Cyber Security Guidelines for Compliance by CISO

MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY

Version 1.4
September 2022

A-Block, CGO Complex
New Delhi – 110003
Website: https://www.nic.in/

DOCUMENT CONTROL

DOCUMENT NAME: Cyber Security Guidelines for Compliance by CISO

DOCUMENT ID REFERENCE: CSGCC

AUTHORIZATION:

S. No	Name	Designation	Role
1	Mr. Alkesh Kumar Sharma	Secretary, MeitY	Approving Authority
2	Dr. Rajendra Kumar	AS, MeitY	Reviewer
3	Mr. Rajesh Gera	DG, NIC	Reviewer
4	Dr. Sanjay Bahl	DG, CERT-In	Reviewer
5.	Mr. Sushil Pal	JS(eGov), MeitY	Reviewer
6	Mr. R.S. Mani	DDG, NIC	Reviewer
7	Dr. Seema Khanna	DDG, NIC	Reviewer
8.	Mr. CJ Antony	DDG, NIC	Reviewer
8	Mr. S.S. Sharma	Scientist-F, CERT-In	Reviewer
9	Mr. Hari Haran	SSA, NIC	Author

VERSION HISTORY:

Issue Date	Effective Date	Description
1.1	7-Jun-2022	Draft- Added Section-5, Cyber Security Resources
1.2	8-Jun-2022	Draft – Added inputs from CERT-In and included DNS Server IPv4 and IPv6 IP addresses.
1.3	10-Jun-2022	Final Release
1.4	5-Sep-2022	Added clauses related to network security, access control, hosting of websites, logging and segregated the clauses into various sub-categories. Guidelines divided into 2 parts, for compliance by the respective stakeholders.

DISTRIBUTION LIST:

The following persons hold copies of the documents; all amendments and updates to the document must be distributed to the distribution list.

S. No.	Name	Location	Document type
1	CISOs and DCISOs of Government Ministries and Departments	Across India	Soft copy of both Part-1 and Part-2
2	Government Employees	Across India	Soft copy of Part-2

DISCLAIMER:

This document is solely for the information of the government employees and

outsourced/contractual resources.

TABLE OF CONTENTS

1. INTRODUCTION

Information Communication Technology (ICT) has become ubiquitous amongst government ministries and departments across the country. The adoption and use of ICT has increased the attack surface and threat perception to government, due to lack of proper cyber security practices followed on the ground.

This guideline for CISO has been complied with the objective to ensure a sanitized and secure framework in the Ministries. CISO is also required to sensitize the government employees, contractual/outsourced manpower and build awareness from a cyber security perspective as per the Cyber security guidelines for Government Employees.

The ownership of Compliance of this guideline (part1 & part 2) rests with the CISO of each Ministry/Department.

This Guideline has been divided into 2 parts as given below:

1.	Guidelines for Secure Local Area Network	Part-1	Part-1 of this guideline is for the compliance of CISOs and DCISOs only. It should not be shared in public domain or with any unauthorized person.
2.	Cyber security Guidelines for Government Employees	Part-2	Part-2 of this guideline is for the compliance by all government employees, including outsourced/contractual/temporary employees who work for the government. CISO will generate awareness and ensure employees comply with the Guidelines.

Part- 1

Guidelines
For
Secure Local Area Network

1. SCOPE

The following guideline on Secure Local Area Network shall be adhered by the respective IT/Network teams of each Ministry/Department. The CISO of the Ministry/Department shall ensure the compliance of this guideline.

2. SECURE LOCAL AREA NETWORK

2.1. Ensure timely action is taken on the alerts and advisories shared by NIC-CERT and CERT-In.

2.2. Ensure that the Applications/websites/services are hosted only at the designated data centres of Government or Cloud Service Providers empanelled by MeitY. No application/website shall be hosted within the LAN segment of a Ministry/Department/Office.

2.3. Ensure that all Websites and Applications are "https" enabled with a valid SSL/TLS Certificate.

2.4. Ensure that a Cyber Crisis Management Plan (CCMP) is prepared and implemented for the Ministry/Department. Cert-In can be contacted for the template for preparing the CCMP by sending a mail to exercises@cert-in.org.in.

2.5. All ICT devices should be connected via the internet gateway of NIC's network (i.e. NICNET) and any other direct internet connection i.e., broadband, 3G/4G/5G etc., should be withdrawn with immediate effect.

2.6. Media Access Control (MAC) address binding is mandatory for all systems/IT devices connected in the Ministries/Department.

2.7. Unmanaged network devices should be replaced with managed devices on an immediate basis.

2.8. Configure host firewall in all systems to restrict lateral movement within the same network segment.

2.9. Internet connectivity to be withdrawn and Only NICNET connectivity to be provided to users who do not adhere to

guidelines mentioned under the head "desktop/laptop and printer security ". Internet connectivity to be restored with the approval of CISO of the ministry.

2.10. Network firewall shall be used to restrict traffic movement outside the network segment. Only selected ports and protocols shall be allowed for communication with selected IPs, as per the requirements of the official work.

2.11. Systems and equipment's which are obsolete and/or using obsolete/ unpatched operating systems, to be removed from the network.

2.12. Ensure that Kavach Multi-Factor Authentication is configured on all the NIC Email Accounts in the Ministry.

2.13. Implementation of Network Access control (NAC) is recommended.

3. DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE

3.1 Standard User (non-administrator) account to be set for all users for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.

3.2 Set BIOS Password for booting.

3.3 Operating System and BIOS firmware to be updated with the latest updates/patches.

3.4 Set OS updates to auto-updated from a trusted source and ensure they are updated on all devices. Install enterprise Antivirus/ EDR client offered by Government on official desktops/laptops. Ensure that the Antivirus client is updated with the latest virus definitions, signatures and patches.

3.5 CISOs shall maintain a list of authorized Applications/software's, which can be used by the employees/users. Applications/Software's which are not part of the authorized list shall not be allowed.

3.6 Ensuring Change of passwords at least once in 30 days.

3.7 Configure NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) in the system's DNS Settings for all users.

3.8 Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in all the user's system NTP Settings for time synchronization.

3.9 Removal of all pirated Operating systems and other software/applications that are not part of the white listed software's should be immediately deleted.

4. LOGGING

4.1 Ensure that logging is enabled on all ICT systems – which includes but not limited to websites/applications, databases, operating systems, ICT devices.

4.2 The logs of ICT Systems shall be retained for minimum one year.

4.3 Central Ministries and Departments shall contact NIC and onboard their ICT systems to PRATIMAAN (Alert system) and IPAM (asset management). State Government Departments/Entities may contact the respective state NIC centres for on boarding their ICT systems to PRATIMAAN and IPAM.

5. COMPLIANCE

The CISOs of the respective Ministry/Department shall ensure compliance of the guidelines mentioned in the Part-I: Secure Local Area Network.

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.