NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT

Karachi, Dated: 13th November, 2025

To

1. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
2. The Chairman, Planning & Development Board Sindh, Karachi
3. The Chairman/Chairperson, CMIT Sindh, Karachi
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: CYBERSECURITY ADVISORY ON RISKS OF HOSTING GOVERNMENT EMAIL INFRASTRUCTURE OUTSIDE NATIONAL JURISDICTION.

In light of the increasing trend of hosting official government email services on foreign cloud platforms or non-certified local providers, which poses significant risks to national cybersecurity, data sovereignty, and intelligence confidentiality, the attached Advisory titled "NCA-14.301025-National CERT Advisory-Risks of Hosting Government Email Infrastructure Outside National Jurisdiction" (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).

2. The advisory highlights the serious implications of hosting government email systems outside Pakistan's jurisdiction, exposing sensitive communications to foreign surveillance, legal exposure, unauthorized access, and data interception. Compromise of such systems could result in data theft, espionage, credential compromise, and disruption of official communications, undermining the confidentiality and integrity of government correspondence. Government Organizations should ensure security of their email hosting servers.

3. It is requested that the attached Advisory be disseminated to all relevant Ministries/Divisions, Departments and Organizations under your administrative control for immediate review and necessary action.

Annexure: NCA-14.301025-National CERT Advisory-Risks of Hosting Government Email Infrastructure Outside National Jurisdiction

(DR. RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II
0310-2131415

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

1. Director General (nCERT). L Block, Pak Secretariat, Islamabad
2. AS(Staff) to Chief Minister Sindh, Karachi.
3. Director (Operations), S&IT Department, Govt. of Sindh
4. PS to Chief Secretary, Sindh.
5. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt. of Sindh, Karach
6. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
7. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.
8. Webmaster, for uploading the advisory on url: https://www.sindh.gov.pk/

Annexure

NCA-14.301025 – National CERT Advisory –Risks of Hosting Government Email Infrastructure Outside National Jurisdiction

1. Introduction

The National CERT of Pakistan has observed an increasing trend among public-sector entities to host official email services on foreign cloud platforms or unregulated local providers. Such practices pose critical national cybersecurity, data-sovereignty, and intelligence-exposure risks, especially given the sensitivity of government communications.

Email servers operated outside Pakistan or on insecure, non-certified infrastructure fall beyond the jurisdictional control of national authorities, leaving them vulnerable to state-sponsored surveillance, data interception, unauthorized access, and legal exposure under foreign laws. These advisory outlines the associated threats and provides mitigation guidance.

2. Impact

Compromise or unauthorized access to government email systems hosted abroad or on insecure platforms may result in:

a. **Espionage and Data Exfiltration:** Persistent access by hostile actors through compromised servers.
b. **Credential Theft:** Harvesting of administrator or user credentials via phishing or server-side compromise.
c. **Service Disruption:** Outages, denial-of-service, or manipulation of routing and DNS records.
d. **Integrity Breach:** Unauthorized modification or injection of falsified official correspondence.
e. **Incident-Response Limitations:** Forensic or legal challenges due to cross-border data location.

3. Threat Details

3.1 Hosting Vectors and Exploitation Conditions

Threat Vector	Description
Foreign Hosting & Cloud Exposure	Data subject to foreign jurisdiction; possible lawful or covert access.
Unregulated Local Hosting	Weak patching, outdated mail software, lack of monitoring.
Misconfigured Servers	Open relays, weak TLS, default admin credentials, and missing DMARC/DKIM/SPF records.
Phishing & Credential Reuse	Attackers exploiting unmanaged MX records or weak authentication.
Supply-Chain Dependencies	Reliance on foreign DNS, certificate authorities, or outsourced data centers.

