ईपीएफओ,मुख्यकार्यालय
श्रम एवं रोज़गार मंत्रालय, भारत सरकार
भविष्यनिधिभवन, 14, भीकाजीकामाप्लेस, नईदिल्ली 110066
EPFO, HEAD OFFICE
MINISTRY OF LABOUR & EMPLOYMENT, GOVERNMENT OF INDIA
14, BHIKAIJI CAMA PLACE, NEW DELHI 110066
www.epfindia.gov.in

HRD/55/2021/e-office/721

Date-26.12.2022

To,

All Additional Central PF Commissioners (HQ)/Director (PDNASS),
All Additional Central PF Commissioners (Zones),
All Regional PF Commissioners (In charge of ROs/DOs/ZTIs/Sub ZTI),
RPFC (ASD), Head Office

Sub: Implementation of the e-office in the Field Offices and instructions for e-files and e-receipts -Reg.

Madam/Sir,

Please refer to the subject cited above. It is to inform that IS Division has successfully launched e-office in all the field offices on "Good Governance Day" i.e 25.12.2022 and e-office solution is now available for all Regional Offices in addition to HO & ZOs. IS Division & Railtel will handhold the EMD Managers of ROs through Whatsapp group for integrating users of respective ROs to e-office. In this regard, following instructions are issued for strict compliance by the Field Offices:-

1. All new files to be created in the e-office portal and all the existing physical files to be converted as e-file. Action to be initiated initially for current files and remaining files to be converted subsequently.

2. All the DAK received in the office w.e.f 01.01.2023 is to be created as e-receipt and to be moved in e-office only.

3. However, Secret/Top Secret/Classified issues/documents not to be handled in e-office and all the communication related to such issues should be kept in the physical mode only.Concerned OIC to ensure the same.{Please refer to circular no-HRM-VIII/e-office/2018 dated 24.08.2021(copy enclosed)}

4. All the communication between Head Office and Zonal Office/PDNASS, between Regional Office and Zonal Office and between ZTIs and PDNASS should be through e-office only so as to ensure that every issue can be tracked and monitored properly.Similarly files may be sent by RO & DO to ZO, ZTIs to PDNASS and ZO & PDNASS to HO & vice versa.

5. It may be noted that there should not be any physical movement of files & DAK after 31.01.2023 in any office.

Yours faithfully,

Encl:As Above

(Uma Mandal)
Addl CPFC (HR)

Copy to (Through EPFO Website)

1. PPS/PS to CPFC
2. PPS/PS to FA & CAO/CVO
3. PPS/PS to All Divisional Heads in Head Office
4. All ACCs
5. Chief Information Security Officer
6. Chief Technology Officer
7. RPFC, NDC for web circulation
8. Hindi Section for Hindi Version
9. Guard File

26/12/22

(Swagata Rai)
RPFC-I (HRD)

कर्मचारी भविष्य निधि संगठन
EMPLOYEES' PROVIDENT FUND ORGANISATION
श्रम एवं रोजगार मंत्रालय, भारत सरकार
MINISTRY OF LABOUR & EMPLOYMENT, GOVERNMENT OF INDIA
मुख्य कार्यालय/Head Office
भविष्य निधि भवन, 14, भीकाएजी कामा प्लेस, नई दिल्ली-110066
Bhavishya Nidhi Bhawan, 14, Bhikaiji Cama Place, New Delhi-110066
Website: www.epfindia.gov.in, www.epfindia.nic.in

No-HRM-VIII/e-Office/2018 Date: 24 AUG 2021

CIRCULAR

Subject: Security Advisory WRT E-Office-reg.

This is to bring to the notice of all concerned that a security advisory w.r.t e-office has been issued by NCIIPC, a unit of NTRO for all Government departments.

The same is enclosed herewith for kind information.

24/8/21

Swagata Rai
Regional PF Commissioner-I(HRD)

To

All the e-office users in EPFO: Through e-office Notice board

From: "Advisory NCIIPC" <advisory@nciipc.gov.in>
Sent: Thursday, November 26, 2020 12:25:58 PM
Subject: Cyber Security Advisory: Cyber Hygiene of e-Office

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Date: 26 Nov 2020

Advisory No: Adv/2020/Nov/016

Cyber Security Advisory: Cyber Hygiene of e-Office

This data is to be considered as **TLP: AMBER**

e-Office was initiated in 2009 and developed by National Informatics Centre with an aim to improve the functioning ofGovernment through more efficient, effective and transparent inter-Government transactions and processes.

Recently, a major breach in one of the State Data Centre has come to light. The State Data Centre was compromised and a web shell was uploaded through which every document in Data Centre was accessible. Further, e-Office of several other State's alsohas been found hosted on public IP, which is not recommended. Following precautions may be taken to ensure functioning of e-Office:

a. Cyber-attacks (including ethical hacking) on government websites, and many more threats such as key logger, phishing, denial of service etc. have been on the rise. Hence, Scanned documents containing sensitive information are not recommended to be hosted on e-Office.
b. Latest antivirus and anti-malware software on client machines through which e-Office is accessed, to be regularly updated.
c. e-Office application is regularly audited against all known vulnerabilities at the time of release. There may be new vulnerabilities that crop up and were not known at the time of release. In case e-Office is allowed to be accessed from public network, possibilities of external attacks increase. Therefore, e-Office should be accessed in restricted environment (NICNET/NKN/SWAN/LAN etc.).
d. Secret/ Top Secret/ Classified documents should not be handled in e-Office.
e. If any user wants to access the e-Office outside the restricted environment, VPN (Virtual Private Network) certificate should be used in such cases.

This document is distributed as TLP: AMBER. Recipients may only share TLP: AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in