वैज्ञानिक तथा औद्योगिक अनुसंधान परिषद्
COUNCIL OF SCIENTIFIC & INDUSTRIAL RESEARCH
अनुसंधान भवन, 2, रफी मार्ग, नई दिल्ली.110 001
Anusandhan Bhawan, 2, Rafi Marg, New Delhi- 110 001

सा./एनपीएस/1/24-25

दिनांक/Dated:08.04.2024
Dated

प्रेषक:वित्त सलाहकार
From: Financial Adviser

सेवा में : सीएसआईआर की सभी राष्ट्रीय प्रयोगशाला/संस्थान/मुख्यालय/एककों के वरिष्ठ वित एवं लेखा नियंत्रक, वित एवं लेखा नियंत्रक, वित एवं लेखा अधिकारी,अनुभाग अधिकारी(वित एवं लेखा)

To : The Sr.COFA/COFA/FAO/SO (F&A) of all CSIR Labs/Instts/Hqrs/Units

विषय: पीएफआरडीए(एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श,2024

Subject: PFRDA(digital Safety Practices for Government Nodal Offices Under NPS Architecture)Advisory,2024.

महोदया/महोदय Madam/Sir,

मुझे उपरोक्त विषय पर पेंशन निधि विनियामक विकास प्राधिकरण से प्राप्त पत्र संख्या- पीएफ़आरडीए/17-18/08/11/0001/2024-एसयूपी-एसजी दिनांक 27.03.2024 आपकी जानकारी,मार्गदर्शन और अनुपालन के लिए अग्रेसित करने का निर्देश हुआ है।

I am directed to forward herewith the Pension Fund Regulatory and Development Authority letter No-PFRDA/17-18/08/11/0001/2024-SUP-SG dated 27.03.2024 on the above mentioned subject for your information, guidance and compliance.

भवदीय/Yours faithfully,

Enclosure:- यथोपरि/As Above

मनोज कुमार 8/4/24

मनोज कुमार/ Manoj Kumar
वित एवं लेखा अधिकारी(निधि व पेंशन)
Finance & Accounts Officer (Fund & Pension)

प्रतिलिपि/Copy to:-
1)सीएसआईआर वैबसाइट/CSIR Website
2)कार्यालय प्रति/Office Copy.

पेंशन निधि विनियामक और विकास प्राधिकरण

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

भारत 2023 INDIA

File No.: PFRDA-17/08/11/0001/2024-SUP-SG Date:27.03.2024

To,

All PrAOs/PAOs/DDOs of Central Government & CABs

All DTAs/DTOs/DDOs of State Government & SABs under National Pension System Architecture

प्रिय महोदय/महोदया,	Dear Sir/Madam,
विषय: पीएफआरडीए (एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024	**Subject: PFRDA (Digital Safety Practices for Government Nodal Offices Under NPS Architecture) Advisory, 2024**
कृपया संलग्न पेंशन निधि विनियामक और विकास प्राधिकरण (एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024 के सम्बन्ध में पीएफआरडीए का परिपत्र संख्या पीएफआरडीए/2024/07/एसयूपी-सीजीएसजी/01 दिनांकित २७.०३.२०२४ प्राप्त करें।	Please find enclosed PFRDA's circular no. PFRD A/2024/ 0U SUP-CGSG/O1 dated 27.03.2024 regarding the PFRDA (Digital Safety Practices for Government Nodal Offices Under NPS Architecture) Advisory, 2024.
2. आपसे अनुरोध है कि उपरोक्त को अपने अंतर्निहित नोडल कार्यालयों के सभी संबंधित अधिकारियों तक प्रसारित करें।	2. It is requested to kindly disseminate the above advisory to all the concerned officials of your underlying nodal offices.

सादर /Yours Sincerely,

(विकास कुमार सिंह)/(Vikas Kumar Singh)

मुख्य महा प्रबंधक /Chief General Manager

बी–14/ए, छत्रपति शिवाजी भवन, कुतुब संस्थागत क्षेत्र, कटवारिया सराय, नई दिल्ली–110016
दूरभाष : 011–26517501, 26517503, फैक्स : 011–26517507, वेबसाईट : www.pfrda.org.in
B-14/A, Chhatrapati Shivaji Bhawan, Qutub Institutional Area, Katwaria Sarai, New Delhi-110016
Phone : 011-26517501, 26517503, Fax : 011-26517507, Website : www.pfrda.org.in

Azadi Ka Amrit Mahotsav
आज़ादी का अमृत महोत्सव

परिपत्र

परिपत्र संख्या : पीएफआरडीए/2024/07/एसयूपी-सीजीएसजी/01 27.03.2024

प्रति,

राष्ट्रीय पेंशन प्रणाली के अंतर्गत
केंद्र सरकार एवं इसके स्वायत्त निकायों के सभी PrAOs/PAOs/DDOs;
राज्य सरकारों एवं इनके स्वायत्त निकायों के सभी DTAs/DTOs/DDOs

विषय: पेंशन निधि विनियामक और विकास प्राधिकरण (एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024

प्राधिकरण राष्ट्रीय पेंशन प्रणाली के तहत सभी सरकारी नोडल कार्यालयों के मार्गदर्शन के लिए पेंशन निधि विनियामक और विकास प्राधिकरण (एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024 (संलग्न) जारी करता है।

यह प्राधिकरण की वेबसाइट (www.pfrda.org.in) पर भी उपलब्ध है।

सादर,

(विकास कुमार सिंह)
मुख्य महाप्रबंधक

पेंशन निधि विनियामक और विकास प्राधिकरण

(एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024

विषयवस्तु :

शब्दावली 2

अध्याय- I- संक्षिप्त शीर्षक और प्रारंभ, उद्देश्य और प्रयोज्यता 3

1. संक्षिप्त शीर्षक और प्रारंभ : 3
2. उद्देश्य: 3
3. प्रयोज्यता: 3

अध्याय II- एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों द्वारा अपनाई जाने वाली डिजिटल सुरक्षा प्रथाएं 3

4. क्रेडेंशियल्स का उपयोग करते समय सुरक्षा उपाय: 3
5. एनपीएस से संबंधित लेनदेन/गतिविधियों को संसाधित करते समय डिजिटल सुरक्षा उपाय और सावधानियां: 4

अध्याय III- सामान्य दिशानिर्देश .... **Error! Bookmark not defined.**

7. सामान्य दिशानिर्देश: 6

अध्याय-IV- सर्वोत्तम प्रथाएँ .... Error! Bookmark not defined.

