



कार्यालय ,रक्षा लेखा नियंत्रक
नं. 1स्टाफ रोड, सिकिंदराबाद-500 009
Office of the Controller Of Defence Accounts
No.1 Staff Road, Secunderabad-500 009
(Phone No.:040-27843385/7957)
Email : cda-secd@nic.in

75
आज़ादी का
अमृत महोत्सव

सं./No. NPS/GEN/CORR/2023-24

दिनांक/ Date: 03.04.2023

परिपत्र/CIRCULAR

सेवा में,/To

1. व.ले.अ/ले.अ.,जी.ई(र.ले.नि., सिंकंदराबाद के अधीन)/SAO/AOsGEGs (under CDA SECBAD)
2. व.ले.अ/ले.अ(प्रशा/वेतन) स्थानीय/SAO/AO (AN PAY) Local
3. उप-नियंत्रक, क्षेत्रीय लेखा कार्यालय(थलसेना), वैजाग/The DCDA AAO Army Vizag
4. व.ले.अ/ले.अ(वेतन) स्थानीय/SAO/AO (Pay Sn) Local
5. र.ले.नि., सिंकंदराबाद के अधीन सभी रक्षा संवितरण कार्यालय/All DDO's under CDA SECBAD
6. र.ले.नि., सिंकंदराबाद के अधीन सभी उप-कार्यालय/All Sub Offices under CDA SECBAD

विषय: राष्ट्रीय पेंशन प्रणाली संरचना के अधीन केंद्रीय अभिलेख अनुरक्षण एजेंसी("CRA") द्वारा प्रदत्त तकनीकी प्लेटफॉर्म/सिस्टम तक पहुंचने के लिए सरकारी नोडल कार्यालयों द्वारा अपनाने जाने योग्य "डिजिटल सुरक्षा प्रथाओं" पर दिशा-निर्देश - के संबंध में

Subject: Advisory on "Digital Safety Practices to be followed by Govt. Nodal offices to access technological platform/system provided by Central Record keeping Agencies ("CRA") under NPS architecture. - reg.

उपरोक्त विषय पर पें.नि.वि.वि.प्रा(PFRDA) के दिनांक 22.02.2023 के पत्रांक PFRDA/17/08/11/0024/2017-SUP-CG-Part(1) की एक प्रति आपकी सूचना, मार्गदर्शन और आवश्यक अनुपालन के लिए संलग्न है।

A copy of PFRDA letter No. PFRDA/17/08/11/0024/2017-SUP-CG-Part(1) dated 20.02.2023 on the subject mentioned above is enclosed herewith for information, guidance and necessary compliance please.

(Handwritten signature)
(जी.धनलक्ष्मी, भा.र.ले.से)
उप-नियंत्रक(एन.पी.एस)

प्रतिलिपि: Copy to:

वरिष्ठ लेखा अधिकारी/The SAO

आई.टी अनुभाग/ IT Section --- र.ले.नि., सिंकंदराबाद की वेबसाइट पर अपलोड करने के।
For uploading on CDA Secunderabad Website.

(Handwritten signature)
व.ले.अ(एन.पी.एस)

Advisory

F.No. PFRDA/17/08/11/0024/2017-SUP-CG-Part(1)

20.03.2023

To,

Nodal offices of Central and State Governments and
Nodal offices of Autonomous Bodies

Subject: Advisory on "Digital Safety Practices to be followed by Govt Nodal offices to access technological platform/system provided by Central Recordkeeping Agencies ("CRA") under NPS architecture

विषय: एनपीएस प्रणाली के अंतर्गत केंद्रीय अभिलेखापाल अभिकरण ("सीआरए") द्वारा प्रदान किए गए तकनीकी प्लेटफॉर्म/तंत्र के अभिगम हेतु सरकारी नोडल कार्यालयों द्वारा पालन किए जाने वाली डिजिटल सुरक्षा सलाह

1. This is in reference to PFRDA's communication on the captioned subject dated 03.06.2020 issued vide file no. PFRDA/17/08/11/0009/2017-SUP-SG-Part(1) and dated 29.09.2021 issued vide file no. PFRDA/17/08/11/0014/2017-SUP-SG-Part(1) (copy enclosed).

यह उक्त विषय पर पीएफआरडीए के संचार दिनांक 03.06.2020 फाइल सं. पीएफआरडीए/17/08/11/0009/2017-एसयूपी-एसजी-पार्ट(1) और संचार दिनांक 29.09.2021, फाइल सं. पीएफआरडीए/17/08/11/0014/2017-एसयूपी-एसजी-पार्ट(1) के संदर्भ में है।(प्रतिलिपि संलग्न)

2. The function of nodal office/s in the Government Sector i.e. Central and State Governments including Autonomous Bodies thereunder, with respect to the 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 fulfil such function/role in the CRA system, the Nodal offices have been provided with separate maker-checker login IDs to access the CRA system so that any single user is not able to unilaterally execute the transaction.

