

ਸਮੱਗਰਾ ਸਿੱਖਿਆ ਅਭਿਆਨ ਸਿੱਖਿਆ ਭਵਨ (ਪੰਜਾਬ ਸਕੂਲ ਸਿੱਖਿਆ ਬੋਰਡ)  
ਬਲਾਕ ਈ ਫੇਜ਼ 8 ਜਿਲ੍ਹਾ ਐਸ.ਏ.ਐਸ.ਨਗਰ

ਵੱਲ,

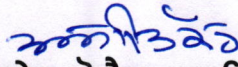
ਸਮੂਹ ਜਿਲ੍ਹਾ ਸਿੱਖਿਆ ਅਫਸਰ (ਐ.ਸਿ.),  
ਸਮੂਹ ਡਾਇਰੈਕਟ ਪ੍ਰਿੰਸੀਪਲ,  
ਸਮੂਹ ਬੀ.ਪੀ.ਈ.ਓ ਅਤੇ ਸਮੂਹ ਸਕੂਲ ਮੁੱਖੀ  
ਪੰਜਾਬ ਸਮੱਗਰਾ ਸਿੱਖਿਆ ਅਭਿਆਨ,  
ਪੰਜਾਬ।

ਮੀਮੇ ਨੰ: ਸਸਅ/ਵਿੱਤ/2022-23/ 2022 207711

ਮਿਤੀ: ਐਸ.ਏ.ਐਸ. ਨਗਰ : 05/08/2022

**ਵਿਸ਼ਾ:- Release of funds under the Centrally Sponsored Scheme (CSS) and monitoring utilization of the funds released- IT Security Advisory for State Governments and Agencies using PFMS.**

ਵਿਸ਼ੇ ਅੰਕਿਤ ਮਾਮਲੇ ਸਬੰਧੀ ਭਾਰਤ ਸਰਕਾਰ ਵਿੱਤ ਮੰਤਰਾਲੇ ਦਾ ਪੱਤਰ ਨੰ:14014/5/2021-PFMS/C.No-8766/1898 ,ਮਿਤੀ 14.07.2022 ਦੀ ਕਾਪੀ ਸਮੇਤ Annexure regarding IT Security Advisory for State Governments and Agencies using PFMS ਭੇਜ ਕੇ ਲਿਖਿਆ ਜਾਂਦਾ ਹੈ ਕਿ ਪੱਤਰ ਵਿੱਚ ਦਰਜ ਹਦਾਇਤਾਂ ਦੀ ਇੰਨ ਬਿੰਨ ਪਾਲਣਾ ਕਰਨੀ ਯਕੀਨੀ ਬਣਾਈ ਜਾਵੇ।

  
ਡਿਪਟੀ ਸਟੇਟ ਪ੍ਰੋਜੈਕਟ ਡਾਇਰੈਕਟਰ  
ਪ.20



1/402778/2022

ਅਤਿ ਜਰੂਰੀ

ਪੰਜਾਬ ਸਰਕਾਰ

ਵਿਤ ਵਿਭਾਗ

(ਵਿਤ ਬਜਟ-1 ਸ਼ਾਖਾ)

**ਵਿਸ਼ਾ:** Release of funds under the Centrally Sponsored Schemes (CSS) and monitoring utilization of the funds released -IT Security Advisory for State Governments and Agencies using PFMS. .

\*\*\*\*\*

ਸਮੂਹ ਵਿਸ਼ੇਸ਼ ਮੁੱਖ ਸਕੱਤਰ, ਵਧੀਕ ਮੁੱਖ ਸਕੱਤਰ, ਵਿਤੀ ਕਮਿਸ਼ਨਰ, ਪ੍ਰਮੁੱਖ ਸਕੱਤਰ ਅਤੇ ਪ੍ਰਬੰਧਕੀ ਸਕੱਤਰ, ਪੰਜਾਬ ਸਰਕਾਰ ਕ੍ਰਿਪਾ ਕਰਕੇ ਉਪਰੋਕਤ ਵਿਸ਼ੇ ਤੇ ਇਸ ਵਿਭਾਗ ਦੇ ਪੱਤਰ ਨੰ:FD-FB-109/5/2021-5FB1/193036, ਮਿਤੀ 07 ਜੂਨ 2021 ਵੱਲ ਧਿਆਨ ਦੇਣ ਦੀ ਕ੍ਰਿਪਾਲਤਾ ਕਰਨ ਜੀ।

