



भारतीय सूचना प्रौद्योगिकी संस्थान, अगरतला (त्रिपुरा)
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, AGARTALA (TRIPURA)
AGARTALA - 799046 (TRIPURA)

F. No. NITA. 3 (130-Gen)/ 2022/ 10249-58.

Dated 18-02-2022

C I R C U L A R

Subject: Communication Security Advisory for Government Officials - reg.

This is for general information to all concerned for compliance in view of Communication Security Advisory for Government Officials vide letter F. No 54-14/2021-TS.1, dated 19-01-2022 of Department of Higher Education, Ministry of Education, Govt. of India (copy enclosed).

DBhally 18-02-22
(Prof. D. Bhattacharya)
Mentor Registrar, IITA
& Registrar (I/C), NITA

To
All concerned officials.

Copy to:

- 1) PS to the Director, NIT Agartala for kind information of the Director, NITA and Mentor Director, IITA.
- 2) All Deans, NIT Agartala.
- 3) The HoD, CSE Department, NIT Agartala.
- 4) The Co-ordinator, IIIT Agartala.
- 5) The Nodal Officer, IIIT Agartala.
- 6) The Head (F&A) and Asstt. Registrar (Admn-1), NIT Agartala.
- 7) The Asstt. Registrar (Admn-2)/ Asstt. Registrar (F&A), NIT Agartala.
- 8) The Audit Officer, NIT Agartala.
- 9) The System Administrator, NIT Agartala with a request to upload in the website of IITA.

DBhally 18-02-22
(Prof. D. Bhattacharya)
Mentor Registrar, IITA
& Registrar (I/C), NITA

14

F. No 54-14/2021-TS.1
Government of India
Ministry of Education
Department of Higher Education
Technical Section 1 (IIITs)

C-Wing, Shastri Bhawan, New Delhi
Dated 19th January, 2022

To
The Director,
IIITs (CFTIs/ PPPs),

Subject: Communication Security Advisory for Government Officials-reg

Sir,

Please find attached herewith a copy of OM No. C.30019/01/2021-CDN, dated 13th January 2022 received from Coordination Section of this Department on the subject cited above for information and compliance.

Yours faithfully,



(A.K. Chattopadhyay)
Under Secretary to the Govt. of India
Tele.: 011-23384861
Email: ak.chattopadhyay@nic.in

Enclosure: As above

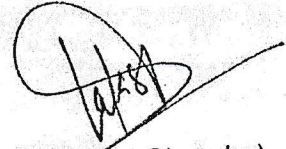
F. No. C.30019/01/2021-CDN
Government of India
Ministry of Education
Department of Higher Education
CDN Section

229, C Wing, Shastri Bhawan, New Delhi
Dated the 13th January, 2022

OFFICE MEMORANDUM

Subject: Communication Security Advisory for Government Officials-reg

The undersigned is directed to enclose herewith a copy of communication bearing no. S-5701(10)/1/2022-S4-50 dated 07.01.2022 received from Intelligence Bureau, Ministry of Home Affairs on the subject mentioned above for compliance.




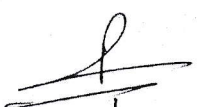
(Lakshmi Chandra)
Under Secretary (CDN)
Intercom: 724

Encl: As above

To:

| |
|--------------------|
| AS(TE) 994932/2022 |
| AS(Edu.) |
| JS(HE) |
| JS(ICC & Vig) |
| JS (Mgt.) |
| EA(CU&A) |
| JS(S&S) |
| JS(NIT) |

All Dir/DSS


 14/1
~~DS(TE/ICC)~~

 14/1
 DP(TC) Kati 14/01/22 80(TC)

PTS-993531

12

SECRET

Copy No 24

IR No. IS-003

INTELLIGENCE BUREAU
(Ministry of Home Affairs)

Subject: Communication Security Advisory for Government Officials

It was observed that a large number of Government officials were using public domain messaging platforms like Whatsapp, Telegram, etc. for classified official communication. Officials usually photograph/scan copies of various classified documents and send the same through the messaging platforms. Such practice is a clear violation of information security instructions as provided in Manual of Departmental Security Instructions (MoDSI) and National Information Security Policy Guidelines (NISPG). All Ministries/ Government departments need to take urgent steps to stop such violations.

2. Classified information shared on public domain messaging platforms like Whatsapp can be harvested by private companies owning the platform as they control storage servers that are often located outside the country. This information can be used by adversaries or can be monetised for gains. In order to curtail the leakage of classified information and misuse of such platforms, the following guidelines are reiterated in the interest of the communication security:

2.1. Classified information falls under the following four categories, namely, TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED. The Top Secret and Secret documents shall not be shared over the internet. According to NISPG, the Top Secret and Secret information shall be shared only in a closed network with leased line connectivity where SAG grade encryption mechanism is deployed. However, Confidential and Restricted information can be shared on internet through networks that have deployed commercial AES 256-bit encryption.

2.2. Pertinently, the use of **Government Email** (NIC email) facility or Government Instant Messaging Platforms (such as CDAC's Samvad, NIC's Sandesh, etc.) is recommended in the Ministry/Departments for the communication of Confidential and Restricted information. However, utmost care should be taken during the classification of information and before the communication of the same over internet (i.e. an information which may deserve a Top Secret/Secret classification shall not be downgraded to Confidential/Restricted for the purpose of sharing the information over the internet).

SECRET

E/A Please ensure all Bits
Wag
11/1

Mishra
12-1-22
US (CDN) [Signature]
13/1
LON
PY


2.3. In the context of **e-Office System**, it may be advised that the Ministry/Department may deploy proper firewalls and white-listing of IP addresses. The 'e-Office server' may be accessed through a Virtual Private Network (VPN) for enhanced security. The Ministry/Department may ensure that only authorized employees are allowed access to the e-Office System. However, Top Secret/Secret information shall be shared over the e-Office system only with leased line closed network and SAG grade encryption mechanism.

2.4. In the context of **Video Conferencing (VC)** for official purpose, Government VC solutions offered by CDAC, CDOT and NIC may be used. The meeting ID and password shall be shared only with authorized participants. To ensure better security, the 'Waiting Room' facility and prior registration of the participants may be used. Even then, Top Secret and Secret information shall not be shared during the VC.

2.5. Officials working from home, may use security-hardened electronic devices (such as Laptops, Desktops, etc.). Such devices may be connected to the office servers through a VPN and Firewall setup. It is pertinent to mention that Top Secret/Secret information shall not be shared in the 'work from home' environment.

2.6. Digital Assistant devices like Amazon's Echo, Apple's HomePod, Google Home, etc. may not be kept in office. Further, Digital Assistants (such as Alexa, Siri, etc.) should be turned off in the smart phones/watches used by the employee. Smart phones may be deposited outside the meeting room during discussion on classified issues.

3. In the light of the above, it is suggested that CISOs of all Ministries/Departments may be directed to brief officers and government employees on the above mentioned point to ensure communication security. For further clarification, MoDSI and NISPG may be referred, or the Ministry/Department may consult IB.


(Karthikeyan K)
Joint Deputy Director

Secretaries of all Ministries in Government of India (list attached)


DIB UO No. S-5701(10)/1/2022-S4- 50

Dated: January 07, 2022

Copy to:

NSCS :

(Shri Rajinder Khanna, Dy. NSA)


Joint Deputy Director