“हर काम देश के नाम”
रक्षा लेखामहानियंत्रक
उलान बटाररोड, पालम, दिल्ली छावनी-110010
CONTROLLER GENERAL OF DEFENCE ACCOUNTS
Ulan Batar Road, Palam, Delhi Cantt.- 110010

Phone: 01125665761 email: cgdanewdelhi@nic.in

No./Mech/IT & S/810/Cyber security Date: 05/09/2024

To,
All PCsDA/CDAs /PIFAs/IFAs

(Through CGDA Website)

Subject: Master circular on cyber security related instructions.

For effective monitoring and strengthening of cyber security framework of our organisation, numerous circulars have been issued from time to time by HQrs office. In order for the officials /employees to have access to all these instructions/advisories at one place, a ‘**Master circular**’ has been prepared.

The ownership of Compliance of these guidelines rests with the Dy. CISOs of each Controller.

Cyber security Guidelines for employees from Govt. of India :

A. **Desktop/Workstation and printer security at office :**

a. Use only Standard user(non-administrator) account for accessing the computer for regular work. Admin access to be given to users with approval of CISO only.
b. Setup unique pass codes for shared printers.
c. Always lock/log off from the desktop when not in use or before leaving the office.
d. Enable desktop firewall for controlling information access.
e. Ensure that the antivirus client installed on your systems is updated with the latest virus definitions, signatures and patches.
f. Ensure that Operating system and BIOS firmware are updated and set BIOS password for booting.
g. GPS, Bluetooth, NFC and other sensors on the desktop should only be enabled when required.
h. Use of all pirated Operating systems and applications should be deleted.
i. Do not use any external mobile App based scanner services for scanning internal government documents.
j. Keep regular backup of critical data.
k. Maintain Airgap between intranet and internet systems as per organization’s existing information security policies as well the baseline security guidelines to ensure cyber resilence.
l. Internet access to the printer should not be allowed.
m. Printer to be configured to disallow storing of print history.
n. 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.)
o. Do not use personal laptops/tablets/mobiles/fitbits or any other electronic gadgets in office LAN.

p. User must ensure that the PC/laptop/workstation in intranet must not be connected to any external network by any means, wired or wireless, under any circumstances.

q. User shall never share hard disk or folders with anyone, by default. However, whenever necessary, only the required folders shall be shared with the specific user for a specific period of time. A proper record needs to be maintained for any such sharing with the period of sharing clearly mentioned.

B. Password Management :

a. Use multi-factor password authentication.

b. Use complex passwords and change passwords at least once in 30 days.

c. Don't save passwords in the browser and don't use the same password in multiple websites/apps.

d. Don't share system passwords or printer pass code or WiFi passwords with any unauthorized persons.

e. Common password such as admin@123, password,admin or which contain words such as unit name, room no. , telephone , mobile or other things which is generally known to other colleagues must be avoided.

C. Internet Browsing Security :

a. Avoid using any third party anonymization services and toolbars /unauthorized VPN services and remote desktop tools like Anydesk in your internet browser.

b. While accessing govt. applications, email services or payment related services for any important services, always use private browsing or Incognito mode.

c. Don't store any username, passwords and payment related information on the internet browser.

d. Always type the site's domain name/URL manually on the browser's address bar while accessing sites where user login is required, rather than clicking on any link.

e. Enable genuine ad-blocker to protect from malvertising.

f. Ensure the genuineness of SSL/TLS website while performing online transactions.

g. Don't use official system for downloading unauthorized/pirated content/software from internet. Avoid installing playing games on official systems.

h. No official documents should be left on internet connected computers.

i. Cache & history should be deleted regularly from browser after every usage on internet connected system.

j. Observe caution while opening any shortened URLs.

D. Mobile Security:

a. Don't root or jailbreak your mobile device. Rooting or Jail breaking process disables many inbuilt security protections and could leave your device vulnerable to security threats.

b. Keep the WiFi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.

c. Before downloading an app, check the developer and popularity of the app and read the user reviews. Do not install app from untrusted sources.

d. Ensure that mobile system is updated with latest patches or available updates.

e. Always keep an updated antivirus security solution installed.

f. While participating in any sensitive discussions switch off the mobile phone or leave the mobile in a secured area outside the discussion room.

g. 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.

h. Don't accept any unknown request for Bluetooth pairing or file sharing.

i. Before installing any app, carefully read and understand the permission requests. 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).
j. Disable automatic downloads in your phone.
k. Use autolock to automatically lock the phone or keypad lock, passcode/security pattern to restrict access to your mobile phone.
l. 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. Report lost/stolen devices immediately to local police station.
m. Observe caution while opening any links share through social media/SMS by exciting offers/discounts etc.