राष्ट्रीय पेंशन प्रणाली (एनपीएस) के संबंध में, सरकारी क्षेत्र (केंद्रीय और राज्य सरकारों एवं स्वायत्त निकायों सहित) में नोडल कार्यालयों का कार्य सर्वोपरि और महत्वपूर्ण है क्योंकि यह ग्राहक पंजीकरण के साथ प्रारंभ होता है और ग्राहक-कर्मचारियों के निकास/निकासी अनुरोध के अनुमति प्रदान करने तक जारी रहता है। नोडल कार्यालयों को सीआरए सिस्टम में इस तरह के कार्य/भूमिका को पूरा करने में सक्षम बनाने के लिए, नोडल कार्यालयों को सीआरए

सिस्टम के अभिगम हेतु अलग से मेकर-चेकर लॉगिन आईडी प्रदान की गई है ताकि कोई भी अकेला यूजर लेनदेन को एकतरफा अंजाम न दे सके।

3. Taking the Authority's endeavour forward of providing ease of transacting through post-pandemic digital/technological tools/enhancement, together with security and safeguard of the interest of the NPS subscriber against digital threats/frauds, it is advised that adequate precautions and safety measures to be ensured at the level of nodal offices.

डिजिटल खतरों/धोखाधड़ी के खिलाफ एनपीएस सब्सक्राइबर के हितों की सुरक्षा और सुरक्षा के साथ-साथ महामारी के बाद के डिजिटल/तकनीकी उपकरणों/संवर्द्धन के माध्यम से लेनदेन को आसान बनाने के प्राधिकरण के प्रयास को आगे बढ़ाते हुए, यह सलाह दी जाती है कि नोडल कार्यालयों के स्तर पर पर्याप्त सावधानियां और सुरक्षा उपाय सुनिश्चित किए जाएं।

4. All the nodal offices/officers in the Central Government Sector (including autonomous bodies), are hereby advised to follow the Digital Safety Practices under the NPS architecture as per the advisory mentioned at point number 1 while accessing the CRA System. The important safety measures are as under: -

केंद्र सरकार के क्षेत्र (स्वायत्त निकायों सहित) के सभी नोडल कार्यालयों/अधिकारियों को एतद्वारा सलाह दी जाती है कि वे सीआरए सिस्टम का उपयोग करते समय बिंदु संख्या 1 में उल्लिखित सलाह के अनुसार एनपीएस संरचना के तहत डिजिटल सुरक्षा प्रथाओं का पालन करें। महत्वपूर्ण सुरक्षा उपायों को निम्नानुसार है: -

- a) To maintain absolute confidentiality and integrity of all records, data and information including subscriber's personal information, contribution and claims data;
अभिदाता की व्यक्तिगत जानकारी, योगदान और दावों के डेटा सहित सभी रिकॉर्ड, डेटा और जानकारी की पूर्ण गोपनीयता और अखंडता बनाए रखना;
- b) To use at least 8 characters or more to create a password. The more characters, Special Symbols, and numbers we use, the more secure is our password;
पासवर्ड बनाने के लिए कम से कम 8 अक्षरों या अधिक का उपयोग करें। हम जितने अधिक वर्णों, विशेष प्रतीकों और संख्याओं का उपयोग करते हैं, हमारा पासवर्ड उतना ही अधिक सुरक्षित होता है;
- c) Users are responsible for safeguarding their User Id and Passwords and must not share passwords/Digital token with other persons;
उपयोगकर्ता अपने उपयोगकर्ता आईडी और पासवर्ड की सुरक्षा के लिए जिम्मेदार हैं और उन्हें अन्य व्यक्तियों के साथ पासवर्ड/डिजिटल टोकन साझा नहीं करना चाहिए;
- d) To change the password once in four weeks or when you suspect someone knows the password or when one Nodal officer is transferred and another nodal officer joins in. Also, the passwords should be kept confidential and are not to be written anywhere;

निष्कर्ष

तीन/चार सप्ताह में एक बार या जब आपको संदेह हो कि कोई आपका पासवर्ड जानता है, पासवर्ड बदलें; या जब एक नोडल अधिकारी को स्थानांतरित किया जाता है और दूसरा नोडल अधिकारी शामिल होता है। साथ ही, पासवर्ड को गोपनीय रखा जाना चाहिए और कहीं भी लिखा नहीं जाना चाहिए;