2 ਵਿਸ਼ੇ ਅਕਿੰਤ ਮਾਮਲੇ ਸਬੰਧੀ ਭਾਰਤ ਸਰਕਾਰ ਵਿੱਤ ਮੰਤਰਾਲੇ ਦੇ ਪੱਤਰ ਨੰ:14014/5/2021-PFMS/C.No-8766/1898, ਮਿਤੀ 14-07-2022 ਰਾਹੀਂ State Governments and Agencies using PFMS ਲਈ, IT Security ਸਬੰਧੀ ਜਾਰੀ ਕੀਤੀਆਂ ਗਈਆਂ ਹਦਾਇਤਾਂ ਦੀ ਕਾਪੀ, ਇਸ ਪੱਤਰ ਨਾਲ ਨੱਥੀ ਕਰਕੇ ਭੇਜਦੇ ਹੋਏ ਬੇਨਤੀ ਕੀਤੀ ਜਾਂਦੀ ਹੈ ਕਿ ਆਪਣੇ ਵਿਭਾਗ ਤੋਂ ਇਨ੍ਹਾਂ ਹਦਾਇਤਾਂ ਦੀ ਇੰਨ ਬਿੰਨ ਪਲਾਣਾ ਕਰਵਾਉਣ ਦੀ ਕ੍ਰਿਪਾਲਤਾ ਕੀਤੀ ਜਾਵੇ ਜੀ।

ਜ.ਬ.ਕੇ  
ਸੁਪਰਡੈਂਟ 2/8/22  
ਰੌੜ

ਸੇਵਾ ਵਿਖੇ

ਸਮੂਹ ਵਿਸ਼ੇਸ਼ ਮੁੱਖ ਸਕੱਤਰ, ਵਧੀਕ ਮੁੱਖ ਸਕੱਤਰ, ਵਿਤੀ ਕਮਿਸ਼ਨਰ  
ਪ੍ਰਮੁੱਖ ਸਕੱਤਰ ਅਤੇ ਪ੍ਰਬੰਧਕੀ ਸਕੱਤਰ, ਪੰਜਾਬ ਸਰਕਾਰ।

ਅੰ:ਵਿ:ਪੰ:ਨੰ : FD-FB-101/09/2021-5FB1/402778 ਮਿਤੀ, ਚੰਡੀਗੜ੍ਹ: 02 ਅਗਸਤ, 2022  
ਇਕ ਉਤਾਰਾ ਮਾਨਯੋਗ ਮੁੱਖ ਸਕੱਤਰ, ਪੰਜਾਬ ਜੀ ਨੂੰ ਸੂਚਨਾ ਹਿੱਤ ਭੇਜਿਆ ਜਾਂਦਾ ਹੈ।

