TIP 14

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

## MeitY TIP 15

Setup unique passcodes for shared printers.

## MeitY TIP 16

Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centres.

## MeitY TIP 17

Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.

WB CS-CoE Explanation

- Use Bluetooth in "hidden" mode rather than "discoverable" mode. This prevents other unknown devices from finding your Bluetooth connection.
- Always keep your Bluetooth off when not in use.
- Turn off NFC (Near Field Communication) if you are not using it. NFC is a short-range wireless technology that allows the exchange of data between devices.
- Always keep your mobile data and location off when they are not required.

## MeitY TIP 18

Download Apps from official app stores of google (for android) and apple (for iOS).

WB CS-CoE Explanation

- Do not download any App from an untrusted sources/link.
- Do not install and keep Any App or software which you do not require regularly.
- Do not give unnecessary permissions to apps that you install on your smart phones.
- The government Department/private Developers can host mobile applications, which is related to delivering/providing government and other public services in the Mobile Seva AppStore, available at https://apps.mgov.gov.in. Users can download applications from Mobile Seva AppStore for accessing various government/public services anytime from anywhere.

## MeitY TIP 19

Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user base, etc.

## MeitY TIP 20

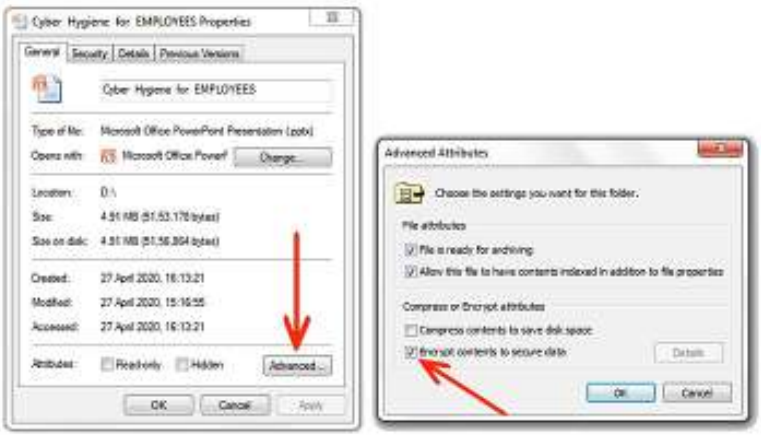
Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.

## MeitY TIP 21

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.

WB CS-CoE Explanation

- Encryption is the process of converting the information into a form where an unauthorized party cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form.

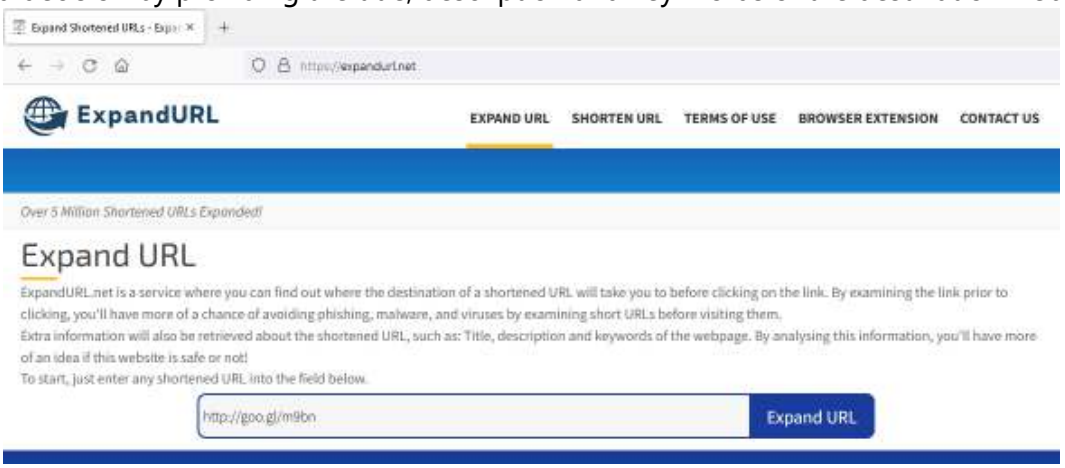



## MeitY TIP 22

Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.

WB CS-CoE Explanation

- Verify shortened URL. Never click on a link without knowing where the link will finally redirect you. Rather use shortened URL expander websites www.expandurl.net. The website helps users in taking an informed decision by providing the title, description and key-words of the destination web page.




## MeitY TIP 23

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.

WB CS-CoE Explanation

- Never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Beware of clicking on phishing URLs providing special offers like big discounts, winning prize, rewards, cash-back offers or ask you to fill up customer review form. Lucrative offers and eye-catching statements are often used to attract people's focus.

## MeitY TIP 24

Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in.

## MeitY TIP 25

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).

# Cyber Security Centre of Excellence

## West Bengal

### Department of Information Technology & Electronics
### Government of West Bengal

# CYBER SECURITY DON'Ts

## MeitY TIP 1

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

WB CS-CoE Explanation

- Using the same password for all your online accounts is like using the same key for all your locked doors. Don't use the same password for multiple accounts. Even if one password gets hacked, your other accounts will not be compromised.
- Since each account having a unique password, there will be a lot of passwords to remember. The best solution is to use a password manager. A password manager stores and encrypts all of your different and complex passwords and help you to log into your online accounts automatically. You only need to remember your master password to access the password manager.