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

सीआरए प्रणाली तक पहुंच केवल नोडल कार्यालय के अधिकृत अधिकारियों द्वारा की जानी चाहिए और पासवर्ड/लॉगिन विवरण आदि अनधिकृत कर्मियों के साथ साझा नहीं किए जाते हैं;

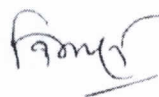
- f) The login IDs provided to Nodal offices by the CRAs, in the capacity of maker and checker for initiation/verification or authorization of transactions in the CRA systems needs to be accessed by separate officials individually and one person should not be given access to more than one login ID;

सीआरए सिस्टम में लेन-देन की शुरुआत/सत्यापन या प्राधिकरण के लिए मेकर और चेकर की हैसियत से सीआरए द्वारा नोडल कार्यालयों को प्रदान की गई लॉगिन आईडी को अलग-अलग अधिकारियों द्वारा व्यक्तिगत रूप से एक्सेस करने की आवश्यकता होती है और एक व्यक्ति को इससे अधिक तक पहुंच नहीं दी जानी चाहिए। एक लॉगिन आईडी;

- g) The Nodal offices are advised to maintain a "Log Book/record" to ensure that there is no unauthorized access of the Login IDs given by CRAs. The said Log book/record may specify inter alia the Name of the official/staff/personnel who have been provided with the login IDs & passwords for accessing the system and the record of subsequent change in the allocation of said Login IDs. Also, the responsibility of the transactions processed/authorized in the CRA system through the given Login IDs shall lie with the officials/staff/personnel to whom such Login IDs have been allocated at the time of these transactions;

नोडल कार्यालयों को सलाह दी जाती है कि वे यह सुनिश्चित करने के लिए कि सीआरए द्वारा दी गई लॉगिन आईडी तक कोई अनधिकृत पहुंच नहीं है, एक "लॉग बुक/रिकॉर्ड" बनाएं। उक्त लॉग बुक/रिकॉर्ड में अन्य बातों के साथ-साथ अधिकारी/कर्मचारियों/कार्मिक का नाम निर्दिष्ट किया जा सकता है, जिन्हें सिस्टम के अभिगम हेतु लॉगिन आईडी और पासवर्ड प्रदान किए गए हैं और उक्त लॉगिन आईडी के आवंटन में बाद के बदलाव का रिकॉर्ड है। साथ ही, दिए गए लॉगिन आईडी के माध्यम से सीआरए सिस्टम में संसाधित/प्राधिकृत लेनदेन की जिम्मेदारी उन अधिकारियों/कर्मचारियों/कार्मिकों की होगी जिन्हें इन लेनदेन के समय ऐसी लॉगिन आईडी आवंटित की गई है;

- h) 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;



अधिकृत व्यक्ति की अनुमति के बिना फाइलों तक न पहुंचें। अंशदान/दावे फ़ाइल में कौन से डेटा की प्रतिलिपि बनाई जा रही है या संशोधित की जा रही है, इसकी निगरानी के लिए मेकर और चेकर का उपयोग करें;

- i) 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.;;
उपयोगकर्ताओं को जानबूझकर स्वयं/दूसरों की जानकारी को पुनः प्राप्त करने या संशोधित करने के लिए कंप्यूटर का उपयोग नहीं करना चाहिए, जिसमें पासवर्ड की जानकारी, दावा डेटा, योगदान डेटा, निकासी अनुरोध, PRAN विवरण आदि शामिल हो सकते हैं;
- j) 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 to scan actively all the files downloaded/uploaded;
एंटीवायरस सॉफ़्टवेयर आपके कंप्यूटर से वायरस का पता लगाने और उसे हटाने में तभी मदद कर सकता है, जब आप एंटीवायरस सॉफ़्टवेयर को अप-टू-डेट रखते हैं। डाउनलोड/अपलोड की गई सभी फाइलों को सक्रिय रूप से स्कैन करने के लिए है फ़ायरवॉल और एंटीवायरस सेट करें;
- k) Scan all the files after you download whether from websites or links received from e-mails;
वेबसाइट या ई-मेल से प्राप्त लिंक से डाउनलोड करने के बाद सभी फाइलों को स्कैन करें;
- l) Always update Web Browser with latest patches. Never click web links in e-mail and no financial institution will ask you to update the accounts through online;
वेब ब्राउजर को हमेशा नवीनतम पैच के साथ अपडेट करें। ई-मेल में कभी भी वेब लिंक पर क्लिक न करें और कोई भी वित्तीय संस्था आपको ऑनलाइन के माध्यम से खातों को अपडेट करने के लिए नहीं कहेगा;
- m) Nodal officers to carefully process all financial and non-financial transactions including the exit/withdrawal request/ change in any KYC/ Bank detail/ ERM transaction and ensure that funds are remitted to Bank account, authorised to receive that amount;
नोडल अधिकारी सभी वित्तीय और गैर-वित्तीय लेन-देन को सावधानीपूर्वक संसाधित करें, जिसमें निकास/निकासी अनुरोध/किसी भी केवाईसी/बैंक विवरण/ईआरएम लेनदेन में परिवर्तन शामिल है और यह सुनिश्चित करें कि उस राशि को प्राप्त करने के लिए अधिकृत बैंक खाते में धन भेजा गया है;
- n) The nodal offices to carefully verify all financial and non-financial transactions including the exit/withdrawal request/ change in any KYC/ Bank detail/