ਜ.ਬ.ਕੇ  
ਸੁਪਰਡੈਂਟ 2/8/22  
ਰੌੜ

ਸੇਵਾ ਵਿਖੇ

ਮੁੱਖ ਸਕੱਤਰ, ਪੰਜਾਬ ਸਰਕਾਰ

ਅੰ:ਵਿ:ਪੰ:ਨੰ : FD-FB-101/09/2021-5FB1/402778 ਮਿਤੀ, ਚੰਡੀਗੜ੍ਹ:02 ਅਗਸਤ, 2022



1/402778/2022

ਪਿੱਠ ਅੰਕਣ ਨੰ : FD-FB-101/09/2021-5FB1/402778 ਮਿਤੀ, ਚੰਡੀਗੜ੍ਹ:02 ਅਗਸਤ, 2022

ਇਕ ਉਤਾਰਾ ਹੇਠ ਲਿਖਿਆ ਨੂੰ ਸੂਚਨਾ ਅਤੇ ਅਗਲੇਰੀ ਲੋੜੀਂਦੀ ਕਾਰਵਾਈ ਹਿੱਤ ਭੇਜਿਆ ਜਾਂਦਾ ਹੈ।

1. ਡਾਇਰੈਕਟਰ, (ਖਜਾਨਾ ਤੇ ਲੇਖਾ), ਚੰਡੀਗੜ੍ਹ।
2. ਸਮੂਹ ਜਿਲਾ ਖਜਾਨਾ ਅਫਸਰ, ਪੰਜਾਬ

ਜ. ਜ. ਕੌਰ  
ਸੁਪਰਡੈਂਟ 28/8/22

ਪਿੱਠ ਅੰਕਣ ਨੰ : FD-FB-101/09/2021-5FB1/402778 ਮਿਤੀ, ਚੰਡੀਗੜ੍ਹ:02 ਅਗਸਤ, 2022

ਇਕ ਉਤਾਰਾ ਮਹਾਲੇਖਾਕਾਰ (ਲੇਖਾ ਅਤੇ ਹੱਕਦਾਰੀ) ਪੰਜਾਬ, ਚੰਡੀਗੜ੍ਹ ਅਤੇ ਪ੍ਰਮੁੱਖ ਮਹਾਲੇਖਾਕਾਰ (ਆਡਿਟ) ਪੰਜਾਬ, ਚੰਡੀਗੜ੍ਹ ਨੂੰ ਸੂਚਨਾ ਅਤੇ ਅਗਲੇਰੀ ਲੋੜੀਂਦੀ ਕਾਰਵਾਈ ਹਿੱਤ ਭੇਜਿਆ ਜਾਂਦਾ ਹੈ।

ਜ. ਜ. ਕੌਰ  
ਸੁਪਰਡੈਂਟ 28/8/22

ਇਕ ਉਤਾਰਾ ਉੱਪ ਸਕੱਤਰ ਵਿੱਤ (ਜੇ) ਅਤੇ ਅਧੀਨ ਸਕੱਤਰ ਵਿੱਤ (ਜਕ), ਸਮੂਹ ਸੁਪਰਡੈਂਟ, ਵਿੱਤ ਖਰਚਾ ਸ਼ਾਖਾਵਾਂ ਅਤੇ ਸੁਪਰਡੈਂਟ ਵਿੱਤ ਬਜਟ-2 ਸ਼ਾਖਾ ਨੂੰ ਸੂਚਨਾ ਅਤੇ ਅਗਲੇਰੀ ਲੋੜੀਂਦੀ ਕਾਰਵਾਈ ਹਿੱਤ ਭੇਜਿਆ ਜਾਂਦਾ ਹੈ।

ਜ. ਜ. ਕੌਰ  
ਸੁਪਰਡੈਂਟ 28/8/22

ਸੇਵਾ ਵਿਖੇ

1. ਉਪ ਸਕੱਤਰ ਵਿੱਤ (ਜੇ)।
2. ਅਧੀਨ ਸਕੱਤਰ ਵਿੱਤ (ਜਕ)।
3. ਸਮੂਹ ਸੁਪਰਡੈਂਟ ਵਿੱਤ ਖਰਚਾ ਸ਼ਾਖਾਵਾਂ।
4. ਸੁਪਰਡੈਂਟ, ਵਿੱਤ ਬਜਟ-2 ਸ਼ਾਖਾ।

ਅੰ:ਵਿ:ਪੰ:ਨੰ: FD-FB-101/09/2021-5FB1/402778 ਮਿਤੀ, ਚੰਡੀਗੜ੍ਹ:02 ਅਗਸਤ, 2022

ਕਾਪੀ:

ਨਿੱਜੀ ਸਕੱਤਰ/ ਪ੍ਰਮੁੱਖ ਸਕੱਤਰ ਵਿੱਤ  
ਨਿੱਜੀ ਸਹਾਇਕ/ ਵਿਸ਼ੇਸ਼ ਸਕੱਤਰ ਵਿੱਤ



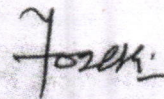
No-14014/5/2021-PFMS/C.No-8766/1898  
Government of India  
Ministry of Finance, Dept. of Expenditure  
Controller General of Accounts  
Public Financial Management System (HQ)  
3rd Floor Shivaji Stadium Annexe  
New Delhi-110001

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 3<sup>rd</sup> 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-



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

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](mailto:incident@cert-in.org.in) and [incident@nic-cert.nic.in](mailto: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.

\*\*\*\*\*