

NCA-18.011026 – National CERT Advisory

Safe and Secure Use of Generative Artificial Intelligence (GenAI) Tools and Platforms

The rapid adoption of public AI chatbots, coding assistants, browser extensions, AI-enabled applications, and third-party AI services is creating new cybersecurity and data-governance risks across organizations. Uncontrolled or unauthorized use of Generative AI, commonly referred to as Shadow AI, may expose sensitive information, intellectual property, credentials, source code, and organizational data while introducing risks from prompt injection, insecure AI-generated code, malicious integrations, inaccurate outputs, and compromised third-party models.

MANDATORY SECURITY & GOVERNANCE MEASURES

Organizations are advised to implement the following controls as a matter of priority:

- 1. Enforce a Generative AI Acceptable Use Policy:** Establish and enforce clear organizational rules defining approved, restricted, and prohibited uses of Generative AI tools, including requirements for data handling, access, accountability, and oversight.
- 2. Protect Sensitive & Classified Information:** Strictly prohibit the submission of classified, confidential, sensitive, personal, proprietary, credential-related, or otherwise restricted organizational information to public or unapproved AI platforms.
- 3. Establish an Approved AI Tool Registry:** Maintain a centrally vetted and regularly reviewed inventory of authorized AI tools, models, browser extensions, plugins, APIs, and platforms. Restrict access to unapproved or unsanctioned AI services.
- 4. Mandate Human Review of AI Outputs:** Require qualified human review and validation of all AI-generated code and other critical outputs before deployment, publication, operational use, or incorporation into organizational decision-making.
- 5. Deploy DLP & AI Monitoring Controls:** Extend Data Loss Prevention (DLP), access monitoring, endpoint security, and related controls to AI interfaces to detect sensitive-data submission, unauthorized AI usage, suspicious API activity, and Shadow AI.
- 6. Align AI Governance with Recognized Frameworks:** Develop organizational AI governance and security practices in alignment with internationally recognized frameworks, particularly NIST AI Risk Management Framework (AI RMF) and OWASP Top 10 for LLM Applications. Organizations should also consider applicable AI management, information-security, privacy, and data-protection requirements.
- 7. Conduct Regular Staff Training:** Provide periodic awareness and role-based training covering safe prompting, sensitive-data handling, AI-generated code, hallucinations, prompt injection, deepfakes, third-party AI risks, and organizational GenAI policy requirements.
- 8. Maintain Audit Trails:** Maintain appropriate logs of authorized AI tool access and usage for security monitoring, compliance verification, incident investigation, and accountability, subject to applicable privacy and organizational requirements.

MONITORING & DETECTION REQUIREMENTS

Organizations should continuously monitor for:

- Sensitive Data Exposure
- Shadow AI

- Unauthorized AI Plugins/APIs
- Prompt Injection
- Unreviewed AI-Generated Code
- Suspicious AI Access
- Policy Violations

Where an AI-related security incident occurs, organizations should immediately contain unauthorized access, preserve relevant evidence and logs, revoke compromised credentials or API keys, investigate the exposure, and implement corrective measures.

INCIDENT REPORTING

All incidents related to sensitive data exposure via AI tools, prompt injection exploitation, AI supply chain compromise, or violations of the Generative AI usage policy must be reported to National CERT Pakistan:

- **Incident Reporting Portal:** <https://pkcert.gov.pk/report-incident/>
- **Email:** cert@pkcert.gov.pk
- **UAN:** +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Enforce a mandatory Generative AI Acceptable Use Policy
2	Prevent submission of sensitive or classified data to public AI tools
3	Establish a vetted registry of approved AI tools and platforms
4	Mandate human review of all AI-generated code and critical outputs
5	Deploy DLP and monitoring controls covering AI interfaces
6	Align with international AI governance frameworks (NIST AI RMF, OWASP LLM Top 10)
7	Conduct regular staff training on safe and secure GenAI use
8	Maintain audit trails of AI tool usage for compliance and investigation

PKCERT