

REMINDER-II (MOST URGENT)

Government of NCT of Delhi
Department of Information Technology

9th Level, B wing Delhi Secretariat IP Estate, New Delhi

<https://it.delhi.gov.in>

E-17/4/2022-Dir(DeGS) / CDNo- 042708413/6731-6812 dated: 15/10/2024

CIRCULAR

Subject: Measures to enhance Cyber Security within the Government

References:

- (1) Circular issued by this office vide File No. E-17/4/2022-Development/CD No.- 042708413/5013-92 dated 20.07.2023
- (2) Circular issued by this office vide File No. E-17/4/2022-Development/computer No.- 134228/7629-7698 dated 19.12.2022
- (3) Circular issued by this office vide File No. E-17/1/2022-Dir (DeGS)/5944-613 dated 21.09.2022
and
- (4) MeitY D.O letter No. M-11/39/2022-NIC dated 31.08.2022

The MeitY, GoI through the said letter, has directed to take immediate measures to enhance the Cyber Security within the Government. The Departments were asked to submit the information as per annexure – A.

Departments were asked to send the action taken report as per the annexure attached latest by 28.07.2023 and also to appoint a senior level officer as Assist. Chief Information Security Officer (ACISO) in r/o concerned department. However, information in this regard is still pending.

As Cyber and information security is a niche area and is the prime concern for the Government, hence, all departments are again requested to provide attention to Cyber Security. The Government will soon start an audit for the compliance of security measures in the department.

Now, as proactive approach towards cyber security, NIC is planning to deploy advance tools like Unified Endpoint Management (**UEM**) & Endpoint Detection and Response (**EDR**) under NICNET for enhancing cyber security.

1. **Unified Endpoint Management (UEM):** UEM is a comprehensive solution for managing user endpoints, ensuring their day-to-day administration is handled efficiently. It provides near real-time software and hardware inventory, defining the scope and attack surface of endpoints. UEM also facilitates the deployment of periodic operating system updates and the installation, update, or removal of third- party software such as browsers, document editors, and PDF readers. Additionally, UEM manages endpoint policies and controls without accessing user data, ensuring privacy while maintaining control over the system.

2. **Endpoint Detection and Response (EDR)**: EDR is a next-generation security tool designed to protect endpoints like desktops and laptops from advanced cyber threats. It offloads endpoint security to AI and machine learning systems, allowing users to work with confidence. Key features of a comprehensive EDR solution include:

- *Signature-based detection for known threats*
- *Behaviour-based detection for suspicious activities*
- *Host firewall/intrusion prevention systems*
- *Application and device control*
- *Vulnerability assessment*
- *Remote incident response*
- *Threat hunting*


The centralized management and reporting of EDR helps specialist security analysts stationed at Security Operations Center (SOC) to proactively monitor and manage security threats and attacks on user endpoints without compromising their privacy or data.

A technical team of IT Officers under the supervision of ACISO of respective departments is required to execute/implement UEM and EDR in the department.

It is, therefore, once again requested to submit the information and details of the nominated Assistant Chief Information Security Officer (ACISO) along-with the detail of IT officer (DPA/SA/SSA/JD), posted in your department through URL: <https://degs.org.in/wm/ACISO> on **PRIORITY**, latest by 18.10.2024.

This is **MOST URGENT**.

This letter is issued with the prior approval of the Pr. Secretary-IT, Delhi.


(K.Murugan)

Chief Information Security Officer, Delhi

Encl: A/a

To,

1. All Pr.Secretaries/Secretaries/HoDs
2. All Local Bodies/Boards/Commissions, Govt. of NCT of Delhi
3. Deputy CISO with a request to help the departments in providing the information.

Copy for information to:

1. SO to Chief Secretary, GNCTD
2. PS to Pr. Secretary (IT), GNCTD.

REMINDER -I (MOST URGENT)

Government of NCT of Delhi

Department of Information Technology9th Level, B wing Delhi Secretariat IP Estate, New Delhi<https://it.delhi.gov.in>

E-17/4/2022-Dir(DeGS) / CDNo. 042708413/5013-92 dated 20/07/2023

CIRCULAR**Subject: Measures to enhance Cyber Security within the Government****References:**

- (1) Circular issued by this office vide File No. E-17/4/2022 Development/computer No. 134228/7629-7698 dated 19.12.2022
- (2) Circular issued by this office vide File No. E-17/1/2022-Dir (DeGS)/5944-613 dated 21.09.2022 and
- (3) MeitY D.O letter No. M-11/39/2022-NIC dated 31.08.2022

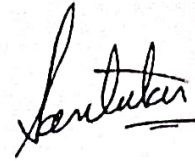
Secretary, MeitY, GoI through the said letter, directed to take immediate measures to enhance the Cyber Security within the Government. The Departments were asked to submit the information as per annexure – A.

