Discussion

on

IT security advisory

for the State Governments and Agencies using PFMS

As per Office Memorandum

No-14014/5/2021-PFMS/C.No-8766/

of

Government of India

Ministry of Finance, Dept. of Expenditure

Controller General of Accounts

Public Financial Management System

Dated: -14 /07/2022

By

Directorate of Treasuries and Accounts

M.P. Bhopal

IT-Security Advisory:

Purpose:

- To mitigate the risks of cyber-attacks and other malicious activity
- साइबर हमलों और अन्य दुर्भावनापूर्ण जोखिमों को कम करना

- To ensure the adoption of the safeguards while accessing PFMS portal through IT systems (desktops / laptops / mobile devices)
- PFMS पोर्टल को एक्सेस के दौरान सिस्टम (डेस्कटॉप / लैपटॉप / मोबाइल डिवाइस)) मे सुरक्षा उपायों का पालन करना।

IT-Security Advisory:

PFMS Application related:

- 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.
- 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.

IT-Security Advisory:

Technical Advisory:

- 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.
- Regular backups shall be taken.
- Use authorized and licensed software only.
- Don't use the same password in multiple services /websites /apps.
- Do not save your login credentials of PFMS in browser.

IT-Security Advisory:

- Don't use any unauthorized remote administration tools (e.g. Team viewer, Ammy admin, Any desk etc.).
- 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.).
- Don't use any 3rd party toolbars (e.g. download manager, weather tool bar, askme tool bar, etc.) in your internet browser.
- 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.

IT-Security Advisory:

- Prevent malware and ransomware from being delivered and spreading to your devices. Do not send encrypted data and communicate with malicious IP addresses.
- 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.
- Installation of "WhatsApp" in the system is not advisable and may be avoided.
- Users shall ensure that unnecessary Apps related to cloud storage (Drop Box, Google Drive etc.) are not installed in the system.

IT-Security Advisory:

- See that contractual employees are not posted in sensitive seats.
- Cleaning of rooms and removing of paper waste by housekeeping staff is done under the supervision of Caretaker staff.
- Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in.
- 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).
- Conduct pre-check of all bills as per established procedure before making any payment.

Remain Alert

Thanks