पेंशन निधि विनियामक और
विकास प्राधिकरण
बी–14/ए, छत्रपति शिवाजी भवन,
कुतुब संस्थागत क्षेत्र,
कटवारिया सराय, नई दिल्ली–110016
दूरभाष : 011-26517501, 26517503, 26133730
फैक्स : 011-26517507
वेबसाईट : www.pfrda.org.in

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY
B-14/A, Chhatrapati Shivaji Bhawan,
Qutub Institutional Area,
Katwaria Sarai, New Delhi-110016
Ph : 011-26517501, 26517503, 26133730
Fax : 011-26517507
Website : www.pfrda.org.in

Advisory

F. No.: PFRDA/17/08/11/0009/2017-SUP-SG-Part (1) **03.06.2020**

To,

All Central Government Ministries & Departments/ State Governments
PrAOs, PAOs, CDDOs, NCDDOs - CG Nodal offices
DTAs, DTOs, DDOs - SG Nodal offices
All Central and State Autonomous Bodies

Advisory on Digital Safety Practices to be followed by Govt Nodal offices to access CRA system under NPS architecture

The function of nodal office/s in the Government Sector i.e. Central and State Governments including Central and State Autonomous Bodies in relation to National Pension System (NPS) is of paramount importance and vital as it begins with subscriber registration and continues till the authorization of exits/withdrawals request of the subscriber-employees. To enable the Nodal offices to fulfill such function/role in the CRA system, the Nodal offices have been provided with the separate maker-checker login-IDs to access the CRA-system.

However, it has come to the notice of the Authority that in certain instances, the maker-checker login-IDs provided by the CRAs to the Nodal office/s for accessing the CRA system to initiate/process and authorize various requests submitted by the subscribers-employees has been used by the unauthorized official/staff of such Nodal offices, i.e., other than the officials authorized to access the CRA-system under the NPS architecture.

Keeping in view the above, all the nodal officers in the Government Sector i.e. Central Government/Ministries/Departments and State Governments including Central and State Autonomous Bodies are hereby advised to follow the following Digital Safety Practices under the NPS architecture while accessing the CRA System :-

1. To maintain absolute confidentiality and integrity of all records, data and information including subscriber's personal information, contribution and claims data;

2. To use at least 8 characters or more to create a password. The more number of characters, Special Symbols, Number we use, the more secure is our password;

3. Users are responsible for safeguarding their User Id and Passwords and must not share passwords/Digital token with other persons;

4. To change the password once in three/four weeks or when you suspect someone knows the password;

5. The access to CRA system should be done by officials of the Nodal office so authorized and Passwords/login details etc. are not be shared with the unauthorised personnel;

6. Do not access files without the permission of the owner. Use maker and checker to monitor what data is being copied or modified in contribution/claims file;

7. Users should not intentionally use the computers to retrieve or modify the information of self/others, which may include password information, claims data, contribution data, withdrawal request, PRAN details etc.;

8. Antivirus software can help to detect and remove viruses from your computer, only if you keep the antivirus software up-to-date. Set firewall and antivirus is to scan actively all the files downloaded/uploaded;

9. Scan all the files after you download whether from websites or links received from e-mails;

10. Always update Web Browser with latest patches. Never click web links in e-mail and no bank will ask you to update the accounts through online;

11. To carefully process/verify the exit/withdrawal request.

Sumeet Kaur Kapoor
Chief General Manager