8. एनपीएस के अंतर्गत प्रदान की गई लॉगिन-आईडी के लिए पासवर्ड प्रबंधन: 7
9. ईमेल संचार: .... Error! Bookmark not defined.
10. कंप्यूटर के उपयोग 8
11. इंटरनेट ब्राउज़िंग: .... **Error! Bookmark not defined.**

अध्याय-V- वसूली और क्षतिपूर्ति 10

संदर्भ 10

शब्दावली

अधिनियम	पेंशन निधि विनियामक और विकास प्राधिकरण अधिनियम 2013
सीएबी	केंद्रीय स्वायत्त निकाय
सीआरए	केंद्रीय अभिलेखपाल अभिकरण
सीजी	केंद्र सरकार
डीडीओ	आहरण एवं संवितरण कार्यालय
डीटीए	कोषागार एवं लेखा निदेशालय
डीटीओ	जिला कोषागार कार्यालय
एनपीएस	राष्ट्रीय पेंशन प्रणाली
पीआरएओ	प्रधान लेखा कार्यालय
पीएओ	वेतन एवं लेखा कार्यालय
पीएफआरडीए / प्राधिकरण	पेंशन निधि विनियामक और विकास प्राधिकरण
पीआरएएन / प्रान	स्थायी सेवानिवृत्ति खाता संख्या
एसएबी	राज्य स्वायत्त निकाय
एसजी	राज्य सरकार

पेंशन निधि विनियामक और विकास प्राधिकरण (एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024

अध्याय-I- संक्षिप्त शीर्षक और प्रारंभ, उद्देश्य और प्रयोज्यता

1. **संक्षिप्त शीर्षक और प्रारंभ :**

1.1. इन परामर्शों को पेंशन निधि विनियामक और विकास प्राधिकरण (एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024 कहा जाएगा।

1.2. इस परामर्श को साइबर सुरक्षा और डिजिटल सुरक्षा प्रथाओं पर आधारित किसी भी अन्य दिशानिर्देश के साथ, जो संगठन में लागू हो या जिसका पालन करना बाध्यकारी हो, विवक्षित और कार्यान्वित किया जाना है।

2. **उद्देश्य :**

एक व्यापक रणनीति स्थापित करना, जो एनपीएस के स्थापत्य के अंतर्गत विभिन्न गतिविधियों के संचालन के लिए चिह्नित किए गए केंद्र/राज्य सरकार (इसके अंतर्गत स्वायत्त निकायों सहित) के नोडल कार्यालयों द्वारा एनपीएस से संबंधित गतिविधियों का संचालन करने के लिए सीआरए द्वारा प्रदान किए गए डिजिटल प्लेटफार्मों का उपयोग करने के दौरान संभावित खतरों से बचाव करने, गोपनीय आंकड़ों की सुरक्षा करने और नैतिक डिजिटल सुरक्षा प्रथाओं को प्रोत्साहित करने के लिए इष्टतम पद्धतियों, निर्देशात्मक पहलों और प्राथमिक कार्यों को एकीकृत करती हो। इस परामर्श का उद्देश्य पंजीकरण, एनपीएस खाता रखरखाव और निकास/प्रत्याहरण जैसे विभिन्न स्तरों पर नोडल कार्यालयों द्वारा एनपीएस से संबंधित विभिन्न गतिविधियों का प्रदर्शन करते समय डिजिटल सुरक्षा के लिए मानक स्थापित करके और एनपीएस से संबंधित विभिन्न गतिविधियों का पालन करते हुए डिजिटल सुरक्षा के ज्ञान से लोगों को लैस करके एनपीएस स्थापत्य के अंतर्गत डिजिटल सुरक्षा जागरूकता की संस्कृति को बढ़ावा देना है।

3. **प्रयोज्यता :**

यह परामर्श, एनपीएस स्थापत्य के अंतर्गत अपने कार्यों के लिए केंद्र और राज्य सरकारों (इसके अंतर्गत स्वायत्त निकायों सहित) के नोडल कार्यालयों पर लागू MHA/MEITY और Cert-In द्वारा जारी साइबर सुरक्षा और अन्य संबंधित दिशानिर्देशों से जुड़ी हुई है और किसी भी तरह से किसी अधिकारी द्वारा उसके कर्तव्य के निर्वहन में हुए कृताकृत्य और चूक के लिए उसकी देयता को न्यून नहीं करती है।

अध्याय II- एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों द्वारा अपनाई जाने वाली डिजिटल सुरक्षा प्रथाएं

4. **क्रेडेंशियल्स का उपयोग करने के दौरान सुरक्षा उपाय :**

एनपीएस के संबंध में सरकारी क्षेत्र अर्थात केंद्र और राज्य स्वायत्त निकायों सहित केंद्र / राज्य सरकारों में नोडल कार्यालय (कार्यालयों) का कार्य सर्वोपरि और महत्त्वपूर्ण है क्योंकि यह अभिदाता पंजीकरण से आरम्भ होकर अभिदाता-कर्मचारियों के निकास/प्रत्याहरण अनुरोधों के प्राधिकृत होने तक जारी रहता है। नोडल कार्यालयों द्वारा सीआरए प्रणाली में ऐसे कार्य/भूमिका की पूर्ति में सक्षम बनाने के लिए, नोडल कार्यालयों को सीआरए प्रणाली का उपयोग करने हेतु अलग मेकर-चेकर लॉगिन आईडी प्रदान की गई है। उपर्युक्त के अलावा, एनपीएस स्थापत्य के अंतर्गत सीआरए प्रणाली का उपयोग करते समय, निम्नलिखित 'डिजिटल सुरक्षा प्रथाओं' का अनुपालन किया जाना है-

4.1. संबंधित कार्यालय/सरकारी विभाग में विभिन्न पदानुक्रम वाले कर्मचारियों/अधिकारियों को आईडी (मेकर और चेकर) का आवंटन (वरिष्ठ अधिकारी को चेकर होना चाहिए)

4.2. एक "लॉग बुक/अभिलेख" का निर्माण जिससे यह सुनिश्चित किया जा सके कि सीआरए द्वारा प्रदत्त लॉगिन आईडी का कोई अनधिकृत उपयोग नहीं किया जा रहा है। उक्त लॉग बुक/अभिलेख में अन्य बातों के साथ-साथ उन अधिकारी/स्टाफ/कर्मियों का नाम निर्दिष्ट किया जाए जिन्हें प्रणाली का उपयोग करने के लिए लॉगिन आईडी और पासवर्ड प्रदान किए गए हैं और उक्त लॉगिन आईडी के आवंटन में होने वाले परिवर्तनों को भी दर्ज किया जाए। साथ ही, प्रदत्त लॉगिन आईडी के माध्यम से सीआरए प्रणाली में संसाधित/प्राधिकृत लेनदेनों की जिम्मेदारी उन अधिकारियों/कर्मचारियों/कर्मियों की होगी जिन्हें लेनदेन के समय ऐसी लॉगिन आईडी आवंटित की गई है।

4.3. उपयोगकर्ताओं को स्वयं/दूसरों की जानकारी को पुनः प्राप्त करने या संशोधित करने के लिए इरादतन कंप्यूटर का ऐसा उपयोग नहीं करना चाहिए, जिसमें पासवर्ड की जानकारी, दावे के आंकड़े, अंशदान के आंकड़े, प्रत्याहरण के अनुरोध, प्रान विवरण आदि शामिल हों;

4.4. एंटीवायरस सॉफ़्टवेयर आपके कंप्यूटर में वायरस का पता लगाने और उन्हें हटाने में तभी मदद कर सकता है, जब आप एंटीवायरस सॉफ़्टवेयर को अद्यतन रखते हों। डाउनलोड/अपलोड की गई सभी फ़ाइलों को सक्रिय रूप से स्कैन करने के लिए फ़ायरवॉल और एंटीवायरस को सेट किया जाए;

4.5. सीआरए प्रणाली का उपयोग नोडल कार्यालय के प्राधिकृत अधिकारियों द्वारा किया जाना चाहिए, ताकि पासवर्ड/लॉगिन विवरण आदि अनधिकृत कर्मियों के साथ साझा न किए जा सकें;

4.6. अभिदाता की व्यक्तिगत जानकारी, अंशदान और दावों के आंकड़ों सहित सभी अभिलेख, आंकड़े और सूचनाओं की पूर्ण गोपनीयता और अखंडता बनाए रखा जाना चाहिए;

4.7. उपयोगकर्ता अपने यूजर आईडी और पासवर्ड की सुरक्षा के लिए जिम्मेदार होंगे और उन्हें अन्य व्यक्तियों के साथ पासवर्ड/डिजिटल टोकन साझा नहीं करना चाहिए;

