No. PB-7(7)(2)/2018-Admn/Pt file/686   Dated: 10.01.2019

To

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

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

Sub:- Guidelines for IT platforms and Revised Password Policy for online Payments under Civil Accounts Organization - reg.
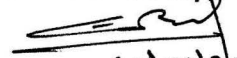
Sir/Madam,

Please find enclosed herewith a copy of O/o CCA, Pr. Accounts Office, Ministry of I&B, OM No.Pr.AO/I&B/B&A/PFMS (CSS)/2018-19/1984-2030 dated 08.01.2019 along with copy of OM No. MF-CGA/ITD/SDTQC/SCP/2018-19/2359 dated 03.01.2019 and OM No. MF.CGA/ITD-SPC/Password Policy/2012-13(Pt. file)/2329 dated 27.12.2018 issued by O/o CGA, M/o Finance, New Delhi on the subject cited above.

In this regard, you are requested to strictly adhered to the guidelines for enhanced security layers on PFMS.

This issues with the approval of ADG (B&A), Prasar Bharati Sectt.

Yours faithfully

10\01\2019

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

Encl: - As above.

Copy to: -

1. The Dy. Director (Accounts), Prasar Bharati Sectt. – for information.
2.   DDG (T)   , **Prasar Bharati Sectt. for its upload on Prasar Bharati Website.**

No.Pr.AO/I&B/B&A/PFMS (CSS)/2018-19/ 1984 -2030

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 04th January, 2019
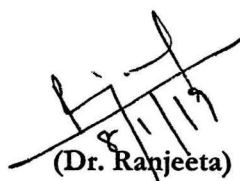
//Office Memorandum//

Subject:- Introduction of Enhanced Security Layers in the online payment process in PFMS: Regarding

Please find enclosed herewith Office of the Controller General of Accounts, Ministry of Finance, Department of Expenditure O.M no. MF-CGA/ITD/SDTQC/SCP/2018-19/2359 dated 3rd January, 2019 regarding enhanced security features/protocols which are being enforced in the operation of Public Financial Management System (PFMS) with a view to enhance its robustness.

2.   All Head of Departments including ABs are requested to issue necessary directions to the Programme Divisions (PDs), Drawing & Disbursing Offices (DDOs) in the Ministry and units/kendras of DG:DD and DG:AIR in Prasar Bharati to strictly adhered to the guidelines for enhanced security layers on PFMS attached at Annexure-A.

3.   This issues with the approval of the CCA (I&B).

Encl:-As Above.

(Dr. Ranjeeta)
Dy. Controller of Accounts

To

(i)   Pr. DG (PIB)/ DG (BOC etc.)/ DG (DPD)/ Pr. Press Registrar of India (RNI)/ DG (Film Division).

(ii)   Director (DFF)/Director (Photo Division)/Director (NMC)/Director (NFAI) /Director (EMMC) /CEO (CBFC)/HOD(FCAT).

(iii)   Director (Admn.), Main Sectt., Ministry of Information & Broadcasting, New Delhi.

(iv)   CEO, Prasar Bharati/CEO, CFSI/ Director General, IIMC/Director, SRFTI/Director, FTII.

(v)   DG (AIR) & DG (DD), New Delhi

(vi)   ADG (B&A), Prasar Bharati, Copernicus Marg, Mandi Huouse, New Delhi-110001.

(vii)   Sr.AO (Admn./IAW), Principal Accounts Office and all PAOs of Ministry of Information & Broadcasting.

Copy to:-

(i)   JS (P&A)/ JS(Film)/ JS(Broadcasting)/ JS(EW)/Sr. Economic Adviser

Copy for information to: -

(i)   PPS to Secretary (I&B)/ PPS to AS & FA (I&B)/ PPS to AS (I&B).

Enhanced Security Layers in the online payment process in PFMS for DDOs/PDs in Ministry and ABs including Units/Kendras of Prasar Bharati

(i) All officials of DDO/PD dealing with DDO/PD module of PFMS shall use NIC/GOV domain e mail ID for user registration. For new User registration only NIC/GOV domain email id will be allowed. The e mail id of all Ministry level users may be reviewed and users who have registered on PFMS with non-NIC/GOV e-mail may be directed to shift to NIC/GOV domain e- mail ID by **15-01-2019**. Beyond this date all non-NIC/GOV domain email IDs will be de-activated. **All DDOs/PDs may download a list of non-NIC/GOV domain e- mails from PFMS for taking necessary action by targeted date.**

(ii) The list of GoI sanction module users in PFMS which include PD, DDO may be verified and updated on weekly basis. If any user is found to be no longer valid the same may be deactivated immediately in consultation with respective PAO. A list of concerned Sanctions Module Users used by DDOs/PDs may be downloaded from PFMS. The same may be reviewed, verified and if any user is found to be no longer valid they may be deactivated immediately in consultation with respective PAO.

A system of two levels approval for creation of user and SMS alert on creation of users to approvers is being built into the system by O/o CGA, MoF, DoE and will be communicated shortly.

(iii) DDOs/PDs in Ministry and Unit/Kendras of PB may be advised strictly not to access the DDO/PD/EAT/DBT module and not use digital signatures for making payment from the computers installed outside their office locations.

(iv) At the time of relieving of any officer who is a DDO/PD in Ministry and Maker/Checker/Administrator in ABs, type user (upon transfer/superannuation) his/her digital signature, if any and 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.