## MeitY TIP 2

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


WB CS-CoE Explanation

- Never select the "Save password" option prompted by your web browser. There are many websites that prompts you to save your login credentials or payment detail for future use. Decline to them.

## MeitY TIP 3

Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)

WB CS-CoE Explanation

- Don't store the passwords in readable form in computers, notebook, notice board etc.
- Don't keep files open containing personal or confidential information on your desks.

## MeitY TIP 4

Don't save your data and files on the system drive (Ex: c:\ or root).

## MeitY TIP 5

Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: google drive, dropbox, etc.).

**MeitY TIP 6**

Don't use obsolete or unsupported Operating Systems.

**MeitY TIP 7**

Don't use any 3rd party DNS Service or NTP Service.

**MeitY TIP 8**

Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).

**MeitY TIP 9**

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

**MeitY TIP 10**

Don't install or use any pirated software (ex: cracks, keygen, etc.).

**MeitY TIP 11**

Don't open any links or attachments contained in the emails sent by any unknown sender.

WB CS-CoE Explanation

Criminals also send fraudulent emails containing malicious links and attachments, pretending to be from a legitimate sender and with a valid important reason.

- Never click on a URL (or download files) contained in an unsolicited e-mail from unknown people even if the link seems benign.
- Check the integrity of URLs before providing login credentials or clicking a link.
- If you see an attachment that doesn't make sense, be cautious. Attachments may contain viruses including ransomware.
- Don't allow your e-mail programs to "auto open" attachments.

**MeitY TIP 12**

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

**MeitY TIP 13**

Don't allow internet access to the printer.

**MeitY TIP 14**

Don't allow printer to store its print history.

## MeitY TIP 15

Don't disclose any sensitive details on social media or 3rd party messaging apps.

WB CS-CoE Explanation

- Avoid disclosing/ sharing any official information on untrusted phone calls, meetings or email messages. Attackers often pose as genuine people to gain confidential official information to cause a data breach.
- Don't share virtual meeting URLs, or screenshots from your video calls on the social media. You may accidentally be leaking information (meeting ID or other confidential information).

## MeitY TIP 16

Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person

WB CS-CoE Explanation

- Store information only on organization allocated removable storage media.
- Always scan all removable media with antivirus
- Erase/remove the contents of removable storage media after use.

## MeitY TIP 17

Don't use any unauthorized remote administration tools (ex: Teamviewer, Ammy admin, anydesk, etc.)

## MeitY TIP 18

Don't use any unauthorized 3rd party video conferencing or collaboration tools for conducting sensitive internal meetings and discussions.

WB CS-CoE Explanation

- For video chatting, it is always better to use Web clients inside of your browser. If you have to download and install any software, make sure that you are downloading from a legitimate website. Criminals often spoof websites and stack them with malware, which may spy into your work.
- Note that many of the well-known video-chatting services are not end-to-end encrypted. Do not share any password or authentication details over it. There is a chance that attackers can access that information.
- If you are not in a meeting, make sure that your webcam is either taped or blocked.
- The microphone should always be mute. In times when private topics may be discussed, having the microphone on mute will help prevent any leaks or unnecessary sharing of embarrassing information.

## MeitY TIP 19

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

## MeitY TIP 20

Don't jailbreak or root your mobile phone.

## MeitY TIP 21

Don't use administrator account or any other account with administrative privilege for your regular work.

## MeitY TIP 22

Don't use any external mobile App based scanner services (ex: Camscanner) for scanning internal government documents.

WB CS-CoE Explanation

- Use **SelfScan**, an android-based mobile scanning App developed entirely in-house by the Dept. of IT&E, Govt. of West Bengal.
- As a design principle, no user data is collected. Data stays with the user.
- Seeks no permission. No storing of data in any server
- An absolutely free app with no registration
- Absolutely free from advertisement. No Cookies!
- No spoofing! No phishing! No third-party interference!

## MeitY TIP 23

Don't use any external websites or cloud-based services for converting/compressing a government document (ex: word to pdf or file size compression)

## MeitY TIP 24

Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.

WB CS-CoE Explanation

- Avoid vishing attacks – do not reveal any sensitive information over phone calls unless the source is completely verified and trusted.
- Ask for some information / verifiable credential, such as the name of immediate senior (if the caller poses as an official of another Government Department).
- Try to get a full assurance as to the identity of the caller prior to disclosing any vital information.

**Released by: Cyber Security Centre of Excellence | Govt. of West Bengal**
**Released on: 15 July 2022**

# Cyber Security Centre of Excellence

Department of IT & Electronics | Govt. of West Bengal

*Helping to make your cyber presence safe*


Webel Bhavan, Ground Floor
Block – EP & GP, Sector – V
Salt Lake
Kolkata – 700 091

Phone No: 033 2357 5218
WhatsApp: +91 90075 61725
Email: cscoe[at]wb[dot]gov[dot]in
Web: https://cscoe.itewb.gov.in