No. I-17016/1/2022-ITD-CGA/10985/264
Ministry of Finance
Department of Expenditure
Controller General of Accounts
Public Financial Management System
GIFMIS Vertical
****

3rd Floor, MLN Bhawan,
'E' Block, GPO Complex, INA Colony
New Delhi-110023
Dated: 23-08- 2024

Office Memorandum

Subject:- Observance of Security Protocols by users of PFMS.

The undersigned is directed to refer OM No.I-17016/1/2022-ITD-CGA/10985/229 dated 30.09.2024 to the subject above and state that this office had issued a set of instructions regarding safe and secured operation on PFMS by users and close monitoring of the compliance to these instructions by all field accounting units. The instructions covered areas of password policy, secured access control, enhanced security in bill processing, network security, Do's and Don'ts to be observed for secured access to PFMS modules, record management, and administrative measures for strict compliance and monitoring by higher authorities. The instructions were issued vide various OM's in the year 2018 to 2019.

2. The measures enforced through all these OM's and other new developments on this subject are reiterated here for each component of security protocols (enclosed). All Principal CCAs/ CCAs/CAs are kindly requested to ensure strict compliance of these instructions and regularly review the enforcement of these advisories at various levels. Any issues related to these areas may be immediately brought to the notice of this office.

This issues with the approval of Competent authority.

(B. Gopala Krishnakanth Raju)
Asstt. Controller General of Accounts
(GIFMIS)

To

All Pr. CCAs/CCAs/CAs with independent charge

Copy to:-

Financial Advisors of all Ministries/Departments

Copy for information to:

i. **PPS to CGA (PFMS)**
ii. **PPS to Additional Secretary (PFS), Department of Expenditure, MoF**
iii. **PS to Additional CGA (PFMS)**
iv. **Sr. AO(ITD) for uploading the OM on CGA's Website**

Consolidated instruction on various aspects of security while using PFMS

1. **Access Management:-**

i. For new user registration of officials dealing with PAO and DDO module of PFMS ,only NIC/GOV domain email id will be allowed. Same e-mail id and mobile number can be used maximum for four user ids within same PAO code and additional three user ids for across PAO codes keeping in view of multiple charges handled by users in different field offices.

ii. New user registration is to be initiated by the concerned approving authority in PFMS.

iii. Approval of new accounts shall be carried out by the designated officers on designated systems only. The IP addresses (Internal) of such systems and associated user accounts should be recorded on file. A system of two levels approval for creation of user and e-mail/SMS alert on creation of users to approvers has been built into the system.

iv. The new login Ids should be approved within the period of 15 days of creation. Marking of User ids which are at created mode i.e. not approved since 15 days as rejected is being enforced in the PFMS.

v. The CCA level user access facilitates MIS at the apex level, which can work as a deterrent to the unscrupulous elements and all the users approved at various levels should be closely monitored.

vi. The list of Govt. of India (GoI) sanction module users in PFMS i.e. PD, DDO, DH, AAO, PAO, Pr.AO, and CCA may be verified and updated on regular basis. If any user is found to be no longer in position then the same may be deactivated immediately. It is reiterated that Report MST-01 "User Details" under Menu "CAM REPORTS" may be reviewed on regular basis to get the status of active users in PFMS.

vii. Marking of inactive user ids > 45 days as disabled is being enforced in PFMS. Further, the said disabled user ids will be enabled only by two levels approvals in the next higher level hierarchy in PFMS. Self-enabling of disabled login id will not be allowed in PFMS.

viii. At the time of relieving of any Group 'A' & Group 'B' officer who is a user in PFMS viz. CCA level user, PAO type user, his/her digital signature & user Id should be deactivated. This should be one condition to be enforced while giving No objection certificate/LPC. Fresh user Id and digital signature should be provided to the new incumbent. Guidelines in this regard were issued vide this office OM No. A.22010/2013-18/CGA/Gr. A/Misc./4930 dated 18/03/2019.

23/08/24

ix. A notification to alert the user for change is given in case user login in the system other than the system generally being used by the user.

2. Password Policy in PFMS :-

i. Password should be of length of minimum 8 characters.

ii. Password mandatorily should include both special as well as Alpha numeric characters.

iii. Password should not have similarity with user name or part of the user name.

iv. To ensure that only the User knows the password he/she should change the password at the time of the first Login into the system.

v. User needs to change password every few weeks as the system automatically prompts for the change in password and does not allow Login without changing the password.

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

vii. In case of any suspicion of the password being compromised, it must be changed immediately by logging into PFMS portal.

viii. All computer systems being used for access of PAO/DDO module must be password protected.

ix. All users should ensure that the desktop must be locked (the shortcut Window l) at the time of leaving their room/workstation.

3. Processing of Payments:-

i. The I Key/DSC of the Pr. AO has to be invariably approved by the CCA level user, whereas I Key/DSC of PAOs by Pr. Accounts Officer level user and that of the CDDOs by PAO level user. The Timeout procedure for inserting the I Key/DSC for every session has been made in PFMS.

ii. The digital signature key used at various levels in PFMS is not to be shared with anyone by the person in whose name the key has been issued and any loss/theft thereof should be immediately reported to senior officials and the same should be disabled on PFMS immediately. Any breach of security/unaurthorised access arising out of loss of digital key shall be the liability of the owner.

iii. The default PIN/password of I Key/DSC may be changed and practice may be adopted for regular changing of its PIN/password. The same may also not to be shared with anyone.

