



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/ **353-360**

Dated: **01/10/24**

CIRCULAR

Subject: Adherence to Cyber Security Protocols and Use of Government/NIC Email IDs

In reference to this office circular no. DE/IT/MISC/2015/Part File/295 dated 02/09/2024 regarding Do's & Don'ts, this is to reiterate the importance of adhering to Cyber Security protocols. Cyber Security is a critical concern for the Government, and all departments are urged to prioritize this area. To mitigate risks and avoid cyber incidents, the following guidelines must be followed, and all are requested to take immediate measures to enhance cyber security preparedness:

- 1. Adherence to Do's & Don'ts:** All employees are required to follow the Cyber Security guidelines outlined in the CIRCULAR-CYBER SECURITY GUIDELINES (Do's/Don'ts) FOR EMPLOYEES dated 02/09/2024, which has been previously circulated and placed on the department's website for ready reference.
- 2. Use of Government/NIC Email IDs:** The Office of the Chief Information Security Officer (CISO)/Department of IT, GNCTD, vide circular dated 06/09/2024, has reiterated the Cyber Security Dos & Don'ts as per Annexure A and B issued vide their earlier circular dated 30/10/2023 & 05/10/2023 (copy enclosed). The circular mandates the use of Government/NIC email IDs for official communications. Further, each department/branch is requested to display prominently Banners on Cyber Security (Dos & Don'ts) at locations with high visibility. Additionally, all official communication within the Government must be conducted using Government or NIC email IDs. The use of third-party email services for official purposes is strictly prohibited.

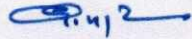
In pursuit of this:

- All branches and officials/officers of DoE must ensure full compliance with these guidelines and use Government/NIC email IDs for any official communication within the Government. Individual officials/officers identified for official communication within the Government must create their Government/NIC email IDs through <https://eforms.nic.in>. All branch in-charges/HoS may coordinate/ request to the **Care Taking Branch, DoE** for making material arrangements regarding Banners display (if any).
- All RDE/DDE/Branch In-charges/HOS are requested to submit (hard copy) /attach a "Compliance Certificate" to the IT branch at email ID: doeitbranch@doe.delhi.gov.in for further submission to the Office of the Chief Information Security Officer (CISO), Delhi, confirming that all official communications within their branch are conducted using official Government email IDs. The certificate should include:

Branch Name	Banners on Cyber Security (Dos & Don'ts) hanged/pasted in Branch/School premises (Yes/No)	Official/officers of Branch are using Govt./NIC email for all official communication (Yes/No)

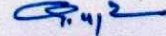
This issue in consultation with the Assistant Chief Information Security Officer (ACISO), DoE, and with the prior approval of the Competent Authority.

Encl: A/a


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

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. P.A to ADE(Admin), Directorate of Education, Old Secretariat, GNCTD
4. Assistant Chief Information Security Officer (ACISO)/JD (IT), DoE, GNCTD.
5. The Chief Information Security Officer (CISO), Department of IT, GNCTD
6. All RDEs/JDEs/DDEs/ADEs/ Branch In-charges /HOS/officers of DoE, GNCTD
7. DD (Care Taking Branch) – for making material arrangements regarding Banners on Cyber Security (Dos & Don'ts) as per the requests from the respective branches (if any).
8. Website In-charge (Edudel, DoE) for uploading the circular on the DoE website.
9. Guard File.



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

431

Government of NCT of Delhi
Department of Information Technology

9th Level, B wing Delhi Secretariat IP Estate, New Delhi

<https://it.delhi.gov.in>

E-17/2/2022/Dir(DeGS) / Computer No- 042708395 / 565-5730 dated: 06/09/2024

CIRCULAR

Subject: Use of Gov.in/Nic.in email ID for official communication.

May please refer to the this office circulars issued vide E-17/4/2022/Dir(DeGS) / Computer No- 042708413/6595-6674 dated 05.10.2023 & E-17/4/2022/Dir(DeGS) / Computer No- 042708413/7610-89 dated 30.10.2023 regarding Do's & Don'ts and MeitY Email Policy on the subject cited above (copy enclosed).

In this connection, it is to inform that Cyber and information security is a niche area and is the prime concern for the Government, hence, all departments are requested to provide attention to Cyber Security.

