छत्तीसगढ़ शासन
वित्त विभाग
—:: मंत्रालय ::—
महानदी भवन, नवा रायपुर अटल नगर
जिला रायपुर

क्रमांक 1662 / पीएफएमएस / ब–4 / चार, नवा रायपुर अटल नगर, दिनांक 17 /08 / 2022

प्रति,

शासन के समस्त विभाग,
समस्त विभागाध्यक्ष,
छत्तीसगढ़

विषय :– IT Security Advisory for State Government and Agencies using PFMS.

संदर्भ :– भारत सरकार, वित्त मंत्रालय, व्यय विभाग, महालेखा नियंत्रक का कार्यालय ज्ञापन एफ.क्र. 14014 / 5 / 2021–पीएफएमएस / सी.क्र.–8766 / 1898, दिनांक 14.07.2022.

-----000-----

पीएफएमएस भारत सरकार की वित्तीय गतिविधियों के भुगतान निष्पादन, निगरानी और ट्रैकिंग के लिए एक वेब आधारित ऑनलाइन सॉफ्टवेयर एप्लीकेशन है। साइबर हमलों और अन्य दुर्भावनापूर्ण तथा कपटपूर्ण गतिविधियों को कम करने के लिए, राज्य सरकारों और पीएफएमएस का उपयोग करने वाली एजेंसियों के लिए भारत सरकार द्वारा तैयार की गई IT Security Advisory संलग्न प्रेषित है।

अतः आपके कार्यालय तथा अधीनस्थ कार्यालयों में PFMS उपयोग करने वाले संबंधित अधिकारियों / कर्मचारियों को इस संबंध में निर्देशित करने का अनुरोध है।

संलग्न :– उपरोक्तानुसार।

(ऋषभ पराशर)
उप सचिव
छत्तीसगढ़ शासन, वित्त विभाग

पृष्ठा. क्रमांक 1663/ पीएफएमएस / ब–4 / चार, नवा रायपुर अटल नगर, दिनांक 17 /08 / 2022

प्रतिलिपि :–

1. महालेखाकार, छत्तीसगढ़, रायपुर
2. मुख्य सचिव के उप सचिव, छत्तीसगढ़ शासन, मंत्रालय, नवा रायपुर अटल नगर
3. सचिव, छत्तीसगढ़ शासन, वित्त के निज सहायक, मंत्रालय, नवा रायपुर अटल नगर
4. समस्त विशेष सचिव / अपर सचिव / संयुक्त सचिव / उप सचिव / अवर सचिव / शोध अधिकारी / विशेष कर्तव्यस्थ अधिकारी, छत्तीसगढ़ शासन, वित्त विभाग, मंत्रालय, नवा रायपुर अटल नगर
5. संचालक, कोष, लेखा एवं पेंशन, छत्तीसगढ़, नवा रायपुर अटल नगर
6. संयुक्त महालेखा नियंत्रक, पी.एफ.एम.एस. ,राज्य परियोजना प्रबंधन इकाई इन्द्रावती भवन नवा रायपुर ,अटल नगर की ओर सूचनार्थ
10. राज्य सूचना अधिकारी, एन.आई.सी. की ओर सूचनार्थ एवं आवश्यक कार्यवाही हेतु
11. समस्त वरिष्ठ कोषालय / कोषालय अधिकारी, छत्तीसगढ़
12. संचालक, वित्तीय प्रबंध एवं सूचना प्रणाली, नवा रायपुर अटल नगर को वित्त विभाग की वेबसाइट www.cgfinance.nic.in पर अपलोड करने हेतु।

(चन्द्र प्रकाश पाण्डेय)
विशेष कर्तव्यस्थ अधिकारी
छत्तीसगढ़ शासन, वित्त विभाग

File No.V-14014/5/2021-PFMS

342
10/08/22

No-14014/5/2021-PFMS/C.No-8766/ 1898
Government of India
Ministry of Finance, Dept. of Expenditure
Controller General of Accounts
Public Financial Management System (HQ)
3rdFloor Shivaji Stadium Annexe
New Delhi-110001

Dated: - 14 /07/2022

Office Memorandum

PFMS is a web based online software application for payment execution, monitoring and tracking of financial activities of Government of India. In order to mitigate the cyber-attacks and other malicious and fraudulent activities, an IT security advisory for the State Governments and Agencies using PFMS, has been prepared and attached as Annexure-I for mandatory compliance at User level.

This issues with the approval of Competent Authority

(Yogesh Kumar Meena)
Dy.Controller General of Accounts

To,

All State Govt. Departments.

Copy for information to:-

1) PS to Addl.CGA, PFMS
2) PS to AS (PFS), DoE
3) PS to Jt.CGAs (AT/CVP/SS/HS/JKP)
4) DDG / Sr.T.D, NIC PFMS
5) All Dy. CGAs / ACGAs / ACAs, PFMS/ Director PFS DOE.
6) All State Directorates, PFMS for wide circulation.
7) Sr. AO –for uploading on PFMS web site.

Annexure-1

IT Security Advisory for State Governments and Agencies using PFMS

To mitigate the risks of cyber-attacks and other malicious activity, all users of PFMS (including Implementing Agencies and State Governments) are hereby advised to ensure the adoption of the following safeguards while accessing PFMS portal through their IT systems (desktops / laptops / mobile devices):

1. Print Payment Advise (PPA) will be discontinued from 30th Sept 2022 for Agencies who are having accounts in DSC enabled Banks. All Agencies are advised to shift from PPA to ePA / DSC mode for payments.
2. For SNA accounts for CSS, Cheques shall NOT be issued. Agencies shall make use of payments mode available in PFMS i.e.PPA/ DSC/ePA only.
3. External storage media and communication devices may be used strictly for official purpose. The unregulated use of devices (like pen drives, mobile phone etc.) can cause transmission of malicious files from device to computers and increases the vulnerability of data theft.
4. Regular backups shall be taken.
5. Use authorized and licensed software only.
6. Don't use the same password in multiple services/websites/apps.
7. Do not save your login credentials of PFMS in browser.
8. Don't use any unauthorized remote administration tools (e.g. Teamviewer, Ammy admin, Anydesk etc.).
9. Don't write down any passwords, IP addresses or other sensitive information on any unsecured material (e.g. sticky/post-it notes, plain paper pinned or posted on your table, etc.).
10. Don't use any 3rd party toolbars (e.g. download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
11. Keep your system password protected. The password may not be shared with any other person. To facilitate access by multiple users, if needed, different users may be created on the system.
12. Prevent malware and ransomware from being delivered and spreading to your devices. Prevent malware from running on devices. Do not send encrypted data and communicate with malicious IP addresses.
13. Users to ensure that anti-virus application is properly installed and is updated regularly. Computers may not be enabled with auto-play feature which prevents anti-

virus application from scanning the device after attachment to CPU.

14. Installation of "WhatsApp" in the system is not advisable and may be avoided.

15. Users shall ensure that unnecessary Apps related to cloud storage (Drop Box, Google Drive etc.) and remote access applications (like Any Desk, Team View) are not installed in the system.

16. Contractual employees are not posted in sensitive seats.

17. Cleaning of rooms and removing of paper waste by housekeeping staff is done under the supervision of Caretaker staff.

18. Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in.

19. Adhere to the security advisories published by NIC-CERT (https://nic-cert.nic.in/advisories.jsp) and CERT-In (https://www.cert-in.org.in).

20. Conduct precheck of all bills as per established procedure before making any payment.

****