

Mi/57/2025-e-gov-MOWR
Government of India
Ministry of Jal Shakti
Department of Water Resources, RD & GR
(e-Governance Section)

Shram Shakti Bhawan
Rafi Marg. New Delhi
Dated: 21.05.2025

CIRCULAR

Subject: Security Measures for eOffice Application – reg.

This is in reference to Director General, Ministry of Electronics and information Technology's DO letter dated 12.05.2025 (copy enclosed) regarding the security measures undertaken for e-Office application considering the heightened threat perception in the cyberspace.

2. In this regard, all the users under DoWR, RD&GR are directed to strictly adhere to the instructions mentioned in the above mentioned DO letter dated 12.05.2025. Also, all the users are requested to please find enclosed herewith the following documents for compliance :

- i. Detailed list of security measures undertaken for e-Office (Annexure-1).
- ii. General Advisory outlining the cyber hygiene (Annexure-2).
- iii. Advisory from NCIIPC regarding access of eOffice in restricted environment (Annexure-3)
- iv. OM from DARPG regarding not to put Secret, Top Secret, and Classified communications in e-Office (Annexure-4).

Encl: As above

Digitally signed by
Mahesh Kumar Kashyap
Date: 22-05-2025
15:50:41
(Mahesh Kumar Kashyap)
Under Secretary (e-Gov & IEC)
Tel: 011- 2376 6944
Email: mk.kashyap@gov.in

To,

All the officers of DoWR, RD&GR and Heads of all the Organizations under DoWR, RD&GR

अभिषेक सिंह, भा.प्र.से.
महानिदेशक

Abhishek Singh, IAS
Director General



भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
राष्ट्रीय सूचना-विज्ञान केन्द्र

Government of India
Ministry of Electronics and Information Technology
National Informatics Centre

D.O. No. NIC- eOPD/2025-01/eOffice-Security

Date: 12-5-2025

Dear Sir/Madam,

I am writing to apprise you of the security measures undertaken for the eOffice application, considering the heightened threat perception in the cyberspace.

2. The eOffice application, currently implemented across all the Ministries and Departments of the Government of India is hosted at the National Data Centre (NDC), Shastri Park, New Delhi and is accessible over NICNET/WebVPN only. Recognizing the critical nature of this application, number of security controls have been instituted to ensure its consistency and availability. All users must be apprised with the same and follow the security instructions in letter and spirit. All users must ensure that user credentials of email and VPN access should be kept securely and changed from time to time. Usage on public computers and devices should be avoided. Detailed list of security measures undertaken for eOffice is attached (**Annexure-1**). Also, enclosed is general advisory outlining the cyber hygiene (**Annexure-2**), Advisory from NCIIPC regarding access of eOffice in restricted environment (**Annexure-3**) and OM from DARPG regarding not to put Secret, Top Secret, and Classified communications in eOffice (**Annexure-4**) to be followed by each ministry/department.

For any further help or support, you can reach out to my colleague/helpdesk **Website:** <https://servicedesk.nic.in>, Email: helpdesk-nic@nic.in, Phone: 1800111555.

With regards

Yours Sincerely


(Abhishek Singh)

To:

The Secretaries of all Ministries/Departments of Government of India

CC:

All HOGs & HODs (NIC Ministries/Departments)

Encl. as above:

1. List of Security measures undertaken for eOffice at NDC, Shastri Park (Annexure –1)
2. General advisory outlining the cyber hygiene (Annexure-2)
3. Advisory from NCIIPC regarding access of eOffice in restricted environment (Annexure-3)
4. OM from DARPG regarding not to put Secret, Top Secret, and Classified communications in eOffice (Annexure-4)

ANNEXURE-1**Security Measures undertaken for eOffice application**

eOffice application has been implemented in all Ministries, Departments of Government of India and the same are hosted in the National Data Centre (NDC), Shastri Park, New Delhi.

2. Following security measures have been ensured for eOffice application:
 - a. Asset details have been properly documented for eOffice infrastructure.
 - b. The servers are hosted in National Data Centre (NDC), Shastri Park, New Delhi and are behind firewall.
 - c. Restricted servers access (for administration activities) is provided through VPN.
 - d. Vulnerability assessment of all the servers is being performed regularly.
 - e. Antivirus has been installed, configured, and full scans are conducted regularly.
 - f. All credentials (OS & DB) are periodically reset.
 - g. Application and Database are on different Network segments.
 - h. Developers and Administrators are on different Network segments.
 - i. Creation of golden images for servers has been done.

