



**DIRECTORATE OF EDUCATION**  
(Govt. of National Capital Territory of Delhi)  
IT-Branch, Old Patrachar Vidyalaya Complex, Delhi-110054

F. No. DE/IT/MISC/2015/Part File/ 295

Dated: 02/09/2024

**CIRCULAR- CYBER SECURITY GUIDELINES(Do's/Don'ts)-for Employees**

Cyber security is crucial for protecting sensitive information and maintaining public trust. With the rise of ICT adoption, the threat landscape for government agencies has expanded, often due to inadequate Cyber security practices. Cyber security issues affect everyone and frequently arise from individual-level ignorance or unhealthy practices. To address this, time to time government agencies have issued essential cyber security guidelines for officials. Therefore, the following Do's and Don'ts have been compiled to guide departmental users. All government officials and officers are advised to adhere strictly to these points.

**Do's:**

- Use strong, unique passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters for all accounts related to electoral management systems, including email and online portals.
- Enable user authentication wherever possible to add an extra layer of security to your accounts.
- Change your passwords at least once in 45 days
- Regularly allow update software request service and security patches on all devices to protect against known vulnerabilities.
- Exercise caution when accessing sensitive information or clicking on links in emails, especially those from unknown or suspicious sources.
- Encrypt sensitive data, both in transit and at rest, to prevent unauthorized access or interception.
- Securely store physical documents containing sensitive information in locked cabinets or safes when not in use.
- Report any suspicious activities or security incidents to the designated authority immediately for prompt investigation and mitigation.
- Keep your Operating System updated with the latest updates/patches.
- Install enterprise antivirus client offered by the government on your official desktops/laptops. You may use any of the following Bot Removal Tool for your digital device as suggested by CERT-In link: <https://www.csk.gov.in/security-tools.html>
- When you leave your desk temporarily, always lock/log-off from your computer session.
- Download Apps from official app stores of google (for android) and apple (for iOS).
- Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
- 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.
- Machines containing sensitive data should be disconnected from the internet.
- Be cautious of suspicious numbers that don't resemble real mobile phone numbers. Scammers often use email-to-text services to mask their identity and avoid revealing their actual phone number. Genuine SMS messages from banks usually contain a sender ID.
- Exercise caution with shortened URLs, such as those involving bit.ly and tinyurl.
- Ensure that websites have valid encryption certificates by checking for the green lock in the browser's address bar before providing any sensitive information.
- Avoid applications that claim to be 'memory cleaners' or 'battery optimizers.'
- Report suspicious/phishing emails or any security incident to [incident@cert-in.org.in](mailto:incident@cert-in.org.in), [incident@cert.org.in](mailto:incident@cert.org.in) and [incident@nic-cert.nic.in](mailto:incident@nic-cert.nic.in).

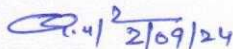
**Don'ts:**

- Don't share passwords or login credentials with anyone, including colleagues or external parties, without proper authorization.
- Don't use public or unsecured Wi-Fi networks to access electoral systems or transmit sensitive data, as these networks may be vulnerable to interception.

- Don't respond to unsolicited emails or messages requesting personal information or login credentials, as these may be phishing attempts aimed at stealing sensitive data.
- Don't install unauthorized software or applications on devices used for electoral purposes, as these may introduce security risks or malware.
- Don't leave electronic devices unattended or unlocked in public places, as this may facilitate unauthorized access or theft of sensitive information.
- Don't ignore security alerts or warnings on devices or systems used for electoral purposes, as these may indicate potential security threats or vulnerabilities.
- Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person.
- Don't use any unauthorized remote administration tools (ex: Teamviewer, Ammy admin, anydesk, etc.)
- Don't use any external mobile App based scanner services (ex: Camscanner) for scanning internal government documents.
- Don't use any external websites or cloud-based services for converting/compressing a government document (ex: word to pdf or file size compression)
- Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.
- Don't install or use any pirated software (ex: cracks, keygen, etc.).
- Don't open any links or attachments contained in the emails sent by any unknown sender.
- Don't allow internet access to the printer.
- Don't write down any password, IP addresses or any sensitive information on any unsecured material (ex: sticky/post-it notes. Plain paper pinned or pasted on user table etc.)
- Don't Publish or post or share any unverified information through social media.
- Don't click on links in SMS received from unverified sources.

All government employees, including temporary and outsourced resources, are strongly urged to prioritize cyber security in all their work areas and activities and remain vigilant against emerging threats. The employees may also check guidelines in r/o cyber security issued time to time from the Govt. websites of CERT-In/Miety

This issue in consultation with the Assistant Chief Information Security Officer (ACISO), DoE, and with the prior approval of the Competent Authority.

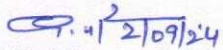
  
 (Raj Kumar Joshi)  
 System Analyst (IT),  
 Directorate of Education, GNCTD

F. No. DE/IT/MISC/2015/Part File/295

Dated: 02/09/2024

Copy to:

1. P.S. to Secretary (Education), Department of Education, Old Secretariat, GNCTD
2. P.A. to Director (Education), Directorate of Education, Old Secretariat, GNCTD
3. Assistant Chief Information Security Officer (ACISO)/JD (IT), DoE, GNCTD.
4. The Chief Information Security Officer (CISO), Department of IT, GNCTD
5. All Branch In-charges, DoE, GNCTD
6. All Govt. officials/officers and outsourced employees of DoE- through website circulation.
7. Website In-charge (EduDel, DoE) for uploading the guidelines on the DoE website.
8. Guard File.

  
 (Raj Kumar Joshi)  
 System Analyst (IT),  
 Directorate of Education, GNCTD