भारत के नियंत्रक एवं महालेखापरीक्षक का कार्यालय
9, दीन दयाल उपाध्याय मार्ग, नई दिल्ली-110124

OFFICE OF THE
COMPTROLLER & AUDITOR GENERAL OF INDIA
Pocket 9, Deen Dayal Upadhyaya Marg,
New Delhi-110 124

Bijay Kumar Mohanty, IA & AS
Director General (IS)

No. 05/DG/IS/Sectt./2024
दिनांक / DATE 19-11-2024

Advisory on Data and Network Security for Email Communications

Data and network security is paramount for the effective and secure functioning of any government organization, especially given the role of email as a primary communication medium. In the current IT-driven environment, email systems face constant threats from non-state actors who exploit this platform to spread malware, misinformation, and undesirable messages. These threats compromise not only individual users but also pose risks to the broader information systems of the organization. It is essential to implement stringent measures to secure email systems against such attacks to protect both data integrity and institutional credibility.

Moreover, it has come to our attention that some individuals having access to our mail IDs are using official email channels to send malicious or frivolous messages. Such misuse strains IT resources, detracts from organizational productivity, and can create unnecessary operational challenges. To address these internal and external threats effectively, it is vital to adopt proactive and collaborative methods of managing email security, which includes the need for vigilance among all users and coordination with the CTO Wing for technical support.

It is advised that all officials who receive potentially malicious or suspicious emails should promptly share the email header with the designated email ID of the CTO Wing(**cag-ciso@cag.gov.in**). This information will enable traceability and assist in identifying malicious actors. Relevant provisions under the *Information Technology Act, 2000* (amended in 2008), *The Indian Penal Code (IPC)(amended and named as Bharatiya Nyaya Sanhita*, and *National Cybersecurity Reference Framework* govern these actions, empowering us to take corrective and preventive measures. By adhering to these protocols, we can maintain a safe, reliable, and secure communication environment for all users

It is crucial to emphasize that forwarding potentially malicious emails or their contents through other means, such as WhatsApp or alternative messaging platforms, either within or outside the organization, constitutes a significant security risk and can be deemed an offense under existing laws. Under the “Information Technology Act, 2000 (amended in 2008)”, the transmission of offensive or false information via electronic communication or unauthorized access and dissemination of information, including the forwarding of malicious content that may disrupt, or damage computer resources can attract penalties. Such actions not only

दूरभाष / Phone : +91-11-23235390 फैक्स / Fax : +91-11-23509495 ई-मेल / E-mail : mohantyBK@gov.in

violate organizational policy but may also expose the organization and individuals to legal consequences under Section 500 and Section 505 of the Indian Penal Code (IPC)(Section 353 and section 356 of Bharatiya Nyaya Sanhita), which deal with the transmission of defamatory and inflammatory content. Therefore, officials are strictly advised to refrain from sharing suspicious or malicious communications across any platform outside the sanctioned channels and to report them directly to the CTO wing for investigation and taking appropriate action.

Any security related issues may be forwarded exclusively to the emailed: **cag-ciso@cag.gov.in**

This issues with the approval of CTO

DG (IS) & Chief Information Security Officer