



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

Karachi, Dated: 22nd October, 2026

To

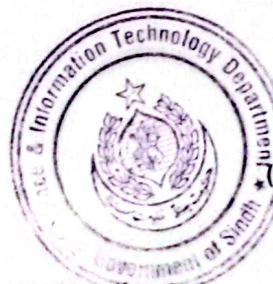
1. The Chairman, Planning & Development Board, Govt. of Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
3. The Chairman Chief Minister's Inspection Enquiries and Implementation Team
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR) 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: ISSUANCE OF ADVISORY ON MOUS / SLAS BETWEEN INTERNATIONAL TECH COMPANIES AND GOVERNMENT OF PAKISTAN (GOP)

I am directed to forward herewith the advisory regarding "Cybersecurity and Data Proliferation Risks in MOUs/SLAs Between International Technology Companies and the Government of Pakistan" for information and necessary action.

In view of above all Government of Sindh Departments and their attached department are requested to ensure that relevant MOUs/SLAs adequately address data privacy, data ownership and custodianship, access controls, third-party access, data retention and secure disposal, cross-border data transfers, breach notification and incident response. Appropriate precautions should also be taken regarding the use of AI tools, cybersecurity practices and third-party applications, with a view to safeguarding government data and Pakistan's digital sovereignty.

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



(MUHAMMAD AKBAR KHAN)
SECTION OFFICER (TECH)

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)



National Cyber Emergency Response Team

Government of Pakistan



Annexure

NCA-44.011026 – National CERT Advisory

Cybersecurity and Data Proliferation Risks

With the recent expansion of digital and AI driven innovations, many government organizations are using AI to modernize public service delivery and streamline government operations. For this purpose, government organizations are also doing collaborations with different AI centres and international service providers.

While such partnerships offer significant developmental benefits, deeper integration of government functions with a foreign commercial cloud and AI service provider may increase exposure to cybersecurity and data governance risks. Official, taxpayer, citizen, and sector-specific data may be uploaded to, processed by, or synchronized with external platforms; copied across personal and official accounts; entered into AI tools as prompts or documents; or shared with integrated third-party services. Without clear contractual, technical, and procedural safeguards, this may result in data proliferation, loss of control over sensitive records, unintended retention, and legal or data sovereignty concerns.

This advisory suggests relevant organizations to take precautionary measures as it is intended to ensure that cybersecurity, privacy, and data protection requirements are addressed before and during implementation of any project.

Possible Risks

1. **Unauthorized Data Disclosure:** Official or taxpayer data exposed beyond the intended scope
2. **Data Proliferation:** Government data copied across tools, accounts, and services outside official control
3. **Data Sovereignty Risk:** Sensitive data stored or processed in foreign-hosted infrastructure
4. **AI Data Leakage:** Sensitive documents or prompts entered into AI tools and retained or reused
5. **Privacy Violations:** Citizen, taxpayer, or employee information mishandled
6. **Supply Chain & Integration Risk:** APIs, connectors, and third-party apps expanding the attack surface
7. **Account Compromise:** Stolen credentials of officials giving access to email, cloud data storage drives, and AI workspaces
8. **Regulatory & Legal Exposure:** Non-compliance with data protection, classification, and records obligations
9. **Reputational & Strategic Risk:** Loss of public trust and aggregation of sensitive data of strategic value

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



CALL TO ACTION – KEY SECURITY PRACTICES

#	Requirement
1	Treat external cloud and AI platforms as third-party services
2	Do not enter sensitive official data in public AI tools
3	Use only official, managed accounts with MFA for official work
4	Share data only after classification and formal approval
5	Review vendor terms on data retention, localization, and use
6	Protect taxpayer, citizen, and employee data carefully
7	Vet all integrations, APIs, and third-party apps before enabling
8	Maintain audit trails for data shared with external parties
9	Seek National CERT guidance when security concerns arise
10	Report suspected data exposure or incidents promptly

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk