



NO.DG-III/ Cyber Advisory/4/111/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT

Karachi, Dated: 22nd October, 2026

To

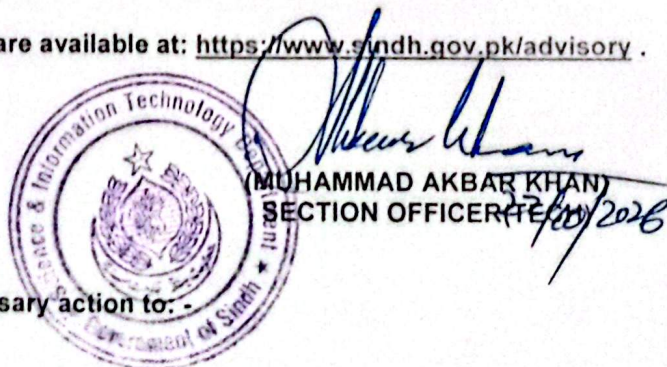
1. The Chairman, Planning & Development Board, Govt. of Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
3. The Chairman Chief Minister's Inspection Enquiries and Implementation Team
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR) Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh _____
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh _____

SUBJECT: CYBER CLEANSING AND SECURITY HARDENING OF IT SYSTEMS AGAINST MALICIOUS EMAIL CAMPAIGN ALIGNMENT WITH PISF REQUIREMENTS

I am directed to forward herewith the advisory on "Cyber Cleansing and Security Hardening of IT Systems Against Malicious Email Campaign", issued with reference to Cabinet Division (NTISB) Letter No. 1-5/2003-59(NTISB-II) dated 6 August 2026, for information and necessary action.

In view of above, all Government of Sindh departments and their attached departments are requested to carry out cyber cleansing of computers, laptops and other devices used for official email; ensure appropriate endpoint security, including anti-virus/EDR/XDR solutions; and implement email security gateway controls to detect and block phishing, malware and other malicious content. These measures should also support compliance with the Pakistan Information Security Framework (PISF).

The details with respect to the subject are available at: <https://www.sindh.gov.pk/advisory>.



A copy is forwarded for information and necessary action to:-

1. CEO Sindh IT Company.
2. DG NCERT Government of Pakistan
3. PS to Chief Secretary, Sindh.
4. Staff Officer to Secretary, S&IT Department, Government of Sindh.
5. Webmaster S&IT Department to publish on the official website(s).

SECTION OFFICER(TECH)

23- Mr. Muhammad Niaz, Deputy Director-II, CAB, Islamabad

24- Dr. Muhammad Muzammil Zia, Project Director CPEC, PC, Islamabad

25- Secretary Aviation Division, Kohsar Complex Constitution Avenue

SUBJECT: CYBER CLEANSING AND SECURITY HARDENING OF IT SYSTEMS AGAINST

MALICIOUS EMAIL CAMPAIGN ALIGNMENT WITH PISF REQUIREMENTS

Reference Cabinet Division (NTISB) Letter No. 1-5/2003-59(NTISB-II) dated 6th August 2026.

2. Reference letter cited above, a malicious email campaign originating from the Prime Minister's Office was conducted, and credible evidence exists that such emails were also sent to accounts of various Ministries/Divisions. All organizations were directed to carry out cyber cleansing of their IT equipment in consultation with NCERT, ascertain the extent of any data pilferage, and implement robust cybersecurity controls.

07.10.26
A (G)

07.11

Copy Sent IT Cell

3. In compliance with the above directive, NCERT has been carrying out cyber cleansing security assessment activities on request from various Ministries/Divisions. To standardize the exercise across all organizations and to ensure that the remediation measures adopted also contribute towards the mandatory **Pakistan Information Security Framework (PISF)** compliance requirement, all Ministries/Divisions are advised to adopt the technical controls outlined below.

4. **Detection and Removal of Malware.** Malware signatures are identified through a **detective control** – i.e., a control that identifies and flags malicious activity after it has occurred or while it is in progress, as opposed to a preventive control which blocks it beforehand. Anti-virus, Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions fall in this category: they continuously scan endpoints against known malware signatures and behavioral indicators, and upon detection, trigger an automated **corrective/response action** – quarantining or deleting the malicious file. Ministries/Divisions are accordingly advised to install and enable an appropriate endpoint security solution (anti-virus, EDR or XDR, selected based on organizational risk profile and available resources) on all systems used for handling official domain email, to scan, detect and root out any malware that may have been downloaded through the malicious email campaign.

5. **Perimeter-Level Email Protection.** In addition to endpoint-level detection, each Ministry/Division shall deploy an **Email Security Gateway** of their own and/or get it configured for the organization through their Email service provider to protect official email at the network perimeter. This preventive control filters phishing, spam and malicious attachments before they reach end-user mailboxes, thereby reducing the likelihood of similar campaigns succeeding in future.

6. Carrying out this exercise will not only cleanse the affected systems of any malware introduced through the referenced email campaign, but will also contribute directly towards **partial compliance with PISF**, specifically:

a. **Control PISFID-058 (Endpoint Security and Malware Protection)** under the **Essential System and Communication Protection Controls** domain, which requires "appropriate security solutions (anti-virus, anti-malware, EDR, XDR, etc.) depending upon the classification of asset and architecture of the organization," with endpoints not to be left without appropriate protection; and

b. The email protection requirement under **Control Group (Email and Web Hosting Services)** of the **Essential Data Centre and Web Hosting Services Controls** domain, which requires "advanced email threat protection controls to detect and block phishing, malware, spam, and malicious content."

7. Ministries/Divisions are encouraged to treat this cleansing exercise as an opportunity to concurrently begin addressing the above controls, rather than as a one-time remedial activity. All Ministries/Divisions are therefore requested to carry out cyber cleansing of their computer systems (PCs/ Laptops/ Other devices handling official emails) by deploying the endpoint and email perimeter controls outlined in Paras 3 and 4 above.

8. NCERT remains available to provide technical assistance, or clarify any aspect of this advisory, as and when required.