4.8. चार सप्ताह में एक बार पासवर्ड बदला जाना चाहिए या जब किसी को पासवर्ड पता चलने का संदेह हो गया हो या जब किसी नोडल अधिकारी का तबादला हुआ हो और प्रणाली में दूसरा नोडल अधिकारी शामिल हुआ हो, तब पासवर्ड बदला जाना चाहिए । साथ ही, पासवर्ड गोपनीय रखे जाने चाहिए और उन्हें कहीं भी प्रकट नही किया जाना चाहिए।

4.9. लॉगिन क्रेडेंशियल्स, अर्थात यूजर आईडी और पासवर्ड का उपयोग और सुरक्षा के अलावा, डिजिटल टोकन/ओटीपी के माध्यम से आधार-आधारित प्रमाणीकरण जैसे किसी भी अतिरिक्त सुरक्षा उपाय का उपयोग भी केवल अधिकृत व्यक्ति द्वारा किया जाएगा और सुरक्षा की जिम्मेदारी केवल उसी अधिकारी की होगी।

4.10. निकास/प्रत्याहरण अनुरोध/ किसी केवाईसी/बैंक विवरण/ईआरएम लेनदेन में परिवर्तन सहित सभी वित्तीय और गैर-वित्तीय लेनदेन को सावधानीपूर्वक संसाधित / सत्यापित करना।

4.11. लेनदेनों को निष्पादित करने और अनुमोदित करने के लिए जिन अधिकारियों को सीआरए प्रणाली क्रेडेंशियल सौंपे गए हैं, उन्हें सीआरए प्रणाली में स्थापित प्रमाणीकरण प्रक्रिया सहित निर्धारित प्रक्रिया का पालन करना आवश्यक है।

4.12. नोडल कार्यालय यह जांच करने के लिए नियमित अंकेक्षण कर सकता है कि प्राधिकरण द्वारा सुझाए गए डिजिटल सुरक्षा प्रथाओं का अक्षरशः पालन किया जा रहा है अथवा नहीं।

4.13. सभी वित्तीय/गैर-वित्तीय लेनदेनों को सेवा अभिलेख के माध्यम से आवश्यक सावधानी बरतने के बाद ही संसाधित किया जाना चाहिए और अभिदाता अनुरोध प्रपत्रों के साथ आवश्यक सहायक दस्तावेजों को सीआरए प्रणाली में, जहां भी लागू हो, अनिवार्य रूप से अपलोड किया जाना चाहिए।

5. **एनपीएस से संबंधित लेनदेन/गतिविधियों को संसाधित करते समय डिजिटल सुरक्षा उपाय और सावधानी :** नोडल कार्यालय, निकासी सहित सीआरए प्रणाली में संसाधित लेनदेन के लिए पूरी तरह से जिम्मेदार होंगे। तदनुसार, एनपीएस की पूरी समयसीमा यानी पंजीकरण, रखरखाव और निकास/दावा निपटान के दौरान सभी लेनदेन केवल अभिदाता के पूरी तरह से संतुष्ट होने के बाद ही संसाधित किए जाएँगे।

5.1 अभिदाता की ऑनबोर्डिंग के दौरान

5.1.1. दस्तावेजों का डिजिटलीकरण और उन्हें सीआरए प्रणाली में अपलोड करते समय, अभिदाता द्वारा प्रदान किए गए अभिदाता पंजीकरण फॉर्म और सहायक केवाईसी विवरणों के अनुसार जानकारी को सहायक आधिकारिक वैध दस्तावेजों ("ओवीडी") और कर्मचारी के सेवा अभिलेख में उपलब्ध जानकारी के साथ सत्यापित किया जाएगा।

5.1.2. सीआरए प्रणाली में प्रस्तुत/अनुमोदन से पहले समुचित सावधानी/प्रमाणन के साथ-साथ उपयोगकर्ता द्वारा सीआरए प्रणाली में एनपीएस से संबंधित गतिविधियों/लेनदेन को बिना किसी विचलन के संसाधित करते समय सीआरए प्रणाली के चरणवार निर्देशों का पालन किया जाएगा।

5.2. अभिदाता रखरखाव गतिविधियाँ

5.2.1. डिजिटलीकरण और सीआरए प्रणाली में अपलोड करते समय, नामांकन, अभिदाता प्रोफाइल, जैसे नाम परिवर्तन, पते में परिवर्तन, मोबाइल नंबर में परिवर्तन, पीएफ और निवेश के लिए विकल्प, बैंक खाता विवरण सहित किसी भी अनुरोध पर मानकों के अनुसार अपेक्षित समर्थन दस्तावेज के साथ उचित सत्यापन के बाद अभिदाता से प्राप्त अनुरोध के अनुसार डिजिटल प्रमाणीकरण (जैसे आधार प्रमाणीकरण) के साथ उसे संसाधित और अनुमोदित किया जाएगा।

5.2.2. अद्यतन/परिवर्तन अनुरोधों के लिए विलंबित और गलत प्रसंस्करण के कानूनी/वित्तीय प्रभाव पड़ सकते हैं।

5.3. निकास और प्रत्याहरण/दावा

5.3.1. सीआरए प्रणाली पर निकास/प्रत्याहरण अनुरोध निष्पादित करते समय, अभिदाता/दावेदार द्वारा प्रदान की गई जानकारी को सहायक दस्तावेजों और कर्मचारी के सेवा अभिलेख में उपलब्ध जानकारी के साथ सत्यापित किया जाएगा।

5.3.2. सीआरए प्रणाली में प्रस्तुत/अनुमोदन से पहले डिजिटल प्रमाणीकरण (जैसे आधार प्रमाणीकरण) में समुचित सावधानी/प्रमाणन के साथ-साथ अभिदाताओं/दावेदारों के निकास/प्रत्याहरण/दावा अनुरोधों को बिना किसी विचलन के संसाधित करते समय सीआरए प्रणाली के निर्देशों का पालन करना होगा।

6. अन्य उपाय :

6.1. सीआरए प्रणाली का उपयोग करने के लिए द्विस्तरीय प्रमाणीकरण (2एफए) लागू करना- 2FA के माध्यम से पासवर्ड के परे सुरक्षा की एक अतिरिक्त परत जोड़ी जाती है, जिसमें आमतौर पर उपयोगकर्ताओं द्वारा जानकारी के एक द्वितीयक स्तर को प्रदान करना होता है, जैसे कि उनके मोबाइल डिवाइस पर भेजा गया कोड। इस सुविधा को बिना किसी विचलन के लागू करके उसका अनुपालन किया जा सकता है।

6.2. नियमित सुरक्षा अपडेट पर बल : एंटीवायरस सॉफ़्टवेयर और फ़ायरवॉल को नियमित रूप से अपडेट किया जाना चाहिए। इसके अलावा, कमजोरियों को दुरुस्त करने और प्रणाली में उभरते खतरों से बचने के लिए नियमित अपडेट आवश्यक हैं, इसलिए आवश्यक अपडेट सुनिश्चित किए जा सकते हैं।

6.3. आंकड़ों के उल्लंघन से निपटने पर मार्गदर्शन : आंकड़ा उल्लंघनों की रिपोर्टिंग और उन्हें कम करने के लिए स्पष्ट प्रोटोकॉल स्थापित किए जाने चाहिए ताकि उनके प्रभाव या सुरक्षा घटनाओं को न्यूनतम किया जा सके।

6.4. सुरक्षा प्रशिक्षण : नियमित प्रशिक्षण सत्र से सुरक्षा सर्वोत्तम प्रथाओं को सुदृढ़ करने में मदद मिलती है और यह सुनिश्चित किया जाता है कि कर्मचारी उभरते खतरों के प्रति सतर्क रहें।

