File No.EDP/1-19/NIC/2020-21

कार्यालय महालेखाकार (लेखापरीक्षा)
मेघालय, शिलांग - 793 001.
OFFICE OF THE ACCOUNTANT GENERAL (AUDIT),
MEGHALAYA, SHILLONG – 793 001.
Email: agauMeghalaya@cag.gov.in Fax No. (0364) 2223494

सत्यमेव जयते

EDP/Audit/12 Dated: 20/12/2022

CIRCULAR

Subject:Cyber security- Installation of KAVACH for accessing NIC emails and other applications.

Please find enclosed herewith headquarters' office letter No. 1389-ISW/282-2020 dated 02.12.2022 forwarded under OM letter No. 21 (03)/2022-Pers./3144816 issued by the GOI, Ministry of Electronics & Information Technology, NIC, New Delhi dated 15.11.2022, regarding installation of Kavach through authenticated source.

In this connection, all officers and staff are instructed to go to https://kavach.mail.gov.in directly by typing it in the web browser and not by searching it over internet. Further, the instructions of headquarters office in aforementioned letter are to be noted and complied.

PARBHA ROY RYNGKHLEM, SAO/EDP/PRR, EDP CELL
Senior Audit Officer/EDP Cell

Memo No. EDP/1-19/NIC/2020-21/209-215 Dated: 20/12/2022

Copy forwarded for information and necessary action:

1. Secretary to the Accountant General (Audit).
2. All Group Officers.
3. All Branch Officers.
4. All Sections
5. All employees through mail
6. Office Website
7. All Notice Boards.

PARBHA ROY RYNGKHLEM, SAO/EDP/PRR, EDP CELL
Senior Audit Officer/EDP Cell

DAG(Admn)/C&AG/2022-23/455 Dt: 2-12-2022

Email AG AU Meghalaya

[Cag-all-offices] Cyber security- Installation of KAVACH for accessing NIC emails and other applications

From : Prabhakaran <sao5is@cag.gov.in> Fri, Dec 02, 2022 02:14 PM

Subject : [Cag-all-offices] Cyber security- Installation of KAVACH for accessing NIC emails and other applications 1 attachment

To : CAG-ALL-OFFICES@lsmgr.nic.in

Cc : 'Vikash Kumar' <kumarvikash@cag.gov.in>, 'Raghvendra Singh' <singhr1@cag.gov.in>, 'Director IS' <diris@cag.gov.in>, 'Deep Kumar' <aao6is@cag.gov.in>, 'SANJAY KUMAR' <sao6is@cag.gov.in>

Office of the Comptroller and Auditor General of India, New Delhi
Information Systems Wing

No. 1389 –ISW/282-2020
02.12.2022

Dy. No-479/CAG/Admn
dt/05/12/2022,

To
All Heads of Department
(As per mailing list)

Sub: Cyber security- Installation of KAVACH for accessing NIC emails and other applications

Madam/Sir

The National Informatics Centre (NIC) has introduced two stage authentication for accessing email and other applications hosted by NIC. The second authentication is done through 'KAVACH' after verification of username and password. NIC has already instructed all users to install the KAVACH in their systems and mobile phones from NIC's KAVACH website. **Any Google Search for the 'KAVACH' may lead to fake sites like https://kavach.mail.nic-, hxxps:/kavah.mail.nic- providing fake download facility for 'KAVACH', which is threat to the security of the systems in IAAD.**

In view of the above and to ensure that KAVACH is downloaded only from authenticated site, all users are requested to go to **https://kavach.mail.gov.in** directly by typing it in the web browser and not by searching it over internet or other methods for installation of KAVACH.

Further, NIC has informed that all cyber incidents should be reported to CERT-In with in 6 hours of noticing the incidents. The OM dated 15th November 2022 issued by NIC in this behalf is attached herewith for necessary information and action.

Encl: As above

SrAO/Admn

Yours faithfully,

-sd/-

(Vikash Kumar)
Director (IS)

R.T/EDP

5/12/22

5/12 AAO/EDP

AG

2/XII

Azadi Ka Amrit Mahotsav

CAG-ALL-OFFICES mailing list -- cag-all-offices@lsmgr.nic.in
To unsubscribe send an email to cag-all-offices-leave@lsmgr.nic.in

NIC_OM_CERTIn_Directions_15Nov2022.pdf
263 KB

No. 21(03)/2022-Pers./3144816
Government of India
Ministry of Electronics & Information Technology
National Informatics Centre
A-Block, CGO Complex, Lodhi Road, New Delhi-110003

Dated: 15th November, 2022

OFFICE MEMORANDUM

The undersigned is directed to refer to the directions issued by CERT-In vide communication No. 20(3)/2022-CERT-In dated 28 April, 2022 (https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf) and to say that the following directives need to be strictly adhered to by all individual concerned.

(i) All cyber incidents (as mentioned in the Annexure) shall be mandatorily reported to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents.

The Incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). Details regarding methods and formats of reporting cyber security incidents (updated from time to time) are also published on the website of CERT-In (www.cert-in.org.in).

(ii) All ICT systems shall mandatorily enable logs and maintain them securely for a rolling period of 180 days.

(iii) All ICT systems shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) for time syhchronisation.

2. This issues with the approval of the Competent Authority.

15/11

(Manoharan R)
Joint Director (Pers.)
Ph. No. 24305442

Encl: As above

Copy to:

1. All officers/officials of NIC....through DigitalNIC
2. CISO, NIC Hqrs ... w.r.t. his note dated 10.11.2022 vide file No. M-13/1470/2022-NIC Hqr(3145304)
3. Staff Officer to DG, NIC ... for kind information
4. Vigilance Officer, NIC
5. Guard File/Personal File/DigitalNIC

-sd-
(Manoharan R)
Joint Director (Pers.)

Annexure

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:

[Refer Rule 12(1)(a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013]

i. Targeted scanning/ probing of critical networks/ systems
ii. Compromise of critical systems/ information
iii. Unauthorised access of IT systems/ data
iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
v. Malicious code attacks such as spreading of virus/ worm/ Trojan/ Bots/ Spyware/ Ransomware/ Cryptominers
vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers
vii. Identity Theft, spoofing and phishing attacks
viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
ix. Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
x. Attacks on Application such as E-Governance, E-Commerce etc.
xi. Data Breach
xii. Data Leak
xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
xiv. Attacks or incident affecting Digital Payment systems
xv. Attacks through Malicious mobile Apps
xvi. Fake mobile Apps
xvii. Unauthorised access to social media accounts
xviii. Attacks or malicious/ suspicious activities affecting Cloud computing systems/ servers/ software/ applications
xix. Attacks or malicious/ suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones
xx. Attacks or malicious/ suspicious activities affecting systems/ servers/ software/ applications related to Artificial Intelligence and Machine Learning.