In pursuit of this, all departments must ensure the adoption of Do's & Don'ts to avoid any cyber-incident within the Government. Further, it is also mandatory for all departments to use Government/NIC email ID for any type of official communication with in the Government. Third party email services should not be used for official communication.

All departments are requested to submit to the O/O the CISO, Delhi, that the "Compliance Certificate confirming that all official communication is on official Govt. email".

This issues with the prior approval of Pr. Secretary-IT.

[Handwritten Signature]
6/9/24

(K.Murugan)

Chief Information Security Officer (CISO), Delhi

Encl: A/a

To,

1. All ACS/Pr.Secretaries/Secretaries/HoDs
2. All Local Bodies/Boards/Commissions, Govt. of NCT of Delhi

Copy for information to:

1. SO to Chief Secretary, GNCTD
2. PS to Pr. Secretary (IT), GNCTD

617

Government of NCT of Delhi
Department of Information Technology

9th Level, B wing Delhi Secretariat IP Estate, New Delhi
<https://it.delhi.gov.in>

E-17/4/2022/Dir(DeGS) / Computer No- 042708413 / 7610 - 89 dated: 30/10/2023

To,

All ACS/Pr.Secretaries/Secretaries/HoDs/Local Bodies/Boards/Commissions,
Govt. of NCT of Delhi.

Subject: Measures to enhance Cyber Security within the Government

Kindly refer to the this office circular issued vide E-17/4/2022/Dir(DeGS) / Computer No- 042708413/6595-6674 dated 05.10.2023 on the subject cited above (copy enclosed).

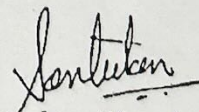
In the said circular, all departments of Govt. of NCT of Delhi were requested to take immediately following measures to enhance the Cyber Security preparedness:

- (i). Banners on Cyber Security's Dos & Don'ts, should be hanged/pasted on each premise of departments of GNCTD at the place with proper visualization
- (ii). Organize Cyber Security Awareness program/ Cyber Suraksha Jagrukta Program at their own level to make the people more aware and safe/secure in r/o any cyber-incident/attack.

In view of this, it is requested to submit a progress report in the O/o the undersigned in the following format:

Department Name	Banners on Cyber Security's Dos & Don'ts, hanged/pasted in department (Yes/No)	Cyber Security Awareness program/ Cyber Suraksha Jagrukta Program organized (Yes/No)

This letter is issued with the prior approval of the Secretary (IT).


(Santulan Chaubey)

Chief Information Security Officer (CISO), Delhi

Encl: A/a

Copy for information to:

1. SO to Chief Secretary, GNCTD
2. PS to Secretary (IT), GNCTD.

431/JDUD
08/10/2023

Government of NCT of Delhi

Department of Information Technology

9th Level, B wing Delhi Secretariat IP Estate, New Delhi

<https://it.delhi.gov.in>

E-17/4/2022/Dir(DeGS) / Computer No- 042708413/6595-6674 dated: 05/10/2023

253/C
430

CIRCULAR

Subject: Measures to enhance Cyber Security within the Government

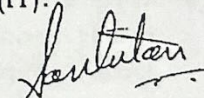
In reference to the subject cited above, it is to inform that keeping Govt. Infrastructure safe & secure from any Cyber Incident/Attack, is area of concern and is on top priority for Government.

In view of this, all departments of Govt. of NCT of Delhi are requested to take immediately following measures to enhance the Cyber Security preparedness:

- (i). Banners on Cyber Security's Dos & Don'ts, as per Annexure-A & B, should be hanged/pasted on each premise of departments of GNCTD at the place with proper visualization
- (ii). Organize Cyber Security Awareness program/ Cyber Suraksha Jagrukta Program at their own level to make the people more aware and safe/secure in r/o any cyber-incident/attack.

As Cyber and information security is a niche area and is the prime concern for the Government, hence, all departments are requested to provide attention to Cyber Security and ensure execution of above mentioned points under perusal of respective HoDs.

This letter is issued with the prior approval of the Secretary (IT).


(Santulan Chaubey)

Chief Information Security Officer (CISO), Delhi

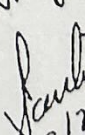
Encl: A/a

To,

1. All ACS/Pr.Secretaries/Secretaries/HoDs.
2. All Local Bodies/Boards/Commissions, Govt. of NCT of Delhi.

Copy for information to:

1. SO to Chief Secretary, GNCTD
- ✓ 2. PS to Secretary (IT), GNCTD.

2
5/20/23
We may review which of the depts have not responded reg. cyber security.

