File No.IT-ADM/201/2021-O/o Clerical Section-IT Department

Government of Jammu and Kashmir
Information Technology Department
Civil Secretariat, Jammu
****

Subject: **Implementation of e-Office - Security Advisory thereof.**

Circular No: 09 - JK (ITD) of 2021
Dated: 30 .09.2021

The implementation of e-Office in the Civil Secretariat including Raj Bhawan J&K has brought about a great deal of efficiency in the overall working and disposal of Government business in the Union territory of Jammu and Kashmir, besides ensuring functionality of the Government both at Jammu as well as in Srinagar. Notwithstanding these benefits, this online system like any other IT based systems, is susceptible to online invasions especially **ethical hacking, key logger, phishing, denial of service, etc.**

While security of this system is being strengthened, dangers of hacking cannot be over ruled. All e-Office users therefore, have to remain extra cautious and vigilant in respect of potential online invasions and hacking attempts.

Accordingly, in order to make all users aware of the security risks, a Security Advisory has been received from National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India, a unit of National Technical Research Organization (NTRO) with respect to Cyber Hygiene of e-Office. **The same is enclosed herewith as Annexure for information and necessary compliance.** Furthermore, it is enjoined upon all e-Office users to be mindful of online invasions and interventions like Hacking / Phishing / Denial of Service attacks etc for Cyber Hygiene of e-Office. If any such case arises, the same shall be reported to the authorities of the UT Government.

Sd/-
(Amit Sharma) JKAS
Administrative Secretary

No:IT-ADM/201/2021 **Dated:30.09.2021**

Copy to the:-

1. Financial Commissioner (Additional Chief Secretary), Finance Department.
2. Financial Commissioner (Additional Chief Secretary), Health & Medical Education Department.

3. Director General of Police, J&K.
4. All Principal Secretaries to the Government.
5. Principal Secretary to the Lieutenant Governor.
6. Joint Secretary (J&K), Ministry of Home Affairs, Government of India.
7. All Commissioner/Secretaries to the Government.
8. Chief Electoral Officer, J&K.
9. Director General, J&K Institute of Management & Public Administration & Rural Development.
10. Divisional Commissioner, Kashmir/Jammu.
11. Chairperson, J&K Special Tribunal.
12. Director Information, J&K.
13. Chief Executive Officer, J&K e-Governance Agency.
14. All Deputy Commissioners..
15. All Heads of Departments/Managing Directors/Secretary, Advisory Boards.
16. Registrar General, J&K High Court, Srinagar.
17. Secretary, J&K Public Service Commission/SSB/BoPEE.
18. Director, Estates.
19. Director, Archives, Archaeology and Museums.
20. Secretary J&K Legislative Assembly.
21. Secretary J&K Academy of Art, Culture & Languages.
22. General Manager, Government Press, Srinagar/Jammu.
23. Private Secretary to the Chief Secretary.
24. Private Secretary to Advisor(F)/(B) & (BK) t o the Lieutenant Governor.
25. Private Secretary to the Commissioner/Secretary to the Government, General Administration Department.
26. **In-charge Website GAD, IT and JaKeGA for uploading the Circular on respective websites.**
27. Circular file.

30/9/21

Under Secretary to the Government,

Information Technology Department

Receipt No: 178868/2021/O/o PM 1

239394/2021/CS

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