INDIAN COUNCIL OF AGRICULTURAL RESEARCH
KRISHI BHAWAN, NEW DELHI-110001

F. No. FIN/22/02/2022-CDN(A&A) **Dated the:24th April, 2023**

ENDORSEMENT

Subject- IT security advisory for CNA agency users-reg.-

Ministry of Finance, Deptt. of Expenditure, Public Procurement Division, New Delhi has issued an O.M. No. V-17007/16/2023-ITD-CGA/C.No-12246/08 dated 03.04.2023 on the subject mentioned above.

As approved by the Competent Authority, this O.M. No. V-17007/16/2023-ITD-CGA/C.No-12246/08 dated 03.04.2023 has been posted on the ICAR Web-Site www.icar.org.in for information, guidance and compliance.

24/4/2023
(Saurabh Muni)
Deputy Director(Finance)

Distribution:

1. Directors/Project Directors of all ICAR Institutes/National Research Centres/Project Directorates/Bureaux.
2. US(Finance&Budget), DARE, Krishi Bhawan
3. All Officers/Sections at ICAR, Krishi Bhavan/KAB-1 & II/NASC
4. PD, DKMA for placing on the ICAR website
5. PSO to DG, ICAR/PPS to Secretary, ICAR/PPS to FA. DARE & ICAR
6. Secretary (Staff Side), CJSC, IIS&WC. Dehradun
7. Secretary (Staff Side), HJSC, ICAR
8. Guard File / Spare Copies.

961 18-4-23

V-17007/16/2023-ITD-CGA/C.No-12246/08 JS(Fin) DS(Fin)

GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF EXPENDITURE
CONTROLLER GENERAL OF ACCOUNTS
PUBLIC FINANCIAL MANAGEMENT SYSTEM (HQ)

3rd Floor, Shivaji Stadium Annexe
New Delhi-110001
Dated: 03.04.2023

Office Memorandum

Sub: IT security advisory for CNA agency users-Reg.

An IT security advisory for CNA agency users has been prepared by the PFMS in order to strengthen the security at user level. The details of new security features are depicted in the annexure –A.

All the CNA agency users are advised to ensure the compliance of the new IT security advisory at their respective levels and put in place a regular monitoring mechanism.

This issues with the approval of the Competent Authority.

Rahul Garg 03/04
(Rahul Garg)
ACGA, (Technology)
PFMS Division

To:

1. Pr.CCAs /CCAs /CAs with (I/C) of all Central Ministries/Departments.

Copy for information to: -

1. Sr.PS to CGA, O/o CGA
2. PS to Financial Advisors of all Central Ministries/Departments.
3. PS to Addl. Secretary, (PFS) D/o Expenditure, M/o Finance.
4. PS to Jt.CGA (JKP/CVP/HKS/SS), PFMS Division.
5. PS to Director, D/o Expenditure, M/o Finance.
6. DDG / SrTDs/TDs, NIC, PFMS Division.
7. Sr.AOs / AAOs, PFMS Division
8. Sr.AOs (Roll-out / CGA) for uploading on PFMS / CGA website.

Dir(F) I
DD(F) III
18/4/23

Annexure-A

IT Security related instructions while Using CNA Accounts.

A. Internal Control:

i. A delegation of financial power to different levels of authorities may be notified for each CNA/IAs.

ii. Every payment out of CNA/IAs shall be on the basis of a valid sanction order sanctioned by the designated competent authority.

iii. Each claim for drawl of money from CNA/IAs shall be prepared by an authority separate from sanctioning authority who shall forward the same to the payment authority.

iv. The payment authority shall authorize payment through DSC and PPA mode from the CNA bank account. Cheque / Online payment mode may be used for execution of payment through holding account.

v. In case of DSC payments by CNA, agency must ensure to send the DSC enrollment file to bank before execution of any payment by the agency. For physical payments i.e. PPA, verified signature of the payment authority shall be communicated to the bank in advance.

vi. Every payment to any Vendor/beneficiaries shall be done only after registration of the payees into the system. The process of registration includes entering the bank details of the payees into the system and authentication by the sanction generating authority based on account validation response received from Bank concerned.

vii. The bank holding the CNA shall send a daily statement indicating the payment details to the payment authority. CNA / IAs should review the following on daily basis.

- Failure payment and find out the failure reasons.
- Verify all the successful payments transferred to the correct beneficiary.
- Bank account balances should be matched against the actual passbook balances.
- Any discrepancy shall be brought to the notice of bank and settled.

viii. The Payment authority shall do a daily reconciliation with the claim raising authority to ensure that only duly authorized claims were disbursed. CNA / IAs must thoroughly check the bank details of beneficiary / vendor for each payment file batch with the corresponding physical bills before putting the Digital signature / PPA.

ix. Parent Agency (Funding agency) must conduct surprise audits on the financial activities of its child agencies once a month.

x. Agency Admin regularly audits the holding account fund transfer and settlement in time to avoid penalties. In case, no settlement is being done within the stipulated time, the amount shall be credited back to the Agency account.

xi. Funding/Parent Agency to ensure "Saving bank account" should be used during the scheme registration and also a non-interest bearing account should be used for holding account.

xii. The log of the approved agencies/ vendor/ individuals list with bank account details in soft and in physical form shall be reviewed and updated on regular basis.

B. **User and access Management:** - In the scenario of agencies working in a digital ecosystem, there must be a secured protocol for creation of and administration of their access in the system. Following security protocols are suggested in this regard:

1. Approval of new users at different levels (i.e sanction, raising claims, authorizing payment) shall be done by higher level designated authorities.
2. The users should access the system through user ID and password. Password should be of length of minimum 8 characters including special and Alpha numeric characters.
3. For new user registration, only the NIC/GOV email id should be used. Users already registered on PFMS with a Non-NIC/GOV email ID should be shifted to NIC/GOV domain email ID. Non-compliant users' accounts should be deactivated immediately. (Applicable only government officials/users)
4. Creation of multiple parallel agency admin IDs should be discouraged. In case of Agency Admin authorizes parallel agency admin ID creation, it should be allowed for a short duration and immediately discontinued after the use.
5. All users should ensure that the desktop must be locked (the shortcut Window+L) at the time of leaving their room/workstation.
6. Agency Admin while approving DSC should check the following
   - Check the validity of DSC.

- Certified DSC is being used by the agency. Agencies are advised to procure the certified DSC device from the empaneled vendors of Controller of Certifying Authority.
- Proper configuration of signatory levels as per the amount ranges.

7. The authorized DSC key owner should not share his/her digital signature key. If any legal issue arising because of the share of the DSC key shall be the liability of the owner. Any loss/theft of the DSC key should be reported and disabled immediately.

8. Users are not allowed to use digital signatures for making payments from the computers installed outside their office locations. Agency shall issue an instruction to their users on this effect.

9. In the current scenario whenever a payment is approved by the Data Approver then a SMS is being sent to the approver informing that payment has been approved by his/her login ID. Now the functionality has been enhanced upto the payment approval and DSC signing level, a SMS will be sent to all Agency ADMIN of the agency, so that at all time, the agency ADMIN user is aware that payment has been approved and execute by the data approver of the agency.

All the Agency admin are hereby directed to update their own Mobile numbers in user profile and for the DA (First & Second level signatory, if any) for receiving SMS while executing the activities

C. **Password Management:**

i All systems-level passwords must be changed at least every 90 days.The authenticating system will check for the expiration of **90** days & force the users to change their password.

ii The immediate last three passwords cannot be repeated.

iii Password reset cannot be done again for the same user ID within **30 minutes**.

iv After **five** un-successful attempts the account of the user should get locked out for **30 minutes** and if required to change his password immediately then use forgot password functionality.

v.The User ID and Password, shall in no circumstances, be shared with anyone by the owner and any breach of security/unauthorized access arising out of sharing the password/user name shall be the liability of the owner.

vi Auto storage of user name and password in browser/web page should be disabled in shared computers used for internet activities.

D. Exit Policy

i. At the time of relieving of any agency official (upon transfer/superannuation) his/her digital signature and system access credentials should be deactivated immediately.

ii. Ensure the user must return the assigned DSC to his/her immediate reporting officer at the time of leaving.

iii. Ensure the user must share his system details with the immediate reporting officer at the time of leaving.

E. Cyber Security: -

In addition to the above internal control framework and security protocols each agency working in IT ecosystem should observe various Do's and Don'ts to minimize malware (Virus, Trojan, and Worms etc.) infections while using internet-connected or standalone Computers. A set of guidelines in this regard is annexed **(Annex '1')**. Besides, Ministry of Electronics and Information Technology has issued a generic cyber security guideline to be followed by senior officers and office staff of GoI during day to day functioning, the guidelines (version 1.4 issued in September, 2022) is annexed **(Annex 'B')**. CNA/IAs may peruse and explore to enforce similar guidelines for their agencies working in the web based digital ecosystem.

Annex- 1

Do's

1. Always use genuine software.
2. Install the latest updates/patches for operating System, Antivirus and Application software.
3. Enable firewall, Operating Systems have an inbuilt firewall which can be used to stop unwanted Internet connections.
4. Limit user privileges on the computer. Always access Internet as a standard Windows user and not as Administrator.
5. Check and verify email sender IDs and web links before opening file attachments and clicking on links in emails and web pages.
6. Protect against social engineering attacks. Phishing emails and SMS are used to get user credentials like username, passwords, credit card and PIN numbers etc.
7. Regularly check the last login details of email accounts and any unauthorized access if noticed should be reported to IT team.

8. Use strong passwords that include a combination of letters, numbers and symbols.
9. Use only officially supplied USB storage media. USB storage media should be regularly formatted after use to erase any malicious files hidden from normal view.
10. Regularly take backup of document files to avoid loss of files in case of emergencies like malware infections, hard disk crash, corrupted applications and other unforeseen incidents.

Don'ts

11. Avoid downloading and installing pirated software.
12. Internet-connected computers should not be used for drafting or storing sensitive official documents.
13. Don't open emails from unknown email IDs. Such mails should be deleted from email account inbox.
14. Don't download and open file attachments that originated from unknown sources.
15. Avoid using personal USB storage devices/Smart Devices on office computers. Don't put unknown USB storage device into your Computer.

****

Cyber Security Guidelines for Government Employees

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	12-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	Government Employees	Across India	Soft copy

DISCLAIMER:

This document is solely for the information of the government employees and outsourced/contractual resources.

TABLE OF CONTENTS

CYBER SECURITY GUIDELINES FOR GOVERNMENT EMPLOYEES

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 has been complied with the objective to ensure a sanitized and secure framework in the Ministries. CISO is 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 rests with the CISO of each Ministry/Department.

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.