3.2 Attack Complexity & Vector

a. **Attack Vector:** Remote (SMTP/IMAP/HTTPS management and admin interfaces)
b. **Attack Complexity:** Low – exploits basic misconfigurations or credential reuse
c. **Privileges Required:** None (in case of open relay or leaked credentials)
d. **User Interaction:** Minimal (phishing or spoofing via misconfigured mail records)
e. **Exploitation Status:** Actively observed targeting of exposed *.gov.pk* and hybrid-cloud mail systems

4. Affected Systems

Systems at highest risk include:

a. Email servers hosted on foreign cloud providers.
b. Hybrid or offshore data centers storing official government correspondence
c. Locally managed servers lacking encryption, MFA, or patch management
d. Departments using unofficial mail domains not governed by *.gov.pk* namespace

5. Exploit Conditions

Successful exploitation typically requires one or more of the following:

a. Direct internet exposure of mail administration consoles
b. Unpatched or outdated mail server software

c. Weak or default credentials used in production
d. Absence of TLS 1.3 encryption or DNSSEC validation
e. Lack of network segmentation between internal and public mail services

6. Recommendations & Mitigation Actions

6.1 Migrate to Nationally Designated Hosting

a. All government entities are advised to host official email services within Pakistan's jurisdiction.
b. Avoid use of foreign cloud or offshore email services for any official communication.
c. All official correspondence should be made through official email within organization or intra organizations instead of using Gmail, Hotmail, Yahoo emails etc.

6.2 Implement Core Technical Controls

a. Enforce TLS 1.3, MFA, and role-based access for all administrators.
b. Enable DMARC, DKIM, and SPF to prevent spoofing.
c. Apply timely patching and vulnerability management for Exchange/Zimbra/Postfix servers.
d. Maintain offline encrypted backups within national data centers.

6.3 Harden Configurations and Access

a. Isolate mail management interfaces from public networks.
b. Restrict administrative access to trusted IP ranges or VPN segments.
c. Disable legacy or unused mail protocols (POP3, IMAP if not required).
d. Conduct regular configuration audits and penetration testing.

6.4 Network & Endpoint Monitoring

a. Integrate mail logs into centralized SIEM or SOC platforms.
b. Monitor for anomalous login patterns, configuration changes, or mass forwarding rules.
c. Deploy anti-phishing gateways and sandbox attachments.

6.5 Compliance and Governance

a. Ensure all vendors handling government email data are PSS-certified and locally registered.

b. Verify contractual clauses for data residency within Pakistan and secure key management.

6.6 Promote Indigenous and Sovereign Technologies

a. Prioritize NTC, NITB, or other MoITT-approved Government based infrastructure providers.
b. Encourage development of local email security and encryption tools.
c. Reduce dependency on foreign cloud ecosystems for critical communication channels.

6.7 Incident Preparedness and Response

a. Update incident-response playbooks to include email-server compromise scenarios.
b. In case of suspected breach:
   i. Isolate the affected mail server.
   ii. Preserve forensic evidence (logs, network captures).
   iii. Reset credentials and verify DNS/MX records integrity.

7. Monitoring & Detection

Organizations should continuously monitor for:

a. Multiple failed or unusual successful logins from foreign IPs
b. Unauthorized configuration or forwarding-rule changes
c. Abnormal outbound mail volume or attachment patterns
d. DNS or MX record tampering
e. Unusual API activity in mail-management panels

8. Patching & Configuration Summary

Category	Affected Systems	Action Status
Vulnerable	Email servers hosted outside Pakistan or on unregulated local providers	**Immediate migration to NTC or certified national host**
Secure	Systems hosted on NTC or approved national infrastructure with encryption, MFA, and compliance to PSS	**Maintain monitoring and periodic audits**

9. Call to Action

The National CERT advises all government ministries, divisions, provincial departments, and critical-infrastructure operators to:

a. Ensure security of their email hosting servers.
b. Cease usage of foreign cloud email services for official communications.
c. Implement full encryption, authentication, and monitoring controls as detailed above.
d. Adopt Pakistan Security Standards (PSS) and support the use of indigenous cybersecurity technologies.