6.5. पैठ का परीक्षण और भेद्यता आकलन : नोडल कार्यालयों को सुरक्षा कमजोरियों की सक्रिय रूप से पहचान करना और उन्हें दूर करने के लिए नियमित रूप से पैठ का परीक्षण या भेद्यता का आकलन करना होगा।

अध्याय III- सामान्य दिशानिर्देश

7. सामान्य दिशानिर्देश :

7.1. एनपीएस स्थापत्य के अंतर्गत नोडल कार्यालयों के कार्यों के लिए आंतरिक साइबर सुरक्षा नीति को विकसित और कार्यान्वित करना।

7.1.1. एक व्यापक साइबर सुरक्षा नीति विकसित करना जो राष्ट्रीय मानकों और दिशानिर्देशों के साथ संरेखित हो।

7.1.2. डिजिटल सुरक्षा सुनिश्चित करने के लिए एनपीएस से संबंधित नोडल कार्यालयों की स्पष्ट भूमिकाओं और जिम्मेदारियों से युक्त एक अभिशासन ढांचा स्थापित करना।

7.1.3. उभरते साइबर खतरों और कमजोरियों को दूर करने के लिए नीति की समय-समय पर समीक्षा और इसे अद्यतन किया जाना।

7.2. नेटवर्क और अवसंरचना सुरक्षा

7.2.1. सुरक्षित नेटवर्क अवसंरचना और अभिगम नियंत्रण स्थापित करना।

7.2.2. फ़ायरवॉल, घुसपैठ का पता लगाने और रोकथाम प्रणाली, और सुरक्षा सूचना और इवेंट मैनेजमेंट (SIEM) सिस्टम जैसे सतत निगरानी उपकरण लागू करना।

7.2.3. संभावित भेद्यता को चिह्नित करने और उन्हें दूर करने के लिए नेटवर्क उपकरणों, अनुप्रयोगों और सेवाओं के नियमित भेद्यता आकलन और उनके पैठ का परीक्षण करना।

7.2.4. राउटर, स्विच और फायरवॉल जैसे सभी नेटवर्क घटकों के सुरक्षित कॉन्फ़िगरेशन स्थापित करना।

7.3. अभिगम/उपयोग नियंत्रण

7.3.1. आंकड़ों और प्रणाली के अनधिकृत उपयोग को रोकने के लिए अभिगम तंत्र को सख्ती से नियंत्रित करना।

7.3.2. मजबूत पासवर्ड नीतियों और बहु-कारक प्रमाणीकरण तंत्र को लागू करना।

7.3.3. न्यूनतम विशेषाधिकार के सिद्धांत के आधार पर अभिगम विशेषाधिकार प्रदान करना।

7.3.4. नियमित रूप से समीक्षा करना और अनावश्यक अभिगम विशेषाधिकारों को हटाना।

7.4. सुरक्षा जागरूकता और प्रशिक्षण

7.4.1. कर्मचारियों के लिए नियमित साइबर सुरक्षा जागरूकता कार्यक्रम आयोजित करना।

7.4.2. संवेदनशील सूचना को संभालने और उसकी सुरक्षा के लिए सर्वोत्तम प्रथाओं पर कर्मचारियों को प्रशिक्षित करना।

7.4.3. फ़िशिंग और सामाजिक अभियंत्रण हमलों जैसे सामान्य साइबर खतरों के बारे में कर्मचारियों को शिक्षित करना।

7.5. रिपोर्टिंग और सहयोग

7.5.1. सुरक्षा संबंधी घटनाओं को तुरंत रिपोर्ट करने के लिए तंत्र स्थापित करना।

7.5.2. खतरे की खुफिया जानकारी और सर्वोत्तम प्रथाओं को साझा करने के लिए साइबर सुरक्षा के लिए जिम्मेदार अन्य केंद्रीकृत एजेंसियों के साथ सहयोग करना।

अध्याय-IV- सर्वोत्तम प्रथाएँ

8. एनपीएस के अंतर्गत प्रदान की गई लॉगिन-आईडी के लिए पासवर्ड प्रबंधन :

अनधिकृत उपयोग ऐसे किसी भी व्यक्ति के लिए एक बड़ी समस्या है, जो कंप्यूटर या स्मार्टफोन या टैबलेट जैसे डिवाइस का उपयोग करते हैं। इन ब्रेक-इन से प्रभावित व्यक्तियों के लिए मूल्यवान आंकड़ों का नुकसान जैसे वर्गीकृत जानकारी, व्यक्तिगत आंकड़ों या अनधिकृत लेनदेन का निष्पादन, वित्तीय नुकसान आदि संभावित परिणामों में शामिल हैं। सरल और आमतौर पर उपयोग किए जाने वाले पासवर्ड से घुसपैठियों को कंप्यूटिंग डिवाइस तक आसानी से पहुंचने और उसका नियंत्रण प्राप्त करने में मदद मिल जाती है। किसी पासवर्ड को सेट और प्रबंधित करते समय कुछ सर्वोत्तम प्रथाएँ निम्नलिखित हैं,

8.1. आदर्श रूप से न्यूनतम 10 अक्षरों वाला एक मजबूत पासवर्ड बनाएं, जिसमें अक्षर, संख्या और वर्ण शामिल हों।

8.2. सभी पासवर्ड (जैसे, ईमेल, कंप्यूटर, आदि) को हर तीन महीने में कम से कम एक बार बदला जाना चाहिए।

8.3. पुराने पासवर्ड का पुन: उपयोग न करें।

8.4. पासवर्ड को कंप्यूटर, नोटबुक, नोटिस बोर्ड, या किसी अन्य स्थान पर, जहां अनधिकृत व्यक्ति उन्हें खोज सकते हैं या उनका उपयोग कर सकते हैं, पठनीय रूप नहीं रखा जाना चाहिए ।

8.5. पासवर्ड को संवेदनशील जानकारी माना जाए और इसे किसी के साथ साझा न किया जाए।

8.6. आपके पास मौजूद प्रत्येक लॉग-इन खाते के लिए हमेशा अलग-अलग पासवर्ड का उपयोग करें। यदि आपके द्वारा उपयोग की जाने वाली कोई साइट हैक हो जाती है तो, एक से अधिक खातों के लिए एक ही पासवर्ड का उपयोग करने के कारण कई जोखिमों का खतरा बना रहता है ।

8.7. जहां भी एप्लीकेशन द्वारा "पासवर्ड याद रखें" सुविधा को संकेत दिया जाता है, वहां इसके उपयोग को हमेशा अस्वीकार करें।

8.8. ध्यान दें कि, कमजोर पासवर्ड का रूप निम्नानुसार होता है :
- ऐसे पासवर्ड में 10 से कम अक्षर होते हैं।
- ऐसा पासवर्ड किसी शब्दकोश (अंग्रेजी या विदेशी) में पाया जाने वाला कोई सामान्य शब्द होता है।
- ऐसा पासवर्ड एक सामान्य उपयोग वाला शब्द होता है जैसे परिवार, पालतू जानवरों, दोस्तों, सहकर्मियों, चलचित्र / उपन्यास / कॉमिक्स पात्रों आदि के नाम, कंप्यूटर की शब्दावली और नाम, कमांड, साइटें, कंपनियां, हार्डवेयर और सॉफ्टवेयर।
- जन्मदिन और अन्य व्यक्तिगत जानकारी जैसे पता और फोन नंबर।
- शब्द या संख्या पैटर्न जैसे 123456, aaaaaa, qwerty, asdfg, zxcvb आदि।