(v) An additional security layer in the form of DSC for CDDO/DDO/PD type users to login into the system will be enforced in the system in phased manner. All CDDO/DDO/PD may immediately assess the requirement of DSCs and procure necessary hardware expeditiously. Necessary advisory may be issued to the Program Division for purchase of DSCs in r/o users functioning as PD and CDDO type wherever applicable.

(vi) 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.

(vii) All DDOs/PDs in Ministry and Checker/Maker/Administrator in ABs are instructed to observe strict confidentiality of user IDs/Passwords and security of Digital signatures if any. HODs are requested to make surprise checks and take strict action against those found to be breaching necessary security protocol issued by O/o CGA, MoF, DoE vide OM No. MF.CGA/ITD-SPC/Password Policy/2012-13/Pt.file/2329 dated 27/12/2018 (copy enclosed for ready reference).

No.MF-CGA/ITD/SDTQC/SCP/2018-19/2359
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: January 3, 2019

Office Memorandum

Subject: Introduction of Enhanced Security Layers in the online payment process in PFMS.

The undersigned is directed to state that following enhanced security features/protocols are being enforced in the operation of Public Financial Management System(PFMS) with a view to enhance its robustness. All Pr. CCAs/CCAs/CAs with independent charge are requested to ensure compliance to following instructions:

1. 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.

2. All officials of PAOs dealing with PAO and DDO module of PFMS shall use NIC/GOV domain e mail ID for user registration. For new User registration only NIC/GOV domain email id will be allowed. The e mail id of all Ministry level users may be reviewed and users who have registered on PFMS with non-NIC/GOV mail may be directed to shift to NIC/GOV domain e mail ID by 15-01-2019. Beyond this date all non-NIC/GOV domain email IDs will be de-activated. A list of non-NIC/GOV domain e mails in respective Ministry/Department is enclosed.

3. The list of GoI sanction module users in PFMS which include PD, DDO, DH, AAO, PAO, Pr.AO, and CCA may be verified and updated on weekly basis. If any user is found to be no longer valid the same may be deactivated immediately. A list of Government of India Sanction Module Users in respective Ministry/Department is enclosed. The same may be reviewed, verified and if any user is found to be no longer valid they may be deactivated immediately.
A system of two levels approval for creation of user and SMS alert on creation of users to approvers is being built into the system.

4. 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. All Pr. CCAs/CCAs/CAs are requested to prepare the list of IP addresses of all computers being used in PAOs and send to ITD by 11-01-2019.

5. At the time of relieving of any officer who is a PAO type user (upon transfer/superannuation) his/her digital signature and 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.

6. An additional security layer in the form of DSC for PAO type users to login into the system is being enforced in the system immediately. For all other type of users in PAOs i.e for PrAOs and CCA level users it is to be enforced w.e.f. 15-01-2019. For DDOs and PDs it will

be enforced in phased manner. All Pr. CCAs/CCAs/CAs may immediately assess the requirement of DSCs for PAOs and Pr.AOs and procure necessary hardware expeditiously. Necessary advisory may be issued to the Program Division for purchase of DSCs in r/o users functioning as PD and DDO type

7. 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.

8. Pr.CCAs/CCAs/CAs shall issue instructions to all Pr.AOs/PAOs under their control for observing strict confidentiality of user IDs/Passwords and security of Digital signatures. Pr CCAs/CCAs/CAs shall make surprise checks and take strict action against those found to be breaching necessary security protocol issued by this office vide OM No. MF.CGA/ITD-SPC/PasswordPolicy/2012-13/Pt file/2329 dated 27/12/2018

(Harish Kumar Srivastav)
Joint CGA (ITD)

To
All Pr. CCAs/CCAs/CAs with independent charge

Copy To:
Ps to CGA
PS to Addl. CGAs

(Annexures being shared with hard copies for respective Controllers)

No. MF.CGA/ITD-SPC/Password Policy/2012-13(Pt.File)/2329 Dated. 27.12.2018
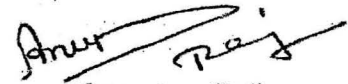
OFFICE MEMORANDUM

Subject: Guidelines for IT platforms and Revised Password Policy for online Payments under Civil Accounts Organization.

In Supersession of this office earlier OM No.MF.CGA/ITD-SPC/Password Policy/2012-13/08-43 dated 17th April 2018 the following password policy is enunciated with immediate effect in order to ensure more secure environment for online payments processing, under Civil Accounts Organization.

1. Password should be of length of minimum 8 and maximum 10 characters.
2. Password mandatorily should include both special as well as Alpha numeric characters.
3. Password should not have the similarity with user name or part of the user name.
4. 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.
5. 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.
6. A new user is created in PFMS only with the approval of authority which has been authorised for the same by system configuration.
7. In case the user is transferred/leaves the office the responsibility rests with the approving authority to disable the User ID.
8. 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 as such.
9. 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.
10. 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.
11. 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.
12. Any legal issue arising because of sharing of digital signature key shall be the liability of the owner of digital signature key.

13. 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.

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

15. Going forward, GOV/NIC domain email ids are mandatory to register on PFMS portal to perform any part of treasury function for the Government of India, all current users making use of Non-GOV/Non-NIC email ids to register on PFMS are supposed to obtain the same at earliest and register using the same. All other ids not using GOV/NIC domain emails for registering on PFMS shall be disabled with effect from 01st February, 2019

This issues for adherence to the above stipulations by the users.

(Anupam Raj)
Asstt. Controller General of Accounts

To

All Pr. CCAs/CCAs/CAs with independent charge