10/10/23

4731C

252/C

Annexure-A

DO's AT OFFICE

- 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.
- Set BIOS Password for booting.
- Ensure that the Operating System and BIOS firmware are updated with the latest updates/patches.
- Set Operating System updates to auto-updated from a trusted source.
- Ensure that the Antivirus client installed on your systems is updated with the latest virus definitions, signatures and patches.
- Only Applications/software's, which are part of the allowed list authorized by ACISO, shall be used.
- Shutdown the desktop before leaving the office.
- Keep printer's software updated with the latest updates/patches.
- Setup unique pass codes for shared printers.
- Printer to be configured to disallow storing of print history.
- Enable Desktop Firewall for controlling information access.
- Keep the GPS, Bluetooth, NFC and other sensors disabled on the desktops /laptops and mobile phones. They may be enabled only when required.
- Use a Hardware VPN Token for connecting to any IT Assets located in Data Centre.
- Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
- Change passwords at least once in 30 days.
- Use Multi-Factor Authentication, wherever available.
- 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
- 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.
- Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
- Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services. Such links may lead to a phishing/malware webpage, which could compromise your device
- Ensure that the mobile operating system is updated with the latest available updates/patches.
- Download Apps from official app stores of Google (for android) and apple (for iOS).
- Before downloading an App, check the popularity of the app and read the user reviews.
- Observe caution before downloading any apps which has a bad reputation or less user base etc.
- While participating in any sensitive discussions, switch-off the mobile phone or leave the mobile in a secured area outside the discussion room.

- D. 428
- Before installing an App, to carefully read and understand the device permissions required by the App along with the purpose of each permission.
 - 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.
 - Use auto lock to automatically lock the phone or keypad lock protected by pass code/ security patterns to restrict access to your mobile phone.
 - 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.
 - Take regular offline backup of your phone and external/internal memory card.
 - Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates.
 - 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, which could compromise your device.
 - Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.
 - Disable automatic downloads in your phone.
 - Always keep an updated antivirus security solution installed.
 - Ensure that Kavach Multi-Factor Authentication is configured on the NIC Email Account.
 - Download kavach app from valid mobile app stores only. Do not download from any website.
 - Use PGP or digital certificate to encrypt e-mails that contains important information.
 - Observe 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
 - Perform a low format of the removable media before the first time usage.
 - Perform a secure wipe to delete the contents of the removable media.
 - Scan the removable media with Antivirus software before accessing it.
 - Encrypt the files /folders on the removable media.
 - Always protect your documents with strong password.
 - Limit and control the use/exposure of personal information while accessing social media and networking sites.
 - Always check the authenticity of the person before accepting a request as friend/contact.
 - Use Multi-Factor authentication to secure the social media accounts.
 - It is recommended to use NIC's Sandes App instead of any 3rd party messaging app for official communication.
 - 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 NIC-CERT.

DON'Ts AT OFFICE

- Don't store any usernames and passwords on the Internet browser.
- Don't store any payment related information on the internet browser.
- Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies etc).
- Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.
- Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software's).
- Don't use your official systems for installing or playing any Games.
- Don't use the same password in multiple services/websites/apps.
- Don't save passwords in the browser or in any unprotected documents.
- 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).
- Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persons
- Any application/software which is not part of the authorized list approved by ACISO, shall not be used. Always lock/log off from the desktop when not in use.
- Internet access to the printer should not be allowed.
- Do not use any external mobile App based scanner services (ex: Cam scanner) for scanning internal government documents.
- Use of all pirated Operating systems and other software/applications that are not part of the authorized list of software's should be immediately deleted.
- 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.
- Don't accept any unknown request for Bluetooth pairing or file sharing.
- Do not share the email password or Kavach OTP with any unauthorized persons.
- Don't use any unauthorized/external email services for official communication.
- Don't click/open any link or attachment contained in mails sent by unknown sender.
- Don't plug-in the removable media on any unauthorized devices.
- Do not click on the links or files sent by any unknown contact/user.
- Do not publish or post or share any internal government documents or information on social media.
- Do not publish or post or share any unverified information through social media.
- Do not give share the @gov.in /@nic.in email address on any social media platform.
- 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).