9. ईमेल संचार :

नोडल कार्यालयों द्वारा ईमेल संचार के लिए कुछ सर्वोत्तम प्रथाएँ निम्नलिखित हैं :

9.1.1. आधिकारिक संचार के लिए केवल सरकार द्वारा प्रदत्त ईमेल पतों का उपयोग करें (जैसे nic ईमेल)।

9.1.2. सिस्टम व्यवस्थापक किसी भी आधिकारिक संचार के लिए व्यक्तिगत ईमेल के उपयोग को प्रतिबंधित करने के लिए उचित नियंत्रण लागू कर सकते हैं।

9.1.3. अज्ञात या अविश्वसनीय स्रोतों से ईमेल में प्राप्त संदिग्ध लिंक पर क्लिक करने या ईमेल अटैचमेंट डाउनलोड करने से बचें।

9.1.4. वर्गीकृत जानकारी ईमेल के माध्यम से संप्रेषित नहीं की जानी चाहिए। किसी आकस्मिक स्थिति में, सक्षम प्राधिकारी का अनुमोदन लेना चाहिए।

9.1.5. सार्वजनिक वाई-फाई कनेक्शन द्वारा आधिकारिक ईमेल खातों का प्रयोग करने से बचें।

9.1.6. ईमेल खातों के लिए पासवर्ड का ऑटो-सेव सक्षम नहीं होना चाहिए।

9.1.7. अपना कार्य पूरा होने के बाद मेल खातों से लॉग आउट करें।

9.1.8. उपयोगकर्ता को ईमेल में प्राप्त लिंक पर क्लिक करने के बजाय ब्राउज़र में पूरा URL टाइप करना चाहिए।

9.1.9. किसी भी संदिग्ध ई-मेल/ ईमेल के अटैचमेंट को न खोलें/न फॉरवर्ड करें/न जवाब दें।

10. कंप्यूटर के उपयोग :

दैनिक आधार पर कंप्यूटर के उपयोग के लिए कुछ सर्वोत्तम प्रथाएँ निम्नलिखित हैं :

10.1 आपके संगठन द्वारा उपयोग के लिए अनुमत एंटीवायरस सॉफ़्टवेयर का उपयोग करके कंप्यूटर्स को वायरस/वर्म से सुरक्षित किया जाना चाहिए।

10.2 सुनिश्चित करें कि आपका ऑपरेटिंग सिस्टम, एप्लिकेशन और एंटी-वायरस सॉफ़्टवेयर सहित सॉफ़्टवेयर पैच अद्यतित हों; और आपके कंप्यूटर में ऑटो अपडेट चालू हो।

10.3 स्क्रीन पर संवेदनशील जानकारी के साथ कंप्यूटर को खुला न छोड़ें।

10.4 अनधिकृत पहुंच को रोकने के लिए कार्यस्थल छोड़ने से पहले हमेशा अपने कंप्यूटर को लॉक करें। उपयोगकर्ता Ctrl + alt +del" दबाकर और "इस कंप्यूटर को लॉक करें" या "विंडो बटन + L" चुनकर कंप्यूटर को लॉक कर सकता है।

10.5 पासवर्ड-सुरक्षित स्क्रीन सेवर सक्षम करें ताकि असुरक्षित छोड़े गए कंप्यूटर भी सुरक्षित रहें।

10.6 अपने कंप्यूटर में प्लग करने के दौरान सावधान रहें। मैलवेयर संक्रमित यूएसबी ड्राइव, बाहरी हार्ड ड्राइव और स्मार्टफोन के माध्यम से भी प्रसारित हो सकता है।

10.7 कंप्यूटर पर लॉगिन करने के लिए गैर-व्यवस्थापक खाता विशेषाधिकारों का उपयोग करें और दिन-प्रतिदिन के उपयोग के लिए व्यवस्थापक विशेषाधिकारों का उपयोग करने से बचें।

10.8 आंकड़ों का बहुत सावधानी से उपयोग करें और जानकारी को सुरक्षित रखने के लिए एन्क्रिप्शन का उपयोग करें।

11. इंटरनेट ब्राउज़िंग :

इंटरनेट पर ब्राउज़ करते समय ध्यान देने योग्य कुछ सर्वोत्तम प्रथाएँ निम्नलिखित हैं :

11.1. किसी लिंक पर क्लिक करते समय या डाउनलोड करते समय हमेशा सावधान रहें। यदि यह किसी भी कारण से अप्रत्याशित या संदिग्ध है, तो उस पर क्लिक न करें।

11.2. अपने सिस्टम व्यवस्थापक/विभाग द्वारा अनुमत फाइलों/सॉफ्टवेयर के अलावा किसी अन्य स्रोत से किसी भी प्रकार की फाइल/सॉफ्टवेयर डाउंनलोड न करें।

11.3. ऐसे वेब ब्राउज़र का उपयोग करें जिसे आपके संगठन द्वारा अनुमति दी गई हो।

11.4. ब्राउज़िंग के लिए हमेशा अपडेट किए गए वेब ब्राउज़र का उपयोग करें।

11.5. इंटरनेट से जुड़े किसी भी उपकरण पर कोई भी जानकारी संग्रहीत/साझा न करें।

11.6. यदि लॉगिन स्क्रीन पर जानकारी दर्ज करने के बाद एक विंडो दिखाई देती हो, जो आपको "पासवर्ड सहेजें" विकल्प का चयन करने के लिए कहती हो, तो ब्राउज़र में संकेतित उस विकल्प का उपयोग नहीं किया जाना चाहिए । खाता जानकारी, जैसे पासवर्ड या क्रेडिट कार्ड जानकारी को वेब ब्राउज़र में संग्रहीत न करें, विशेष रूप से उन कम्प्यूटरों पर जो अन्य उपयोगकर्ताओं द्वारा उपयोग में लाए जाते हों।

11.7. ब्राउज़र एड्रेस बार में HTTPS चिह्न देखें। "https" में "s" का अर्थ सुरक्षा से है, जिसका अर्थ है कि वेबसाइट एसएसएल एन्क्रिप्शन को नियोजित कर रही है। यह सत्यापित करने के लिए कि कोई साइट सुरक्षित है या नहीं, अपने ब्राउज़र के बार में हरे रंग के पैडलॉक आइकन के साथ "https:" की जांच करें।

11.8. प्रत्येक लॉगआउट के बाद ब्राउज़र से उसके इतिहास को मिटाने की आदत डालें।

11.9. सरकार की कोई भी वर्गीकृत जानकारी को निजी क्लाउड सेवाओं (Google ड्राइव, ड्रॉपबॉक्स, iCloud आदि) पर संग्रहीत नहीं किया जाना चाहिए और ऐसा करने से आप डेटा-लीकेज के शिकार हो सकते हैं।

11.10. दौरे में, उन सेवाओं का उपयोग करने से बचें जिनके लिए स्थान की जानकारी देनी होती है, जब तक कि कार्यालय कर्तव्यों के निर्वहन के लिए यह आवश्यक न हो।

11.11. ब्राउज़ करते समय, कुछ पॉप-अप क्लोज बटन के विकल्प के साथ दिखाई दे सकते हैं। ये नकली हो सकते हैं और क्लिक करने से स्पाइवेयर का खतरा हो सकता है।अतः, ऐसे पॉप-अप से सावधान रहें और उस पर क्लिक करने से बचें।

11.12. ब्राउज़र में पॉपअप ब्लॉकर विकल्प को चालू रखा जाना चाहिए और यदि आवश्यक हो तो चुनिंदा रूप से विश्वसनीय साइटों के लिए अनुमति दी जानी चाहिए।