3. Besides, the following standard practices have also been ensured for eOffice:
 - a. The eOffice applications are hosted over valid SSL for encryption.
 - b. eOffice access is restricted to NICNET/NKN/WebVPN.
 - c. No anonymous access is allowed. The authentication is through Parichay and each application has its own authorization.
 - d. Application security audit is done periodically.
 - e. Comprehensive Security Assessment is done regularly.
 - f. Maintaining of Application logs.
 - g. Regular updates and management of asset details with severity tracking is ensured.
 - h. Continuous vulnerability assessment is done of all eOffice VMs/servers.
 - i. Continuous antivirus scan of all eOffice VM's is undertaken.
 - j. Continuous VAPT on the eOffice instances is ensured.
 - k. Periodic review of security hardening scripts is conducted.
 - l. Application Penetration testing is done regularly.
 - m. The user credentials for all servers are regularly changed.
 - n. Monitoring of all the servers and related services through Command & Control Centre (CCC) dashboard.

CIS Governance Division

Cyber and Information Security Group,
National Informatics Centre,
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
csg-advisory@nic.in

NIC-CISG/2025-04/078

Dated: 24-04-2025

CVE ID: None

Severity: High

**ANNEXURE-2**

**Emergency Security Alert: Security Precautions to be Undertaken for
Safeguarding Govt Websites, Applications and ICT Infrastructure**

A. Description:

Due to the prevailing geo-political situations and increased threat perception in the cyberspace, all are advised to stay on high alert and ensure proper cyber security hygiene and best practices are followed both at Client level (i.e., desktop, laptop etc.) and at the Application, Database, Server, Data Centre & Network level.

B. Cyber Security precautions to be undertaken:

The following Security Precautions should be strictly adhered to by all those who are involved in the development, design, testing, implementation, audit, operations, management and troubleshooting of any Government Website or Application or Database or ICT Infrastructure/Services:

- Ensure that all Operating systems on servers & client machines, including Applications, Frameworks, Softwares, Packages, IDEs etc. are running with latest updates/patches.
- Ensure that Endpoint Security Agents, provided by NIC, are installed on all client machines and servers. Full System scan to be done at least once in a week and quick/flash scans to be done at least once in a day.
- Ensure that all servers and client machines are properly security hardened.
- Ensure that logging is enabled in all servers, CMS, databases, network & security devices and any other ICT Infrastructure or Service.
- Ensure that X-Forwarded For (XFF) is enabled for all the applications/websites which are behind a Load Balancer or WAF.
- Remote desktop, Telnet, SSH and any other administrative access like CMS etc should be allowed only for VPN IPs.
- Do not use any remote administration tools like Anydesk, Ammy Admin, Team Viewer etc.
- Critical applications should be placed behind the Web Application Firewall (WAF).
- Ensure that NIC's DNS server settings (1.10.10.10/2409::1) is configured on all servers in NDCs and on all machines in NICNET
- Ensure that NIC's NTP Server settings (samay1.nic.in / samay2.nic.in) is configured on all servers and client machines in NDCs and NICNET.
- Always download updates and patches from the official website or repositories of the OEM. Never download the updates/patches from any unauthorized third-party websites.

- Disable Powershell in Windows based servers and client machines.
- Do not use the root account or super administrator account in your servers/clients, for day to day activities.
- Check all files present under the 'website root' directory and 'upload' directory for any unauthorized file modifications and deletions every day.
- Ensure that the websites, applications and databases are monitored round the clock for any unauthorised changes or modifications
- Change all administrator credentials for servers, databases, applications, CMS and other management components at least once in 60 days.
- Ensure all the sites and applications are accessible through https (i.e. with valid SSL certificate).
- Ensure all API calls are done through encrypted channel.
- Use geo-fencing for the websites wherever applicable.
- Ensure that all websites/applications/portals are security audited (Limited audit in Six months and Comprehensive audits annually). The security audit to be ensured before/after the implementation, installation, or major enhancement of ICT infrastructure also.
- Ensure that Application Source Code is not hosted in any external repositories (ex:github) outside Government Network
- Don't store credentials on phone/computer or exchange any sensitive information through third party messaging apps/email, social media.
- Ensure that the staging environment is not directly exposed to the internet. Temporarily shut-down all staging servers.
- In case of any security incident report it to NIC-CERT at: incident@nic-cert.nic.in

X-----X-----X

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 of Government 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 also has been found hosted on public IP, which is not recommended. Following precautions may be taken to ensure functioning of e-Office:

- 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.
- Latest antivirus and anti-malware software on client machines through which e-Office is accessed, to be regularly updated.
- 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.).
- Secret/ Top Secret/ Classified documents should not be handled in e-Office.
- 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



No.N-11016/6/2016-ARC
Government of India
Ministry of Personnel, Public Grievances & Pensions
Department of Administrative Reforms &&Public Grievances

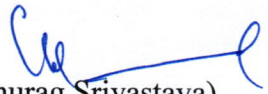
5th Floor, Sardar Patel Bhawan,
Sansad Marg, New Delhi -110001

Dated the 9th July, 2018

OFFICE MEMORANDUM

Subject: Minutes of the meeting taken to discuss matter regarding processing of classified documents/files on e-office held on 28th June, 2018.