E. Email Security :

a. Ensure that Kavach multi factor authentication is configured on the NIC email account. Download Kavach from valid mobile app stores only.
b. Don't use external email services for official communication.
c. 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, the same should be immediately reported to NIC-CERT.
d. Don't click any link or attachment contained in mails sent by unknown sender. Ensure the authenticity of the sender before opening the attachment in the email. Check for headers of original mail to check the authenticity.
e. Use PGP or digital certificate to encrypt emails that contains important information.
f. Be aware of current social engineering attacks and do not install any files in computer systems based on the directions over phone, wherein the caller would be pretending to be someone very important government official and insisting on urgency to download the files sent over email.
g. Be cautious while opening emails with attachments and hyperlinks on gov/nic email. Observe extra 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.

F. Removable Media Security :

a. Perform low format on removable media before first time ysage.
b. Don't plug-in the removable media on any unauthorized devices.
c. Scan the removable media with Antivirus software before accessing it and perform a secure wipe to delete the contents of the removable media.
d. Secure the files/folders on the removable media by encryption.
e. Disable auto-run functionality of the removable media while plug-in on the computer system.
f. Do not use removable disk in unsecured systems. Always protect your documents with strong password.

G. Social Media Security :

a. Limit and control the use/exposure of personal information while accessing social media and networking sites.
b. Always check the authenticity of the person before accepting a request as friend/contact.
c. Use Multi Factor Authentication to secure the social media accounts.
d. Avoid sharing any form of personal information like mobile no., address, aadhar etc. on social media.

e. Review social media privacy setting to ensure the level of security to personnel networking profile.
f. Do not publish or post or share any internal government documents or any unverified information on social media.
g. Do not share the @gov.in/@nic.in email address on any social media platform.
h. Do not share any official documents through messaging apps like whatsapp, telegram, signal etc. It is recommended to use NIC's Sandes app instead of any 3rd party messaging app for official communication.
i. Avoid to click on Ads that promise free money,prizes or discounts.

H. Online video calls and conferencing :

a. Enable the password authentication to enter in the meeting room.
b. Enable waiting room feature in video conferencing software.
c. Lock meeting once all the participants have joined.
d. Turn off the screen sharing functionality and remote monitoring features.
e. Be careful while opening links and documents.
f. Be careful what you show in the background and what is on your screen before using the screen sharing function.
g. Turn off anything that gives the app too many permissions.

I. Malware Defense Related :

a. Always set automatic updates for Operating System, Anti Virus and applications as envisaged in earlier points.
b. Configure web browser to block pop-ups, disable unnecessary plugins and enable secure browsing features.
c. Enable hidden file and system file view to find any unusual or hidden files.
d. Turn off auto play.
e. Configure the following parameter in the registry of PCs running Windows 8(and above) and all the servers using Windows 2012, to prohibit storing unencrypted passwords in RAM.
f. Type %temp%in "Windows Run"and delete all entries after opening any suspicious attachments.
g. Open command prompt and type netstat-na. checkout foreign established connection with IP addresses and its ownership.
h. Type "msconfig"in "Windows Run" and check for any unusual executable running automatically.
i. Check Network adapter for data/packets received and sent. If the outgoing/sent is unusually high, it is very likely that the system is compromised.
j. Type ipconfig/displaydns" in command prompt and look out for any URLs which you have not accessed recently.
k. Always be cautious while opening attachments even from the known sources. Try to use non-native applications for opening attachments(ex. Use wordpad to open a word document).
l. When in doubt, better to format the internet connected computer instead of performing some "patch works".
m. Prohibit any remote login to the system(RDP,SMB, RPC) for local administrators.
n. Check regularly if any unusual applications running from %appdata%, %tmp%, %temp%, %localappdata%, %programdata% directories.

o. Isolate hosts in the same VLAN, so that one workstation would not be able to gain access to another one on network levels L2/L3 and could access shared network segments (printers, servers etc.)

p. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources as well as addresses and block these before receiving and downloading messages.

q. Disable file and printer sharing services. If these services are required, use strong passwords or active directory authentication.

r. Disable or prevent ActiveX controls in Microsoft office word document from running without prompting.

s. Disable Macros in Microsoft office documents(doc/docx,xls/slsx, ppt/pptx and mdb/accdb). By default, Microsoft products come with VBS macro disabled.

t. Disable Java scripts or similar scripting functions in Adobe acrobat reader for PDF files.

u. Configure built in feature for "Protected View" settings in Microsoft office to open the Microsoft office word documents in protected view.

v. Check for unrecognized tasks being registered in task scheduler using "Schtasks/Query/FO list/V" from command prompt.

w. Use Tools that can analyze for malicious code execution.

x. Avoid internet access through administrator account. Instead, use a limited user account, which limits the impact of malware that tries to gain administrative access.