11.13. ध्यान दें कि इंटरनेट पर निशुल्क चीजें यदाकदा ही उपलब्ध होती हैं। "फ्री" स्क्रीनसेवर आदि में अक्सर मैलवेयर होते हैं। अतः ऐसे ऑनलाइन निशुल्क छूटों से सतर्क रहें।

11.14. किसी भी वित्तीय या संवेदनशील लेनदेन के लिए सार्वजनिक कंप्यूटर और सार्वजनिक वाई-फाई कनेक्शन का उपयोग करने से बचें। ऐसे कंप्यूटरों पर सरकारी ईमेल एक्सेस करने से सूचना भंग होने का खतरा रहता है।

11.15. यदि आपकी सेवा के दौरान आपको कुछ सूचना प्रणालियों को सुरक्षित रूप से प्रयोग करने की आवश्यकता होती है, तो इसके लिए इंटरनेट पर एमपीएलएस लिंक, वीपीएन आदि जैसे सुरक्षा नियंत्रणों का उपयोग करने की सलाह दी जाती है।

अध्याय-V- वसूली और क्षतिपूर्ति

12. नोडल कार्यालय किसी भी साइबर सुरक्षा में चूक के कारण हुए अभिदाता के नुकसान की क्षतिपूर्ति और बहाली के उद्देश्य से एनपीएस से संबंधित आंतरिक नीति तैयार करने पर भी विचार कर सकता है। इस संबंध में, नोडल कार्यालय प्रभावित पक्षों को क्षतिपूर्ति प्रदान करने के लिए साइबर उल्लंघनों के कारण हुई मौद्रिक हानि, यदि कोई हो, की वसूली के लिए उपयुक्त नीति या दिशानिर्देशों के साथ-साथ संबंधित प्रक्रियाओं और मानक संचालन प्रक्रियाओं को स्थापित करने के लिए संबंधित प्रशासनिक विभाग/मंत्रालय/राज्य सरकार के साथ मामले को उठा सकते हैं। इसके अतिरिक्त, नोडल कार्यालय अपने उपभोक्ता के हित में, शामिल राशि की वसूली के अलावा दोषी व्यक्तियों के विरुद्ध उपयुक्त कार्रवाई भी कर सकता है।

संदर्भ

यह परामर्श MHA/MEITY और Cert-In द्वारा जारी साइबर सुरक्षा और अन्य संबंधित दिशानिर्देशों से जुड़ा हुआ है और किसी भी तरह से अधिकारी द्वारा उसके कर्तव्यों के निर्वहन के दौरान हुए कृताकृत्य या चूक की देयता को न्यून नहीं करता है। अतः, इस मामले पर विस्तृत मार्गदर्शन के लिए निम्नलिखित का सन्दर्भ लिया जा सकता है।

(i). सूचना सुरक्षा सर्वोत्तम अभ्यास (गृह मंत्रालय द्वारा))- https://www.mha.gov.in/sites/default/files/Documents_InformationSecurity_25062019.pdf.

(ii). सूचना प्रौद्योगिकी (उचित सुरक्षा प्रथाओं और प्रक्रियाओं और संवेदनशील व्यक्तिगत आंकड़े या सूचना) नियम, 2011- https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

(iii). सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश-भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (सीईआरटी-इन) द्वारा जारी, इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार - https://www.meity.gov.in/writereaddata/files/Guidelines%20on%20Information%20Security%20Practices%20for%20Government%20Entities.pdf

संदर्भ के लिए पीएफआरडीए द्वारा जारी परिपत्र

1. परिपत्र दिनांक 12.04.2023 – "एनपीएस स्थापत्य के अंतर्गत केंद्रीय अभिलेखपाल अभिकरणों ("सीआरए") द्वारा प्रदान किए गए तकनीकी प्लेटफॉर्म/प्रणाली का उपयोग करने के लिए सरकारी नोडल कार्यालयों द्वारा अपनाई जाने वाली डिजिटल सुरक्षा प्रथाओं" पर परामर्श : https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2558

2. परिपत्र दिनांक 15.06.2022 - सीईआरटी-इन द्वारा जारी साइबर सुरक्षा निर्देश और अक्सर पूछे जाने वाले प्रश्न https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2190

3. परिपत्र दिनांक 15.06.2022 - साइबर जागरुकता दिवस (सीजेडी)

CIRCULAR

CIRCULAR No.: PFRDA/2024/07/SUP-CGSG/01 27.03.2024

To,

All PrAOs/PAOs/DDOs of Central Government & CABs;

All DTAs/DTOs/DDOs of State Government & SABs under National Pension System Architecture.

Subject: Pension Fund Regulatory and Development Authority (Digital Safety Practices for Government Nodal Offices under NPS Architecture) Advisory, 2024

Authority hereby issues, Pension Fund Regulatory and Development Authority (Digital Safety Practices for Government Nodal Offices under NPS Architecture) Advisory, 2024 (enclosed) for guidance of all the Govt Nodal Offices under NPS.

The same is also available on the website of Authority (www.pfrda.org.in).

Yours Sincerely,

(Vikas Kumar Singh)

Chief General Manager

एनपीएस स्थापत्य के अंतर्गत सरकारी नोडल कार्यालयों के लिए पीएफआरडीए डिजिटल सुरक्षा प्रथाएँ) परामर्श, 2024

https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2189

4. परिपत्र दिनांक 22.02.2023 - एनपीएस अभिदाताओं के लाभ के लिए निकास और वार्षिकी के समानांतर प्रसंस्करण को सक्षम करने के लिए प्रत्याहरण/केवाईसी दस्तावेजों को अनिवार्य रूप से अपलोड करना https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2506

5. परिपत्र दिनांक 20.02.2024 - सरकारी क्षेत्र के अंतर्गत सीआरए प्रणाली के आधार-आधारित उपयोग के माध्यम से एनपीएस लेनदेन को सुरक्षित करना
https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2903

6. परिपत्र दिनांक 12.01.2024 - राष्ट्रीय पेंशन प्रणाली (एनपीएस) के अंतर्गत संचित पेंशन धन का आंशिक प्रत्याहरण
https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2860

******

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

(DIGITAL SAFETY PRACTICES FOR GOVERNMENT NODAL OFFICES UNDER NPS ARCHITECTURE) Advisory, 2024

PFRDA DIGITAL SAFETY PRACTICES FOR GOVERNMENT NODAL OFFICES UNDER NPS ARCHITECTURE) ADVISORY, 2024

Contents

GLOSSARY 2

CHAPTER- I- SHORT TITLE AND COMMENCEMENT, OBJECTIVE AND APPLICABILITY 3

1. Short title and commencement: 3
2. Objective: 3
3. Applicability: 3

CHAPTER II- DIGITAL SAFETY PRACTICES TO BE FOLLOWED BY GOVT NODAL OFFICES UNDER NPS ARCHITECTURE 3

4. Safety Measures while utilising credentials: 3
5. Digital Safety Measures and Precaution while processing NPS-related transactions/activities: 5

CHAPTER III- GENERAL DIRECTION 6

7. General Direction: 6

CHAPTER-IV- BEST PRACTICES 7

8. Password Management for login-IDs provided under NPS: 7
9. Email Communications: 8
10. Computer Usage: 8
11. Internet Browsing: 8

CHAPTER-V- RECOVERY AND INDEMNIFICATION 9

REFERENCES 10

GLOSSARY

Act	Pension Fund Regulatory and Development Authority Act 2013
CAB	Central Autonomous Body
CRA	Central Recordkeeping Agency
CG	Central Government
DDO	Drawing & Disbursing Office (DDO)
DTA	Directorate of Treasuries and Accounts
DTO	District Treasury Office
NPS	National Pension System
PrAO	Principle Accounts Office
PAO	Pay and Accounts Office
PFRDA/Authority	Pension Fund Regulatory and Development Authority
PRAN	Permanent Retirement Account Number
SAB	State Autonomous Body
SG	State Government

PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY DIGITAL SAFETY PRACTICES FOR GOVERNMENT NODAL OFFICES UNDER NPS ARCHITECTURE) ADVISORY, 2024

CHAPTER- I- SHORT TITLE AND COMMENCEMENT, OBJECTIVE AND APPLICABILITY

1. Short title and commencement:

   1.1. These advisories may be called the Pension Fund Regulatory and Development Authority (Digital Safety Practices for Government Nodal Offices Under NPS Architecture) Advisory, 2024.

