Dr K R Murali Mohan
Chief Information Security Officer

सत्यमेव जयते

दूरभाष / Tel : 26962819, 26567373,
26562134, 26562122 (EPBAX)
फैक्स / Fax : 26569908, 26515637,
26863847, 26862418
वेबसाइट/website : www.dst.gov.in

भारत सरकार
विज्ञान और प्रौद्योगिकी मंत्रालय
विज्ञान और प्रौद्योगिकी विभाग
टेक्नोलॉजी भवन, नया महरौली मार्ग
नई दिल्ली-110 016

GOVERNMENT OF INDIA
MINISTRY OF SCIENCE AND TECHNOLOGY
DEPARTMENT OF SCIENCE AND TECHNOLOGY
TECHNOLOGY BHAVAN, NEW MEHRAULI ROAD
NEW DELHI-110 016

No. DST/TTG/CyberSecurity/2022 Dated: 16th Sept, 2022

Office Memorandum

Sub: Cyber Security Guidelines for Government Employees – reg.

Deptt. of Science & Technology (DST) is in receipt of Cyber Security Guidelines for Government Employees in the form of a document (copy attached) prepared by National Informatics Centre, Ministry of Electronics & Information Technology, Govt. of India.

(i) The guidelines specifies the 'dos and don'ts' with respect to cyber security and ensuring proper cyber security hygiene in the government offices including contractual/outsourced manpower in the Department.
(ii) These guidelines are to be adhered by all officers/staff including contractual and outsourced manpower in the Department.
(iii) All government employees, including temporary, contractual/outsourced resources are required to strictly adhere to the guidelines mentioned in this document. Any non-compliance may be acted upon by the CISOs.
(iv) Action Taken Report (ATR) be submitted periodically.
(v) It is requested that the guidelines be circulated among all the staff within division/institute/office.

2. This issues with the approval of competent authority.

Encl : As above

(K R Murali Mohan) 16/9/22
Chief Information Security Officer, DST

To

1. PSO to Secretary, DST
2. AS&FA, DST/Senior Advisor, PCPM, DST
3. JS(Estt & SMP), DST/JS(Admn), DST/CCA, DST/All Divisional Heads, DST
4. All the officers of DST/staff including contractual as well as other staff including consultants and DEOs working in DST - through e-Office dashboard.
5. All Autonomous Institutes of DST and Dy.CISOs – As per list attached at Annexure-I.
6. PMU, DST- with a request to upload in DST's e-Office dashboard.