J. Internet Connection control :

a. Enable strong and latest secure encryption in Wireless networks.

b. Change default credentials for wireless admin console and network.

c. Update wireless router firmware regularly.

d. Avoid submitting sensitive information when using public WiFi.

e. Avoid to connect personal devices to unsecured network such as public unprotected network.

f. Turn off remote management functionalities like WPS and Universal Plug and Play. (UPnP).

g. Enable MAC address filtering and MAC binding to keep unauthorized devices away from wireless network.

h. Keep wireless network down when not in use.

K. Honey Trapping and Social Engineering :

a. Be vigilant of suspicious/unsolicited communications by unknown individuals. Be particularly wary of individuals who seem to be overly interested in personal/professional life or who ask for sensitive information. Whenever an unknown individuals tries to contact an officer through whatsapp, telegram, facebook , linkedin or any other social media app/website, govt. official should immediately inform his superior officers. The beginning of these interactions may be such as liking every posts, commenting/complementing on near every posts.

b. Any content posted on social media should not reveal any sensitive information like rank/Dept/Unit/Current project/Tour plans etc.

c. Steer away from unknown dating sites and don't trust generous offers.

d. Don't meet any unknown or little known person in any shady or lonely places like hotel rooms etc.

e. Do not engage in video calls from unknown numbers in social media platforms like whatsapp, facebook , telegram , signal etc.

L. Security Advisory and Incident Reporting :

a. Adhere to NISPG guidelines and other Security advisories published from time to time by CERT-In , MHA, NCIIPC, MeitY and other important government organisations.

b. Report any cyber security incident, including suspicious mails and phishing mails to CISO or Tech/IT team of your organisations for further escalation to NIC-CERT (incident@nic-cert.nic.in) and CERT-In (incident@cert.org.in)

M. Cyber attacks-

(a) Vishing and Phishing- Vishing and Phishing techniques wherein the adversary is using phone calls(Vishing) as a manipulative tactic to trick their victims into opening spear phishing emails sent on their NIC email, further leading to downloading of malicious files or credential harvesting.

(b) Phishing Domain- phishing campaign is primarily aimed to harvest the NIC credentials of government officials, to steal sensitive documents pertaining to Indian Government and to get unauthorized access to Government servers.

(c) Phishing email

(d) Attempts by Pakistani Intelligence Operatives -PIOs are using fake identities, including posing as defence correspondents of Ministries and are using spoofed numbers to gain the trust of unsuspecting individuals to ferret out sensitive information

N. Others-

- Avoid sharing sensitive information over open telephone calls.
- Use watermarks in classified documents- To overcome uncontrolled reproduction and pilferage of sensitive documents, appropriate classification & water marking of printed documents is recommended as a standard practice. Watermarking keeps the uniqueness of the copies of printed documents as well as identifies the owner of the document, thus enhancing info security and accountability

O. 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/cyber-security-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
7	https://security.nic.in/docs/ Security_Policies_for_GOI/Password %20Management%20Guidelines.pdf	NIC Password Policy
8	https://guidelines.india.gov.in/	Guidelines for Indian Government Websites

Cyber security Guidelines for Organisations-

1. Indicators of Compromise(IoCs)-

- Enforce blocking or filtering protocols to restrict access to the identified malicious IPs and domains. Additionally, perform comprehensive examinations of network logs and security alerts to detect any potential indicators of compromise
- Enhance employee awareness and training programs

2. MoD Net/Internet Users-

- Installation of 'Maya OS/Ubuntu' in all internet connected PCs
- No data processing or transmission of classified data, confidential and above, should be done on Internet endpoints/PCs.
- MoD Net Intranet (Air gaped network) to be used for data transmission/official work in DoD, DDP,DESW and MoD Fin.
- Ensure that no Internet devices are plugged into Intranet systems/MoD Net.
- Make sure that multi factor authentication is enabled for all accounts using in the network.
- Internet dependency should be minimized for all critical systems and control system devices should not be connected directly to the internet.
- All unused legacy applications should be removed from all machines on the network to avoid abuse.
- Critical networks, behind firewalls must be isolated from all the external network.
- Organisations should keep backup of important data, systems and configurations.