23/08/24

iv. After each use the I Key/DSC token, it may be removed from the system.

v. Any legal issue arising because of sharing of digital signature key shall be the liability of the owner of digital signature key.

vi. All guide lines stipulated to be followed for making payments should be strictly adhered to and verification against physical documents should be done at all levels unless stipulated by explicit directions for use of electronic mediums.

vii. All Pay and Accounts Officers authorized for making payments shall verify each payment file of a batch with the corresponding physical bill/e-Bill without fail before putting the digital signature.

viii. PAOs may be advised strictly not to access the PAO/DDO module and not use digital signatures for making payment from the computers installed outside their office locations.

ix. System validation has been enforced to restrict the passing of bills at all the three levels in Pay & Accounts office viz. Dealing Hand, Asstt. Accounts Officer, Pay and Accounts Officer using the same I.P Address.

x. To avoid fraudulent payment, system validation has been enforced that DSC of same official cannot be used in all the three roles viz. Sanctioning Authority(PD checker), Drawing & Disbursing officer(DDO), and Pay & Accounts Officer(PAO) under same PAO code

xi. The session of PFMS may be logged out if not in use. Idle session may lead to unauthorized access and load on server.

4. Network Security:-

A. Do's and Don'ts to minimize Malware (Virus, Trojan, and Worms etc.) infections while using internet-connected or standalone Computers.

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 user but not as Administrator.

23/08/24

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 logging details of email accounts.**
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.**
11. **Users should be periodically briefed about Cyber Security measures.**

Don'ts

1. **Avoid downloading and installing pirated software.**
2. **Internet-connected computers should not be used for drafting/storing sensitive official documents/correspondences.**
3. **Don't open emails from unknown email IDs. Such mails should be deleted from email account inbox.**
4. **Don't download and open file attachments that originated from unknown sources.**
5. **Auto storage of user name and password in browser/web page should be disabled in shared computers used for internet activities.**
6. **Avoid using personal USB storage devices/Smart Devices on office computers. Don't put unknown USB storage device into your Computer.**
7. **Don't share passwords with anyone. Don't use the same password on all websites and services.**

B. Few indicators of a Generic Malware infected computer:

1. **Computer runs slowly than normal, stops responding or freezes often. Computer crashes and restarts every few minutes.**
2. **Unusual error messages pop up constantly.**

23/08/24

3. **New toolbars, links, or favorites added to your web browser.**

4. **Home page, mouse pointer, or search program changes unexpectedly.**

5. **Unusual network traffic and connectivity from the computer even without doing any Internet activity.**

(These are common signs of malware infection, but they may also be indicative of mere hardware or software problems.)

C. **Tips to check and protect from malware infections in Windows computer.**

I. Always set automatic updates for Operating System, Anti-Virus and Applications. For Windows OS auto update can be done as follows:-

Control Panel-->Windows Updates-->Change Settings-->Install updates automatically.

II. Checking for unusual network traffic with Windows "netstat-na" command.

Type "cmd" in "run" and type "netstat-na". Checkout foreign Established connection and IP addresses. Check the IP address for its ownership.

III. Check for any unusual executable running automatically at Windows startup.

Type "msconfig" in "run" and check for any unusual executable running automatically. (Disable, delete or uninstall any unnecessary/unknown executable/program.)

IV. Enable hidden files, folders and system files view of find any unusual or hidden files, especially useful while using USB storage devises.

Control Panel-->Folder Options-->View-->select the "Show hidden files and folders" option and unselect "Hide protected operating system files"

Make sure there is no hidden file and folders present in the USB Storage device. Format the device if any unusual files (files having extensions exe, com, dat, scr and ini etc) are present besides the data files (doc, ppt, xls and pdf etc).

V. Delete the contents of Windows "Temp" and "Temporary Internet files" regularly.

a. **Type %temp% in "run" and delete all the contents of temporary folder.**
b. **For deleting Temporary Internet Files follow steps as given by different browsers like Windows Internet Explorer, Google Chrome, Mozilla Firefox, Opera and Apple Safari.**

5. Record Management:-

23/08/24

i. The log of the approved agencies/ vendor/ individuals list with bank account details in soft and in physical form shall be maintained by PD, DDO, and PAOs. The same may be reviewed jointly and updated on regular basis.

ii. The IP address of the systems and User ids used for approval of new user ids/deactivation of user ids must be maintained and reviewed on regular basis.

6. Generic Cyber Security Protocols

Ministry of Electronics and Information Technology has issued a generic cyber security guidelines to be followed by senior officers and office staff in day to day functioning, The guidelines September , 2022 is enclosed for strict compliance by all offices using PFMS at various levels.

Encl: As above

23/08/24

(B. Gopala Krishnakanth Raju)
Asstt. Controller General of Accounts
(GIFMIS)