   1.2. This advisory is to be construed and acted upon, together with any other guidelines on cyber security and digital safe practices, as may be applicable in the organization or which it is obliged to follow.

2. Objective:

To establish a comprehensive strategy that integrates optimal methodologies, instructional initiatives, and pre-emptive actions to address possible hazards, safeguard confidential data, and encourage ethical digital safety practices while accessing the digital platforms provided by CRA to conduct the activities related to NPS by the nodal offices of Central/State Government (including autonomous bodies under it) identified for conducting various activities under the architecture of NPS. This advisory aim to encourage fostering a culture of digital safety awareness under NPS architecture by equipping people with the knowledge to keep the digital safe by establishing norms for digital safety and following the best practices while performing various activities related to NPS by the nodal offices at various levels such as registration, NPS account maintenance and during exit/withdrawals.

3. Applicability:

This advisory shall apply to the nodal offices of Central and State Governments (including autonomous bodies under it) for their functions under the architecture of the NPS. This advisory is in addition to the Cybersecurity and other related guidelines issued by MHA/MEITY and Cert-In and in no way reduces the liability of the officer for any omission or commission in the discharge of their duties.

CHAPTER II- DIGITAL SAFETY PRACTICES TO BE FOLLOWED BY GOVT NODAL OFFICES UNDER NPS ARCHITECTURE

4. Safety Measures while utilising credentials:

The function of nodal office(s) in the Government Sector i.e. Central State Governments including Central and State Autonomous Bodies in relation to NPS is of paramount importance and vital as it begins with subscriber registration and continues till the authorization of exits/withdrawal requests 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 separate maker-checker login IDs to access the CRA system. Apart from the above, the following 'Digital Safety Practices' may be followed under the NPS architecture while accessing the CRA System-

4.1. Allotment of the IDs (maker and checker) to employees/officials having different levels of hierarchy (the checker being the senior official) in the concerned office/Government Department.

4.2. 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 changes in the allocation of said Login IDs. Also, the responsibility for 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.

4.3. 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 requests, PRAN details, etc.;

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

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

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

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

4.8. 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.

4.9. Apart from usage and safeguarding the login credentials, i.e. user ID and password any additional safety measures such as Aadhaar-based authentication through digital token/OTP is also to be used only by the authorised person and responsibility for safeguarding shall lie on him/her only.

4.10. To carefully process/verify all financial and non-financial transactions including the exit/withdrawal request/ change in any KYC/ Bank detail/ ERM transaction.

4.11. The officers assigned with the CRA system credentials to execute and approve transactions, are required to adhere to the laid process including authentication process established in CRA system.

4.12. 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.

4.13. All financial/non-financial transactions should be processed only after doing necessary due diligence offline through service records and necessary supporting documents along with the subscriber request forms must be mandatorily uploaded in the CRA system, wherever applicable.

5. Digital Safety Measures and Precaution while processing NPS-related transactions/activities: The Nodal offices are fully responsible for transactions processed in the CRA system including withdrawals. Accordingly, all transactions must be processed only after being fully satisfied with the same during all journey of subscriber, i.e. registration, maintenance and exit/claim settlement.

5.1. While onboarding subscriber

5.1.1. While digitisation and uploading of documents on the CRA system, the information as per the Subscriber Registration form and supporting KYC details, as provided by the subscriber are to be verified with the supporting officially valid documents ("OVDs") and the information available in the service records of the employee.

5.1.2. The step-wise instructions of the CRA system are to be followed by the user while processing NPS-related activities/transactions in the CRA system without deviation, along with proper due diligence/certification before submission/approval in the CRA system.

5.2. Subscriber Maintenance Activities

5.2.1. While digitisation and uploading on the CRA system, any request for update/change in nomination, subscriber profile, such as name change, change in address, change in mobile number, choice for PF& Investments, Bank account detail, including Re-KYC are to be processed and approved along with digital authentication (such as Aadhaar Authentication) as per the request received from the subscriber after due verification with the required supporting document as per norms.

5.2.2. Delayed and incorrect processing for update/change requests may have legal/financial implications.

5.3. Exit and withdrawals/Claims

5.3.1. While executing the Exit/withdrawal request on the CRA system, the information provided by the subscriber/claimant is to be verified with the supporting documents and the information available in the service records of the employee.

5.3.2. The instructions of the CRA system are to be followed by the user while processing Exit/withdrawals/Claims requests of the subscriber/claimants without any deviation, along with proper due diligence/certification with digital authentication (such as Aadhaar Authentication) before submission/approval in the CRA system.

6. Other Measures:

6.1. Implementing two-factor authentication (2FA) for accessing the CRA system. 2FA adds an extra layer of security beyond passwords, typically requiring users to provide a secondary piece of information, such as a code sent to their mobile device. This facility may be implemented and adhered to without deviation.

6.2. Emphasis on Regular Security Updates: The antivirus software and firewalls are to be updated regularly. Also, regular updates are essential to patch vulnerabilities and

protect against emerging threats to the system, hence, necessary updates may be ensured.

6.3. Guidance on Handling Data Breaches: Clear protocols should be established for reporting and mitigating data breaches to minimize their impact or security incidences.

6.4. Security Training: Regular training sessions can help reinforce security best practices and ensure that employees remain vigilant against evolving threats.

6.5. Penetration Testing and Vulnerability Assessments: Nodal office to conduct regular penetration testing or vulnerability assessments to proactively identify and address security weaknesses.

CHAPTER III- GENERAL DIRECTION

7. General Direction:

7.1. Develop and Implement an internal Cyber Security Policy for the functions of nodal offices under NPS architecture.

7.1.1. Develop a comprehensive cyber security policy that aligns with national standards and guidelines.

7.1.2. Establish a governance framework with clear roles and responsibilities of nodal offices related to NPS to ensure digital safety.

7.1.3. The policy should be reviewed and updated periodically to address emerging cyber threats and vulnerabilities.

7.2. Network and Infrastructure Security

7.2.1. Establish secure network infrastructure and access controls.

7.2.2. Implement firewalls, intrusion detection and prevention systems, and continuous monitoring tools such as Security Information and Event Management (SIEM) systems.

7.2.3. Conduct regular vulnerability assessments and penetration testing of network devices, applications, and services to identify and remediate potential vulnerabilities.

7.2.4. Establish secure configurations of all network components like routers, switches, and firewalls.

7.3. Access Control

7.3.1. Strictly control access mechanisms to prevent unauthorized access to data and systems.

7.3.2. Enforce strong password policies and multi-factor authentication mechanisms.

7.3.3. Grant access privileges based on the principle of least privilege.

7.3.4. Regularly review and remove unnecessary access privileges.

7.4. Security Awareness and Training

7.4.1. Conduct regular cyber security awareness programs for employees.

7.4.2. Train employees on best practices for handling and protecting sensitive information.

7.4.3. Educate employees about common cyber threats such as phishing and social engineering attacks.

7.5. Reporting and Collaboration

7.5.1. Establish mechanisms for reporting security incidents promptly.

7.5.2. Collaborate with other centralised agencies responsible for cyber security to share threat intelligence and best practices.