3. Compliance of Directions under Sub section (6) of Section 70B of Information Technology Act 2000-

- Retain all the internal logs (network, firewall etc.) for a duration of at least 180 days

4. Information Leakage through CCTV/Video surveillance(VSS)-

- Stay vigilant and keeping system upto date with the latest security practices can significantly enhance the security of CCTV system and protect it from potential threats and unauthorized access
- The rules and regulation as applicable, notified by the Government or procurement of goods and services must be followed
- The procurement of Video surveillance system from the brand having history of security breaches and data leakages should be avoided

- Use the testing infrastructure available with Standardization Testing and Quality Certification (STQC) Laboratory or any other agency notified by MeitY from time to time for testing the CCTVs.
- Maintain the network isolation (Air-Gap) from the public network to minimize the risk of unauthorized access and potential cyber-attacks. Use MAC address binding to prevent unauthorized access by unidentified devices
- Other checks- strong password, Regular Firmware updates,Encryption of data,Regular Security Assessments.

5. Website security-

- The Website should be audited by CERT-In empanelled Auditors and get Advisor(Cyber) clearance.
- Security Audit of the website should be performed annually.
- Website will be hosted with NIC only.
- Deployment of Secure Https and SSL certificate in all DAD applications/Websites.

6. Secure application design, development,implementation and operation- The guidelines released by CERT-In may be utilized to modify/transform the current applied processes in order to fill the gaps.

7. Network security-

- Internet and LAN/WAN connections should not be available on the same machine.
- Each machine on LAN/WAN Network should be duly protected against any physical access by unauthorized person. A strong password may be used.
- Each machine on LAN/WAN Network should be duly protected against virus/ malicious content by installing good quality antivirus. The antivirus must be updated & the machine should be scanned periodically.
- Unused open nodes of the LAN/WAN network must be disabled & closed.
- Password of any LAN/WAN application should not be saved at the login page.
- Any incident/ doubt of cyber attack on your network (both LAN & WAN) must be intimated to this HQrs & CERT-In immediately.

8. Hardware Security measures

- AMC of H/W peripherals should be done properly and periodically.
- All the Server/PCs should be on UPS with 24x7 power backup facility.
- Proper earthing should be available for all the H/W peripherals.
- Antivirus should be installed on PCs/Servers and updated time to time.
- H/W peripherals should be secured from Physical damage/ Natural disaster .Fire safety measures should be followed properly Acccss Control system should be managed for Server room.

9. Digital Signature Policy-

Signer Responsibilities

- Signers must obtain a signing key pair from the Department's Identity Management Group. This key pair will be generated using the

Department's Public Key Infrastructure (PKI) and the public key will be signed by the Department's Certificate Authority (CA).

- Signers must sign documents and correspondence using software approved by the IT wing.
- Signers must protect their private key and keep it secret.
- If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact Identity Management Group immediately to have the signer's digital key pair revoked.

Recipient Responsibilities

- Recipients must read `documents and correspondence using software approved by IT wing.
- Recipients must verify that the signer's public key was signed by the Department's Certificate Authority (CA), by viewing the details about the signed key using the software they are using to read the document or correspondence.
- If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.

10. Database Credentials Policy

1. **Access**:

- Each program or business function must have unique credentials; sharing is not allowed.
- Passwords are considered system-level and must adhere to the Password Policy.
- Implement processes to implement **Password Policy Guidelines**:

2. Storage:

- Credentials should not be hardcoded in the program's source code.
- They can be stored in a separate, secured file or on the database server.
- Use an authentication server (e.g., LDAP) to manage credentials if possible.
- Credentials must not be stored in a web server's document tree.
- Must comply with the Password Policy.

3. Retrieval:

- Read credentials from storage only when needed and clear them from memory immediately after use.
- Store credentials in a separate file from the main codebase, with no additional code present.
- Keep credential files out of executable directories

These measures are designed to ensure secure and controlled access to databases, minimizing the risk of unauthorized access and potential breaches.

11. Wireless Communication Policy-

All wireless infrastructure devices must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use approved authentication protocols and infrastructure
- Use approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.

12. Data Transmission Policy-

- **Web Traffic**: Use SSL/TLS with strong security protocols for all web-based communications.
- **Email Transmission**: Do not use email for sensitive data unless encrypted with tools like PGP or S/MIME. Alternatively, encrypt data files before attaching them to emails.
- **Non-Web Data**: Encrypt sensitive data using application-level encryption for non-web transmissions.
- **Database Connections**: Encrypt connections between application servers and external databases using FIPS-compliant algorithms.
- **Network-Level Encryption**: If application-level encryption isn't available, use network-level encryption methods such as IPSec or SSH tunneling for sensitive data.

2. All the PCsDA/CsDA are advised to ensure strict compliance of the guidelines given above by all employees (including contractual/outsourced) under their jurisdiction. Sensitization cum training sessions should be conducted by Dy.CISO/IT Heads explaining the salient features of these guidelines.

This issues with the approval of Addl. CGDA(IT)

Sr.ACGDA(IT)