Administration Section
O/o Addl. Director General (B&A)
Prasar Bharati Secretariat
Room No. 604, Tower C,
Copernicus Marg, New Delhi - 110001
Email-pbadmnao15@gmail.com
Phone No. 23118459

No. PB-9(13)(1)/2019-Admn/Circular/256-264 **Dated: 12.07.2019**

To

The Sr. Accounts Officer
Pay & Accounts Office
All India Radio
Delhi, Mumbai, Chennai & Kolkata

The Sr. Accounts Officer
Pay & Accounts Office
Doordarshan
Delhi & Guwahati

Sub: - Security Advisory in r/o User Registration and Approval in Public Financial Management System (PFMS) – reg.

Sir/Madam,

Please find enclosed herewith a copy of O/o CCA, Pr. Accounts Office, M/o I&B, New Delhi's OM No. Pr.AO/B&A/I&B/PFMS(CSS)/2018-19/488-503 dated 04.07.2019 along with OM no. MF-CGA/ITD/SDTQC/2018-19/122/175 dated 07.05.2019 issued by the O/o CGA, M/o Finance, New Delhi on the subject mentioned above for necessary action and strict compliance.

This issues with the approval of DDG (F), Prasar Bharati Sectt.

Yours faithfully,

Encl: - As above.

12/07/2019

(S.S. Negi)
Sr. Accounts Officer (Admn)

Copy to: -

1. The Director (Tech), Prasar Bharati Sectt. with the request to upload the enclosed Office Memorandums on Prasar Bharati Website.
2. The Dy. Director (Admn.), All India Radio/Doordarshan, New Delhi – for information.

No. Pr.AO/B&A/I&B/PFMS(CSS)/2018-19/ 488-503
Government of India
Ministry of Information and Broadcasting
O/o Chief Controller of Accounts
Principal Accounts Office
Budget and Accounts Section
7th Floor, A- Wing, Shastri Bhawan, New Delhi – 110001

Dated : 4th July, 2019

Office Memorandum

Sub:- Security Advisory in r/o User Registration and Approval in Public Financial Management System (PFMS)-reg.

Please refer this office letter no. Pr..AO/B&A/I&B/PFMS(CSS)/2018-19/132-47 dated 13.05.2019 forwarding therewith O.M. no. MF-CGA/ITD/SDTQC/2018-19/122/175 dated 7th May, 2019 issued by the office of Controller General of Accounts, on the subject mentioned above.

2. Security protocols mentioned in the ibid O/o CGA O.M. are not being followed in Letter & Spirit by the Pay and Accounts offices of this Ministry, thereby threatening the security of the PFMS. At the time of relieving of any user of PFMS, his/her digital signature and user id should be deactivated at the time of his/her relieving. This should be one of the conditions to be enforced while giving No objection certificate/LPC. Whereas, it is observed that no intimation is being received in the Pr. Accounts Office (B&A Section) regarding deactivation of digital signature and user-id for officers transferred/retired from the office.

3. Further, it has come to the notice of PFMS that attempts are being made on PFMS to register with fake user-ids. The fake ids, which came to notice are of PAOs Login Id, for which request was made to Pr.AO approval. It is therefore requested that the Fresh user id and digital signature should be provided to the new incumbent, as per the guidelines circulated by O/o CGA from time to time.

4. In view of above, it is once again reiterated to strictly adhere to the security protocols circulated vide O/o CGA OM no MF-CGA/ITD/SDTQC/2018-19/122/175 dated 7th May, 2019 in respect of Access Management and Record management for registration and approval of new user-ids in the PFMS.

(**Chander Sain**)
Sr. Accounts Officer

To

(i) PAO (MS) / PAO (BOC etc.) / PAO (IRLA) at New Delhi, PAO (DD) Kolkata /PAO (AIR), Lucknow/ PAO (FD), Mumbai/ PAO (DD), Nagpur & PAO (DD),Chennai .
(ii) PAO (AIR) Kolkata, PAO (AIR) Mumbai, PAO (DD) & PAO (AIR), New Delhi, PAO (AIR) Chennai & PAO(DD), Guwahati.
(iii) ADG (B&A), Prasar Bharati, Copernicus Marg, Mandi House, New Delhi-110001 with a request to issue similar directions to PAOs attached with Prasar Bharati for compliance.
(iv) DCA (BOC etc. & IRLA) M/o I&B, Soochna Bhawan, New Delhi.

MOST URGENT

No.MF-CGA/ITD/SDTQC/SCP/2018-19/122/175
Government of India
Ministry of Finance,
Department of Expenditure
Office of the Controller General of Accounts
IT-Division
***

3rd Floor, MLN Bhawan,
'E' Block, GPO Complex, INA Colony
New Delhi-110023
Dated: May 7th, 2019

Office Memorandum

Subject: Security Advisory for online payment process in Public Financial Management System (PFMS).

The following security protocols should be observed for operation of Public Financial Management System (PFMS). All Pr. CCAs/CCAs/CAs with independent charge are requested to ensure compliance to following instructions:-

1. **Access Management** :-

(i) New account request should be accepted from registered users only.
(ii) For new user registration of officials dealing with PAO and DDO module of PFMS only NIC/GOV domain email id will be allowed.
(iii) Approval of new accounts shall be carried out by designated officers on designated systems only. The IP addresses (Internal) of such systems and associated user accounts should be recorded on file.
(iv) The list of 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 the same may be deactivated immediately.
(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) 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 issued vide this office OM No. A.22010/2013-18/CGA/Gr. A/Misc./4930 dated 18/03/2019.

2. **Password Policy in PFMS** :-

(i) Password should be of length of minimum 8 and maximum 10 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 password and user name should not be shared with anyone by the owner and any legal issue 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 for access of PAO/DDO module should be password protected.

3. **Processing of Payments:-**

(i) The I Key of the Pr. AO has to be invariably approved by the CCA, whereas I Key of PAOs by Pr. Accounts Officers and for the CDDOs by PAOs. Thus ensuring a check and balance accordingly. The Timeout procedure for inserting the I Key for every session has been made in PFMS.

(ii) The digital signature key used at various level 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.

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

(iv) 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.

(v) All Pay and Accounts Officers authorised for making payments shall verify each payment file of a batch with the corresponding physical bill without fail before putting the digital signature.

(vi) 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. Necessary systemic check of binding the IP addresses is being done.

(vii) 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 a 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.
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 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.
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:-**

(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 Userids used for approval of new userids/deactivation of userids must be maintained and reviewed on regular basis.

(Nalin K. Srivastava)
Dy. CGA (ITD)

To

All Pr. CCAs/CCAs/CAs with independent charge

Copy To:
Ps to CGA
PS to Addl. CGAs
PS to Jt. CGAs