Departments were asked to send the action taken report as per the annexure attached latest by 26.12.2022 and also to appoint a senior level officer as Chief Information Security Officer (CISO) in r/o concerned department. However, information in this regard is still pending.

As Cyber and information security is a niche area and is the prime concern for the Government, hence, all departments are again requested to provide attention to Cyber Security. The Government will soon start an audit for the compliance of security measures in the department.

It is, therefore, once again requested to send the information and details of the nominated Assistant Chief Information Security Officer (ACISO) in your department to IT Department in the attached Annexure-A latest by 28.07.2023.

This letter is issued with the prior approval of the Secretary (IT).



(Santulan Chaubey)

Chief Information Security Officer (CISO), Delhi

Encl: A/a

To,

1. All ACS/Pr.Secretaries/Secretaries/HoDs
2. All Local Bodies/Boards/Commissions, Govt. of NCT of Delhi
3. Deputy CISO with a request to help the departments in providing the information.

Copy for information to:

1. SO to Chief Secretary, GNCTD
2. PS to Secretary (IT), GNCTD.

50105/c

REMINDER (MOST URGENT)

Government of NCT of Delhi
Department of Information Technology

9th Level, B wing Delhi Secretariat IP Estate, New Delhi

<https://it.delhi.gov.in>

E-17/4/2022-Development / Computer No. 134228/7629-7698 dated: 19/12/2022

CIRCULAR

Subject: Measures to enhance Cyber Security within the Government

References:

- (1) Circular issued by this office vide File No. E 17/1/2022-DII (DeGS)/5944-613 dated 21.09.2022
- (2) MeitY D.O letter No. M-11/39/2022-NIC dated 31.08.2022

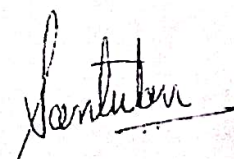
Secretary, MeitY, GoI through the said letter, directed to take immediate measures to enhance the Cyber Security within the Government. The Departments were asked to submit the information as per annexure – A.

Departments were asked to send the action taken report as per the annexure attached latest by 10.10.2022 and also to appoint a senior level officer as Chief Information Security Officer (CISO) in r/o concerned department. However, information in this regard is still pending.

As Cyber and information security is the prime concern for the Government, all departments are requested to provide attention to Cyber Security. The Government will soon start an audit for the compliance of security measures in the department.

It is, therefore, once again requested to send the information and details of the nominated Assistant Chief Information Security Officer (ACISO) in your department to IT Department in the attached Annexure-A latest by 26.12.2022.

This letter is issued with the prior approval of the Secretary (IT).


(Santulan Chaubey)

Chief Information Security Officer (CISO), Delhi

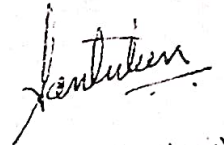
Encl: A/a

To,

1. All ACS/Pr.Secretaries/Secretaries/HoDs
2. All Local Bodies/Boards/Commissions, Govt. of NCT of Delhi
3. Deputy CISO with a request to help the departments in providing the information.

Copy for information to:

1. SO to Chief Secretary, GNCTD
2. PS to Secretary (IT), GNCTD.



(Santulan Chaubey)

Chief Information Security Officer (CISO), Delhi

Information Technology Department
Government of National Capital Territory of Delhi
9th Level, B-Wing, Delhi Secretariat
<https://delhi.gov.in>

Dated: 21/9/22

File No. 17/11/2022-11/39/2022-MIC dated 31/8/22

CIRCULAR

Subj: Measures to enhance the Cyber Security within the Government – reg.

Please find enclosed herewith a copy of Ministry of Electronics and Information Technology's DO letter No. M-11/39/2022-MIC dated 31st August 2022 (copy enclosed).

