GOVT. OF NCT OF DELHI
DEPARTMENT OF SOCIAL WELFARE
7TH FLOOR, MSO BUILDING, ITO, NEW DELHI
(ADMINISTRATION BRANCH)

F.No.44(45)/2023/DSW/Admn./Estt./Misc./ 21171 – 21175 **Dated:** 11 MAR 2024

CIRCULAR

Please find enclosed herewith a circular/letter No. F.17/2/2019-Dir (DeGS/Sec(IT)CD-93058/694-773 dated 25.01.2024 issued by Department of Information Technology, GNCTD on Information Security Audit Related Advisory for Government Organisation for adhering to the mentioned guidelines in purview of engaging vendors for security audit for strict compliance.

This issues with prior approval of the competent authority

11/3/24
Section Officer (Admn.)

F.No.44(45)/2023/DSW/Admn./Estt./Misc./ 21171 – 21175 **Dated:** 11 MAR 2024
Copy to:

1. All Branch Incharges (HQ) of Department of Social Welfare.
2. PA to Director(SW), Department of Social Welfare, New Delhi-110002
3. PA to Secretary(SW), Department of Social Welfare, New Delhi-110002
4. Sr. System Analyst for uploading the circular on the website of the Department.
5. Guard file.

11/3/24
Section Officer (Admn.)

87/CC
11/3/24

Government of NCT of Delhi
Department of Information Technology
9th Level, B wing Delhi Secretariat IP Estate, New Delhi
https://it.delhi.gov.in

F.17/2/2019-Dir (DeGS/Sec(IT)CD-93058/764-773 dated: 29/01/2024

CIRCULAR

Please find enclosed herewith the guideline vide 3(15)/2004-CERT-In (Vol.XII) dated 29.12.2023 issued by Indian Computer Emergency Response Team (CERT-In) on Information Security auditing related advisory for Government organizations (copy enclosed).

CERT-In, MietY, GoI, through the said letter, has directed to put some appropriate mechanism to ensure compliance to the following below mentioned advisories at the time of engaging CERT-In empanelled organisations, in interest of security of sensitive information belonging to the Government and Critical Sector:

i. Organisation should ensure that every auditing organisation and its auditors (personnel) engaged in audit should sign Non-Disclosure Agreements (NDAS) prior to the commencement of auditing work. For this purpose, organisation may use model NDA prepared by CERT-In. Model NDA is available on CERT-In website (https://www.cert-in.org.in/ ->Cyber Security Assurance-> Empanelment by CERT-In).

ii. Since, engaging non-Indians firms for auditing requirements by the Government and critical sector organisations may involve exposing sensitive information to non-Indian persons/entities or having foreign links, the concerned Government Ministries / organisations should obtain NOC from MHA before engaging any non-Indian firms.

iii. Organisation should ensure that the data collected during on-premises auditing including audit report should not be allowed to be taken out of the Government premises. Organisation should also ensure compliance against Policy Guidelines for Handling Audit related Data. "Policy Guidelines for Handling Audit related Data" is available on CERT-In website (https://www.cert-in.org.in/ ->Cyber Security Assurance-> Empanelment by CERT-In).

Hence, all departments are requested to adhere the above mentioned guidelines in purview of engaging vendors for security audit. This may be treated most urgent.

This issues with the approval of Secretary (IT).

Encl: A/a

29/1/24
(K Murugan)
Chief Information Security Officer, Delhi

To:

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

Copy for information to:
1. SO to Chief Secretary, GNCTD
2. PS to Secretary (IT), GNCTD.
3. SIO, Delhi State Unit, NIC

4884/DD(A)
30/1/24

SH/ JD VD
16/01/2024

17/2024/.
12-01-20

Confidential

3(15)/2004-CERT-In (Vol. XIII)
Ministry of Electronics & Information Technology (MeitY)
Indian Computer Emergency Response Team (CERT-In)
Electronics Niketan, 6, CGO Complex
Lodi Road, New Delhi-110003

Date: 28th December, 2023

Subject: Information security auditing related advisory for Government organisations - regarding.

The Indian Computer Emergency Response Team (CERT-In) under Ministry of Electronics & Information Technology (MeitY), Government of India has created a panel of 'Information security auditing organizations' for auditing, including vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the Government and critical infrastructure organizations to enhance the cyber security posture. These information security auditing organisations have been vetted by Ministry of Home Affairs. The list of CERT-In empanelled auditing organisations can be accessed at CERT-In website at https://www.cert-in.org.in. At present, the list is being consulted by all the Government organisations and critical sectors for their information security auditing requirements.

08-01-24
Secy (IT)

JD(IT)

2. In relation to the process of engaging the CERT-In empanelled information security auditing organisations, on advice of IB/MHA, it is felt necessary to issue the following advisories to ensure that the audit engagement process is secure and does not pose any threat to sensitive information belonging to Government and critical sector.

16/01/2024

ALPM

i. Organisation should ensure that every auditing organisation and its auditors (personnel) engaged in audit should sign Non-Disclosure Agreements (NDAs) prior to the commencement of auditing work. For this purpose, organisation may use model NDA prepared by CERT-In. Model NDA is available on CERT-In website (https://www.cert-in.org.in/ ->Cyber Security Assurance-> Empanelment by CERT-In).

ii. Since, engaging non-Indians firms for auditing requirements by the Government and critical sector organisations may involve exposing sensitive information to non-Indian persons/entities or having foreign links, the concerned Government Ministries / organisations should obtain NOC from MHA before engaging any non-Indian firms.

iii. Organisation should ensure that the data collected during on-premises auditing including audit report should not be allowed to be taken out of the Government premises. Organisation should also ensure compliance against Policy Guidelines for Handling Audit related Data. "Policy Guidelines for Handling Audit related Data" is available on CERT-In website (https://www.cert-in.org.in/ ->Cyber Security Assurance-> Empanelment by CERT-In).

3. It is requested that a communication may please be sent to all the Government organisations and critical sectors within the purview of your domain to put in place an appropriate mechanism to ensure compliance to the above advisories at the time of engaging CERT-In empanelled organisations, in interest of security of sensitive information belonging to the Government and critical sector.

(Dr. Sanjay Bahl)
Director General, CERT-In
Tel.: 011-24368544 / 22902703

To:

1) **All Secretaries of Central Government Ministries/Department**
2) **All Chief Secretaries of States & UTs.**

Copy to:

1) **Sh. B.K. Jha**
Under Secretary (S),
IS-I Division (Security Desk),
Ministry of Home Affairs
Room No. 1, North Block,
New Delhi - 110001

2) **Sh. Niranjan Samal**
Assistant Director,
Intelligence Bureau,
35, S.P. Marg
New Delhi - 110021