Annexure-I

1. The Director, Agharkar Research Institute (ARI), Gopal Ganesh Agarkar Road, Pune-411 004, Maharashtra. (Kind attn: Dr. Prasad P. Kulkarni Scientist 'F' & Dy.CISO, ARI)
2. The Director, Aryabhatta Research Institute of Observational Sciences (ARIES), Manora Peak, Nainital-263002, Uttarakhand. (Kind attn: Dr. Indranil Chattopadhyay, Scientist-F & Dy. CISO, ARIES)
3. The Director, Birbal Sahni Institute of Palaeobotany, 53, University Road, Lucknow 226 007. (with a request to nominate suitable scientist/officer as Dy.CISO)
4. The Director, Bose Institute (BI), 93/1, Acharya Prafulla Chandra Road, Kolkata-700 009, West Bengal. (Kind attn: Prof. Rajarshi Ray, Professor & Dy.CISO, J C Bose Institute)
5. The Director, Centre for Nano and Soft Matter Sciences (CeNS), P.B.No.1329, Professor UR Rao Road, Jalahalli, Bengaluru-560 013. (Kind attn: Dr. Pralay K. Santra, Scientist D & CISO, CeNS)
6. The Director, Indian Association for the Cultivation of Science (IACS), 2A & B Raja. S. C. Mullick Road, Jadavpur, Kolkata – 700032, West Bengal. (Kind attn: (with a request to nominate suitable scientist/officer as Dy.CISO)
7. The Director, Indian Institute of Astrophysics (IIA), Koramangala, Bengaluru-560 034. (Kind attn: Sh. Anish Parwage, Engineer-D (Computer) & Dy.CISO, IIA)
8. The Director, Indian Institute of Geomagnetism (IIG), Mumbai Headquarter(Panvel Campus) Plot 5, Sector 18, Near Kalamboli Highway, New Panvel, Navi Mumbai, 410218 (Kind attn: Prof. S. Gurubaran, Professor-G & Dy.CISO, IIG)
9. The Director, International Advanced Research Centre for Powder Metallurgy and New Materials (ARCI), Balapur PO, Hyderabad-500 005, Andhra Pradesh. (Kind attn: Dr. Ravi Bathe, Sc. "F" and Head & Dy.CISO, ARCI)
10. The Director, Institute of Nano Science and Technology (INST), Habitat Centre, Sector-64, Phase-10, Mohali-160062, Punjab (Kind attn: Dr. Ehesan Ali, Scientist-E & Dy.CISO, INST)
11. The Director, INSTITUTE OF ADVANCED STUDY IN SCIENCE & TECHNOLOGY (IASST), Vigyan Path, Paschim Boragaon, Garchuk, Guwahati - 781035, Assam (Kind attn: Prof. Devasish Chowdhury, DY.CISO, IASST)
12. The President, Jawaharal Nehru Centre for Advanced Scientific Research (JNCASR), Jakkur, Bengaluru-560 064. (Kind attn: Prof. James Chelliah Head, Complab & Dy.CISO, JNCASR)
13. The Director, Raman Research Institute (RRI), C.V.Raman Avenue, Sadashivanagar, Bengaluru – 560 080 (Kind attn: Sh. Jacob Rajan, in-charge, Computer group & Dy.CISO, RRI)
14. The Director, S.N.Bose National Centre for Basic Sciences (SNB), Sector-III, Block-JD, Salt Lake, Kolkata- 700 098. (Kind attn: Sh. Sanjoy Choudhury, Scientist D & Dy.CISO, SNB)
15. The Director, Sree Chitra Tirunal Institute for Medical Sciences & Technology (SCTIMST) Thiruvananthapuram - 695 011, Kerala (Kind attn: Dr. Geetha G. Scientist G(Sr. Grade) & Dy.CISO, SCTIMST)