Secretary, MICT, GOI through the letter has directed to take immediate measures to enhance the Cyber Security Measures within the Government. It is also suggested the following measures may be taken immediately to enhance the Cyber Security preparedness:

- (i) MAC binding of each and every PC/Node connected with Network should be done for accessing Government applications.
- (ii) The Operating System of all PCs/devices should be upgraded with the latest version/patches and the obsolete equipment should be withdrawn from the network.
- (iii) Admin rights from the Systems may be withdrawn from the Users and should be controlled by CISO/DCISO.
- (iv) All devices should be connected via single network gateway of NIC and any other connectivity i.e. broadband, 3G/4G may be phased out for increasing the security.
- (v) Use of all pirated OS and Applications must be immediately stopped.
- (vi) Need based internet Connectivity through NICNet may be provided to the selected users with the approval of CISO and all the other users should be given access to NICNET.
- (vii) Antivirus software must be deployed on each and every machine
- (viii) Unmanaged LAN network device should be taken out of the Network.

Contd. 2/-

21/9/22

701


Departments are hereby directed to send the action taken report as per Annexure attached latest by 10.10.2022

In addition to above, kind attention is also invited to guidelines for "Key Roles and Responsibilities of CIP (Information Security) Officers (CISOs) in Ministry, Departments and Organization managing ICT Operations issued by India-Computer Emergency Response Team, Ministry of Electronics and IT, GOI (copy enclosed).

All HoDs/Administrative Secretaries are thus requested to appoint a senior officer as CISO (Chief Information Security Officer) in the concerned Department under intimation to IT Department.

This issues with the approval of Secretary (IT).

Encl. As above.


(Krishan Kumar)
Jt. Director (IT)

To

All ACS/Pr. Secretaries/Secretaries/HoDs
All Local Bodies/Boards/Commissions
Govt. of NCT of Delhi

Copy for information to: -

1. Staff Officer to Chief Secretary, Delhi
2. PS to Secretary (IT), 9th Level, B-Wing, Delhi Secretariat, New Delhi

451LC

961

31C

Ministry of Electronics & Information Technology
Government of IndiaDO No M-11/39/2022-NIC
Dated 31st August 2022

Dear Chief Secretary,

During a recent review on cyber security preparedness of ministries / departments and associated government organisations the Minister of Electronics & Information Technology has directed to take immediate measures to enhance the cyber security measures within the government.

2. In this regard, it is requested that your ministry / department may take the following measures immediately to enhance the cyber security preparedness

- i. MAC binding of each and every PC / Node connected with Network should be done for accessing govt applications
- ii. The operating system of all PCs / devices should be upgraded with the latest version / patches and the obsolete equipment should be withdrawn from the network
- iii. Admin rights from the systems may be withdrawn from the users and should be controlled by CISO / DCISO
- iv. All devices should be connected via single network gateway of NIC and any other connectivity, i.e. broadband 3G/4G may be phased-out for increasing the security.
- v. Use of all pirated OS & applications must be immediately stopped
- vi. Need based internet connectivity through NICNET may be provided to the selected users with the approval of CISO and all the other users should be only given access to NICNET
- vii. Antivirus software must be deployed on each and every machine
- viii. Unmanaged LAN network devices should be taken out of the network

3. You may please advise the CISO to do rigorous checks on the above measures and kindly send the action taken report by 10th September, 2022. It is only with your continued support and cooperation that we can build a strong, safe, secure and resilient cyber security system for the government.

Yours sincerely,

(Alkesh Kumar Sharma)

Chief Secretaries of all the States/UTs

Action Taken ReportS.NoSuggestionAction Taken
Status in Yes/No

- | | | |
|---|---|--|
| 1 | MAC binding of each and every PC/Node connected with Network should be done for accessing Government applications | |
| 2 | The Operating System of all PCs/devices should be upgraded with the latest version, patches and the obsolete equipment should be withdrawn from the network. | |
| 3 | Admin rights from the Systems may be withdrawn from the users and should be controlled by CISO/DCISO. | |
| 4 | All devices should be connected via single network gateway of NIC and any other connectivity i.e. broadband, 3G/4G may be phased out for increasing the security. | |
| 5 | Use of all pirated OS and Applications must be immediately stopped. | |
| 6 | Need based internet Connectivity through NICNet may be provided to the selected users with the approval of CISO and all the other users should be given access to NICNET. | |
| 7 | Antivirus software must be deployed on each and every machine | |
| 8 | Unmanaged LAN network device should be taken out of the Network. | |

Detail of CISO of the Department: -

- (i) Name of the Officer
- (ii) Designation of the Officer
- (iii) Phone Number (Official)
- (iv) Phone Number (Mobile)
- (v) E-Mail ID