CHAPTER-IV- BEST PRACTICES

8. Password Management for login-IDs provided under NPS:

Unauthorized access is a major problem for anyone who uses a computer or devices such as smartphones or tablets. The possible consequences for victims of these break-ins include the loss of valuable data such as classified information, personal data or execution of unauthorised transactions, financial loss, etc. Simple and commonly used passwords enable intruders to easily gain access and control a computing device. Following are some of the best practices to consider while setting up and managing a password,

8.1. Create a strong password with a minimum length of ideally 10 characters and comprising of mix of alphabets, numbers, and characters.

8.2. All passwords (e.g., email, computer, etc.) should be changed periodically at least once every three months.

8.3. Don't reuse old passwords.

8.4. Passwords should not be stored in readable form in computers, notebooks, notice boards, or in any other location where unauthorized persons might discover or use them.

8.5. Treat passwords as sensitive information and do not share it with anyone.

8.6. Always use different passwords for every log-in account you have. Using the same password for more than one account risks multiple exposures if one site you use is hacked.

8.7. Always decline the use of the "Remember Password" feature wherever it is prompted by the applications.

8.8. Remember weak passwords have the following characteristics:

- The password contains less than 10 characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage words such as Names of family, pets, friends, colleagues, Movie / Novel / Comics characters, etc. Computer terms and names, commands, sites, companies, hardware, and software.
- Birthdays and other personal information such as address and phone numbers.
- Word or number patterns like 123456, aaaaa, qwerty, asdfg, zxcvb, etc.

9. Email Communications:

Following are some of the best practices with email communication by the nodal offices:

9.1.1. Use only Government-provided email addresses for official communications (e.g. nic email).

9.1.2. System administrators may deploy appropriate controls to restrict the use of personal email addresses for any official communications.

9.1.3. Avoid downloading email attachments or clicking on suspicious links received in emails from unknown or untrusted sources.

9.1.4. Classified information be not communicated via emails. In case of emergent requirements to do so, the approval of competent authority should be obtained.

9.1.5. Avoid accessing official email accounts from public Wi-Fi connections.

9.1.6. Auto save of password for email accounts should not be enabled.

9.1.7. Log out from mail accounts after your work is done.

9.1.8. The user should type the complete URL in the browser instead of clicking links received in an email.

9.1.9. Do not open/forward / reply to any suspicious e-mails/attachment of emails.

10. Computer Usage:

Following are some of the best practices for computer use on a day-to-day basis:

10.1. Computers should be protected from viruses/worms using Antivirus software permitted for use by your organization.

10.2. Make sure your operating system, application, and software patches including anti-virus software are up to date; and auto updates are turned on in your computer.

10.3. Don't leave the computer unattended with sensitive information on the screen.

10.4. Always lock your computer before leaving the workplace to prevent unauthorized access. A user can lock the computer by pressing Ctrl +alt +del" and choosing „lock this computer" or "window button+ L".

10.5. Enable a password-protected screen saver so that the computers that were left unsecured will be protected.

10.6. Be careful of what you plug into your computer. Malware can spread through infected USB drives, external hard drives, and even smartphones.

10.7. Use non-administrator account privileges for login to the computer and avoid accessing administrator privileges for day-to-day usage.

10.8. Treat data very carefully and use encryption to encode information securely.

11. Internet Browsing:

Following are some of the best practices to keep in mind when browsing on the Internet:

11.1. Always be careful when clicking on links or downloading. If it's unexpected or suspicious for any reason, don't click on it.

11.2. Do not download any type of files/software from any source other than those allowed by your system administrator/department.

11.3. Use a web browser that has been permitted by your Organization.

11.4. Always use an updated web browser for browsing.

11.5. Do not store/ share any information on any device that is connected to the Internet.

11.6. The "Save password" option prompted by the browser should not be selected if a window appears after entering information on the login screen, asking you to do so. Don't save account information, such as passwords or credit card information in web browsers, especially on those PCs which are shared with other users.

11.7. Look for the HTTPS sign in the browser address bar. The "s" in "https" stands for secure, meaning that the website is employing SSL encryption. Check for an "https:" with a green padlock icon in your browser address bar to verify that a site is secure.

11.8. Make a habit of clearing history from the browser after each logout session.

11.9. No classified information of government can be stored on private cloud services (Google drive, Dropbox, iCloud etc.,) and doing so may expose you for data leakage.

11.10. When on tour, avoid using services that require location information, unless it is necessary for discharge of office duties.

11.11. While browsing, some pop-ups may appear with option of close button. These may be fake and may actually try to install spyware when you click on it. Beware of such pop-ups and avoid clicking on it.

11.12. Popup blocker option should be kept turned ON in the browser and may be selectively allowed for trusted sites, if required.

11.13. Remember that things on the internet are rarely free. "Free" Screensavers etc., often contain malware. So be aware of such online free offers.

11.14. Avoid using public computers and public Wi-Fi connections to access and carry out any financial or sensitive transactions. Accessing government email on such computers has a risk of causing information breaches.

11.15. If your job requires you to access certain information systems securely, it is advisable to use security controls such as MPLS link, VPN over the internet etc., for such access

CHAPTER-V- RECOVERY AND INDEMNIFICATION

12. Nodal office may also consider devising NPS related internal policy for the purpose of indemnification and restitution of loss of the subscriber occurred due to lapse in any cyber security. In this regard, Nodal offices may take up the matter with concerned administrative department/Ministry/State Government for establishing suitable policy or guidelines as well as related processes and standard operating procedures to recover the monetary loss, if any, caused due to cyber breaches for indemnifying the affected parties.

Moreover, in the interest of subscriber nodal office may also undertake suitable action against the guilty persons, apart from recovery of the amount involved.

REFERENCES

This advisory is in addition to the Cybersecurity and other related guidelines issued by MHA/MEITY and Cert-In and in no way reduces the liability of the officer for any omission or commission in the discharge of their duties. Therefore, the following may additionally be referred to for detailed guidance on the matter.

(i). Information Security Best Practices (by Ministry of Home Affairs)- https://www.mha.gov.in/sites/default/files/Documents_InformationSecurity_25062019.pdf.

(ii). Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011- https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

(iii). Guidelines on Information Security Practices for Government Entities-Issued by Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics and Information Technology Government of India- https://www.meity.gov.in/writereaddata/files/Guidelines%20on%20Information%20Security%20Practices%20for%20Government%20Entities.pdf

Circulars issued by PFRDA for reference

1. Circular dated 12.04.2023 - 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. https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2558
2. Circular dated 15.06.2022 - Cyber Security Directions and FAQs issued by CERT-In https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2190
3. Circular dated 15.06.2022 - Cyber Jaagrookta Diwas (CJD) https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2189
4. Circular dated 22.02.2023 - Mandatory upload of Withdrawal/ KYC documents to enable Parallel Processing of Exit and Annuity for the benefit of NPS Subscribers https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2506
5. Circular dated 20.02.2024 - Securing NPS transactions through Aadhaar-based access of CRA system under the Government sector https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2903
6. Circular dated 12.01.2024 - Partial Withdrawal of Accumulated Pension Wealth under the National Pension System (NPS) https://www.pfrda.org.in/myauth/admin/showimg.cshtml?ID=2860

******