16. The Director, WADIA INSTITUTE OF HIMALAYAN GEOLOGY (WIHG), 33, General Mahadeo Singh Road, Dehradun – 248001 (Uttaranchal) (Kind attn: Dr. Vikram Gupta, Scientist 'F' & Dy.CISO, WIHG)
17. The Director, National Innovation Foundation-India, Amrapur, Gandhinagar-Mahudi Road, Gandhinagar, Gujarat- 38265012. (Kind attn: Er. Tushar Garg, Scientist & Dy.CISO, NIF)
18. The Director, Vigyan Prasar, A-50, Institutional Area, Sector-62, Noida-201309, Uttar Pradesh. (with a request to nominate suitable scientist/officer as Dy.CISO)
19. The Executive Director, Technology Information, Forecasting and Assessment Council (TIFAC), A Wing, Vishwakarma Bhawan, Shaheed Jeet Singh Marg, New Delhi-110016. (Kind attn: Dr. Yashwant Dev Panwar, Sc F & Dy.CISO, TIFAC)
20. The Secretary, Science and Engineering Research Board, 5 & 5A, Lower Ground Floor, Vasant Square Mall, Sector-B, Pocket-5, Vasant Kunj, New Delhi – 110 070 (with a request to nominate suitable scientist/officer as Dy.CISO)
21. The Director General, North East Centre For Technology Application and Reach (NECTAR), 2nd Floor, Vishwakarma Bhawan, Shaheed jeet Singh Marg, New Delhi-110016 (Kind attn: Dr. Krishna Kumar, Advisor (Technical) & Dy.CISO, NECTAR)
22. The President, Indian National Science Academy (INSA), Bahadur Shah Zafar Marg, New Delhi-110 002 (Kind attn: Sh. Karthikeyan S., Assistant Executive Director-II & Dy.CISO, INSA)
23. The Executive Secretary, National Academy of Sciences –India (NASI), 5, Lajpatrai Road, Mumfordganj, New Katra, Allahabad – 211 002 (Kind attn: Sh.B.P.Singh, Dy.CISO, NASI)
24. The Executive Secretary, Indian Science Congress Association, 14, Dr. *Biresh* Guha Street, Kolkata-700 017. (with a request to nominate suitable scientist/officer as Dy.CISO)
25. The Executive Secretary, INDIAN ACADEMY OF SCIENCES (IASc)P.B. no.8005, CV Raman Avenue, Sadashivnagar, Bangalore – 560 080. (Kind attn: Er K S Sumesh, IT Support Engineer & Dy.CISO, IASc)
26. The President, Indian National Academy of Engineering *(INAE)*, Block II, Ground Floor, Technology Bhawan, New Mehrauli Road , New Delhi - 110016. (Kind attn: Dr. Debjani Bhattacharya, Research Officer & Dy.CISO, INAE)
27. *The Secretary,* Technology Development Board, Technology, Block II, Second Floor, Technology Bhawan, New Mehrauli Road New Delhi-110016. (with a request to nominate suitable scientist/officer as Dy.CISO)
28. The Director, National Atlas&Thematic Mapping Organisation Govt. of India, (Deptt. Of Science &Technology), C.G.O. Complex, (7th Floor), DF Block, Salt Lake City, Calcutta - 700 064 (with a request to nominate suitable scientist/officer as Dy.CISO)
29. The Surveyor General of India, Survey of India, Post Box No. 37, Dehra Dun - 248001 (Uttarakhand) (Kind attn: Shri Pardeep Kumar Dy. Surveyor General & Dy.CISO, Survey of India)

Part- 2

Cyber Security Guidelines For Government Employees

1. SCOPE AND TARGET AUDIENCE

The following guidelines are to be adhered to by all government employees, including outsourced/contractual/temporary employees, who work for government Ministry/Department.

2. DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE

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 BIOS Password for booting.

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 client installed on your systems are updated with the latest virus definitions, signatures and patches.

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.

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, NFC and other sensors disabled on the desktops /laptops and mobile phones. 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) for scanning internal government documents.

2.18 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.

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 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).

3.7 Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persons

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 (ex: Nord VPN, Express VPN, Tor, Proxies etc).

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's).

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 shortener services. Such links may lead to a phishing/malware webpage, which could compromise your device.

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).

5.5 Before downloading an App, check the 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, to 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, 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 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.

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 NIC-CERT.

6.7 Use PGP or digital certificate to encrypt e-mails that contains important information.

6.8 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.

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 it.
7.4 Encrypt the files /folders on the removable media.
7.5 Always protect your documents with strong password.
7.6 Don't plug-in the removable media on any unauthorized devices.

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 give share the @gov.in /@nic.in email address on any social media platform.

8.8 It is recommended to use NIC's Sandes App instead of any 3rd party messaging app for official communication.

9. SECURITY ADVISORY AND INCIDENT REPORTING

9.1 Adhere to the Security Advisories published by NIC-CERT (https://niccert.nic.in) and CERT-In (https://www.cert-in.org.in).

9.2 Report any cyber security incident, including suspicious mails and phishing mails to NIC-CERT (incident@nic-cert.nic.in) and CERT-In (incident@cert.org.in).

10. CYBER SECURITY RESOURCES

The following resources may be referred for more details regarding the cyber security related notifications/information published by Government of India:

S. No	Resource URL	Description
1	https://www.meity.gov.in/cybersecurity-division	Laws, Policies & Guidelines
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in	Security Tools & Best Practices

5	https://infosecawareness.in/	Security Awareness materials
6	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips

11. COMPLIANCE

All government employees, including temporary, contractual/outsourced resources are required to strictly adhere to the guidelines mentioned in this document. Any non-compliance may be acted upon by the respective CISOs/Ministry/Department heads.