The undersigned is directed to send herewith the copy of minutes of the above meeting for information and necessary action.


(Anurag Srivastava)
Deputy Secretary (ARC)
Tel. no. 23362325

To,

1. Secretary,
Ministry of Electronics & Information Technology
Electronics Niketan,6,CGO Complex, Lodhi Road,
New Delhi-110003.
e-mail: secretary@deity.gov.in
2. Home Secretary
Room No. 113,North Block,
New Delhi-110001
hshso@mha.gov.in
3. Smt. Neeta Verma, DG, NIC, Ministry of Electronics and Information Technology, dg@nic.in
4. Shri G. K. Gaur, DDG, NIC, Ministry of Electronics and Information Technology,
gaurgk@nic.in
5. Shri Saroj K. Patro, Scientist 'E', NIC, Ministry of Electronics and Information Technology,
sk.patro@nic.in
6. Shri Kapil Kumar Sharma, Scientist 'E', NIC, kapilks@nic.in

7. Dr. Gulshan Rai, National Cyber Security Coordinator, National Security Council Secretariat, ncsc@gov.in
8. Dr. Balmiki Prasad, Director (Security), Ministry of Home Affairs, dirsecurity-mha@gov.in

Copy to:-

1. Shri K. V. Eapen, Secretary (AR&PG) - in Chair
2. Smt. Vasudha Mishra, Additional Secretary
3. Ms. Smita Kumar, Joint Secretary
4. Ms. Kiran Puri, Joint Secretary
5. Shri V. A. Chavda, Joint Secretary
6. Shri Anurag Srivastava, Deputy Secretary
7. Shri Rajender Sethi, Sr. Technical Director (NIC)
8. Shri Khamchin Naulak, Under Secretary
9. Shri Sunil Kumar Singh, Section Officer

Minutes of the meeting held under the chairmanship of Secretary, Department of Administrative Reforms & Public Grievances (AR&PG) at 12:00 Noon on 28th June, 2018 to discuss matter regarding processing of classified documents/files on e-Office.

List of participants is at Annexure.

2. Secretary (AR&PG) welcomed the participants.

3. Advice of all experts was sought on whether the following can/should be dealt on e-Office: Processing of Notes for Cabinet/CCEA/COS etc;

- (i) Parliament Questions and other Parliament matters;
- (ii) Files involving Inter-Ministerial Consultations including PMO and Finance, DoP&T etc;
- (iii) Vigilance Cases/Court Cases;
- (iv) The matters dealing with Secret/Top Secret/Classified information.

4. All participants offered their considered views and the following decisions were taken:

- (i) E-Office, as is operational today, may not be able to cater to the requirements of Secret/Top Secret/Classified communications; hence, it was decided that for the present, such communications/files may be handled on physical mode.
- (ii) NIC would work out a different instance of e-Office, with a separate system and server for catering to such classified information and would make a presentation in due course of time for consideration.
- (iii) All departments may rationalize the categorization of files/documents as Secret/Top Secret/Classified/Non-Classified, with due diligence.
- (iv) Regarding Parliament Questions and other Parliamentary matters, though in general, there is no bar on using e-Office, however, care must be taken to ensure that no material of a sensitive nature may be processed on e-Office presently.
- (v) Similarly, for files requiring inter-ministerial consultations or Vigilance/Court Cases, it is permissible under the current system of e-Office, provided the thumb rule of not transmitting Secret/ Top Secret/Classified information on e-Office till it is suitably equipped to deal with them, is followed. It was reiterated that, to comply with e-Office guidelines, a Department/Ministry has to maintain only 80% of their files on electronic mode and there is ample scope to cover all files which are more conveniently dealt with in a physical form, within the 20% of admissible numbers.

5. The meeting ended with vote of thanks to the Chair.

.....

Annexure

List of Participants

DAR&PG

10. Shri K. V. Eapen, Secretary (AR&PG) - in Chair
11. Smt. Vasudha Mishra, Additional Secretary
12. Ms. Smita Kumar, Joint Secretary
13. Ms. Kiran Puri, Joint Secretary
14. Shri V. A. Chavda, Joint Secretary
15. Shri Anurag Srivastava, Deputy Secretary
16. Shri Rajender Sethi, Sr. Technical Director (NIC)
17. Shri Khamchin Naulak, Under Secretary
18. Shri Sunil Kumar Singh, Section Officer

MeitY

19. Shri Ajay P. Sawhney, Secretary
20. Smt. Neeta Verma, DG, NIC,
21. Shri G. K. Gaur, DDG, NIC
22. Shri Saroj K. Patro, Scientist 'E', NIC
23. Shri Kapil Kumar Sharma, Scientist 'E', NIC

National Security Council Secretariat

24. Dr. Gulshan Rai, National Cyber Security Coordinator, NSCS

Ministry of Home Affairs

25. Dr. Balmiki Prasad, Director (Security)