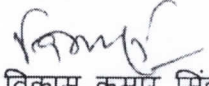
किम्प

ERM transaction and ensure that funds are remitted to Bank account, authorised to receive that amount;

नोडल कार्यालय सभी वित्तीय और गैर-वित्तीय लेन-देन को सावधानीपूर्वक सत्यापित करें, जिसमें निकास/निकासी अनुरोध/किसी भी केवाईसी/बैंक विवरण/ईआरएम लेनदेन में परिवर्तन शामिल है और यह सुनिश्चित करें कि धनराशि उस बैंक खाते में भेजी जाती है, जो उस राशि को प्राप्त करने के लिए अधिकृत है;

- o) The Nodal office may carry out regular audits to scrutinize whether the digital safety practices as advised by the Authority are being followed in letter and spirit.

नोडल कार्यालय यह जांचने के लिए नियमित ऑडिट कर सकता है कि प्राधिकरण द्वारा सलाह दी गई डिजिटल सुरक्षा प्रथाओं का अक्षरशः पालन किया जा रहा है या नहीं।


(Vikas Kumar Singh)/ विकास कुमार सिंह)

Chief General Manager/ मुख्य महाप्रबंधक



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
वेबसाइट : 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/17/08/11/0014/2017-SUP-SG-Part (1)

29.09.2021

To,

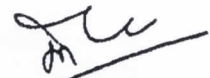
All Central Government Ministries & Departments/ State Governments
PrAOs, PAOs, CDDOs, NCDDOs - CG Nodal offices
DTAs, DTOs, DDOs - SG Nodal offices
All Central and State Autonomous Bodies

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

This is in further to the PFRDA's communication no. PFRDA/17/08/11/0009/2017-SUP-SG-Part (1) dated 03.06.2020. (Copy attached)

2. In continuation to the same, all the Government Sector Nodal offices are hereby advised to adopt the following additional digital safety practices while accessing the System of the Central Record Keeping Agencies (CRAs):
 - a. The login IDs provided to Nodal offices by the CRAs, in the capacity of maker and checker for initiation/verification or authorization of transactions in the CRA systems needs to be accessed by separate officials individually and one person should not be given access to more than one login ID.
 - b. The Nodal offices are advised to maintain a "Log Book/record" to ensure that there is no unauthorized access of the Login IDs given by CRAs. The said Log book/record may specify *inter alia* the Name of the official/staff/personnel who have been provided with the login IDs & passwords for accessing the system and the record of subsequent change in the allocation of said Login IDs. Also, the responsibility of the transactions processed/authorized in the CRA system through the given Login IDs shall lie with the officials/staff/personnel to whom such Login IDs have been allocated at the time of these transactions.
 - c. Nodal offices are advised to ensure that passwords of the said Login-IDs are protected and are changed frequently in line with the advisory dated 03/06/2020 issued by the Authority. Additionally, it is to be ensured that the passwords to the Login IDs are changed, whenever there is a change in the official handling the same. Also, the passwords should be kept confidential and are not to be written anywhere.

- d. The Nodal office may carry out regular audits to scrutinize whether the digital safety practices as advised by the Authority are being followed in letter and spirit.
3. The following checks and controls are enabled in the CRA system to pre-empt any breach of the system by unauthorized persons with malafide intention.
 - a. Execution of service requests after it has been authorized by two separate officials in the maker checker mode so that any single user is not able to unilaterally execute the transaction.
 - b. Hard coded bank details in the CRA system which can be changed only after such a service request has been authorized by a senior DTA/PrAO level official, post the maker activity. Further, pursuant to the execution of any such bank account detail change request, the system does not allow any ERM request to be processed for 30 days from the date of execution of such change.
 - c. The official carrying out the verification of the ERM request shall ensure that the bank details displayed at the time of requesting the ERM are the same as those which have been authorized to receive the amount.
 - d. On initiation and completion of any ERM request, a system generated email/SMS is sent to concerned Nodal Office/Subscriber intimating of the initiated / completed ERM transaction.



Sumeet Kaur Kapoor
Chief General Manager



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
वेबसाइट : 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.



Sumet Kaur Kapoor
Chief General Manager