ZONAL ACCOUNTS OFFICE
OFFICE OF THE PRINCIPAL CHIEF CONTROLLER OF ACCOUNTS
CENTRAL BOARD OF DIRECT TAXES
4th FLOOR, AAYAKAR BHAWAN, BASHEERBAGH, HYDERABAD 500004
PHONE.NO 040- 23425589/23236512(fax) email: zaohyd.cbdt@nic.in

Lr. No ZAO/CBDT/HYD/PC/2019-20/PFMS ID
Dated : 10/12/2019

To

The Pr. CIT (Admin)
O/o the Pr. CCIT, Hyderabad
10th Floor, Income Tax Towers,
Masab Tank,
Hyderabad – 500004

Sir,

Sub: New procedure has been introduced by PFMS for new ID User registration and approval in PFMS wef 10.12.2019 – reg.

I am to inform you that a new procedure has been introduced for new sanction ID User Registration and approval in PFMS with effect from 10/12/2019 in view of the security aspects. It is mandatory for every user to have gov.in or nic.in mail id and a valid mobile number to receive communication from PFMS portal. The existing users i.e., PD, DDO, DDO Maker, DDO Checker etc., who did not give their Gov.in/nic.in mail ID in PFMS portal have been rejected by PFMS with effect from 10/12/2019.

The new users and the users rejected by PFMS have to follow the detailed procedure as laid down in ANNEXURE-‘A’ for log in to PFMS portal. After creation of user as per Annexure-‘A’, the hierarchy of approval authority is given Annexure-‘B’ in respect of each user (copy enclosed) and accordingly the users have to get the approval for getting new login credentials.

It is, therefore requested to bring this new procedure to the notice of all the offices under the jurisdiction of Pr. CCIT, Hyderabad.

Yours faithfully,

(A. SRINIVAS)
Sr. Accounts Officer,
Pre-Check Section,
O/o the ZAO, CBDT, Hyderabad

Encl: as above
1. Every user is required to change the password upon his/her first login in PMS.

2. User needs to keep the password safe and not to share it with anyone.

3. The password must be changed after each login to ensure security.

4. The password cannot be the same as the previous one.

5. The password must be strong and not easily guessable.

6. The password must be kept confidential and not shared with anyone.

7. The password must be changed regularly to ensure security.

8. The password must be kept safe and not shared with anyone.

9. The password must be changed after each login to ensure security.

10. The password must be strong and not easily guessable.

11. The password must be kept confidential and not shared with anyone.

12. The password must be changed regularly to ensure security.

13. The password must be kept safe and not shared with anyone.

14. The password must be changed after each login to ensure security.
<table>
<thead>
<tr>
<th>SI NO</th>
<th>USER ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CCA</td>
</tr>
<tr>
<td>2</td>
<td>Root</td>
</tr>
<tr>
<td>3</td>
<td>P. Accounts Officer</td>
</tr>
<tr>
<td>4</td>
<td>CCA</td>
</tr>
<tr>
<td>5</td>
<td>P. Accounts Officer</td>
</tr>
<tr>
<td>6</td>
<td>P. Accounts Officer</td>
</tr>
<tr>
<td>7</td>
<td>P. Accounts Officer</td>
</tr>
<tr>
<td>8</td>
<td>Pay &amp; Accounts Officer</td>
</tr>
<tr>
<td>9</td>
<td>Drawing &amp; Disbursing Officer</td>
</tr>
<tr>
<td>10</td>
<td>DDO Maker</td>
</tr>
<tr>
<td>11</td>
<td>DDO User</td>
</tr>
<tr>
<td>12</td>
<td>Programme Division Checker</td>
</tr>
<tr>
<td>13</td>
<td>D/O PFR/CEO</td>
</tr>
<tr>
<td>14</td>
<td>OAC (PFR)</td>
</tr>
<tr>
<td>15</td>
<td>OAC (PD)</td>
</tr>
</tbody>
</table>

**Legend**

- CCA: Company Controller
- Root: Root User
- P. Accounts Officer: Pay & Accounts Officer
- Drawing & Disbursing Officer
- DDO Maker
- DDO User
- Programme Division Checker
- D/O PFR/CEO
- OAC (PFR)
- OAC (PD)

**Notes**

- The table represents the user creation/approval hierarchy.
- Annexure - B