A-CIL AI SECURITY CHECKLIST 2026

MOHUYA CHAKRABORTY

A-CIL | Sunrise Point, SF1, 10G, New Town, Action Area 2C, WB, Kolkata 700157

AI SECURITY & CYBER RISK CHECKLIST FOR STARTUP (2026 EDITION)

Prepared by **Aspiration Cyber Intelligence Lab (A-CiL)**.

This checklist helps SMEs and AI-driven startups identify critical security and compliance gaps before scaling operations.

- ✓ Do you have documented data flow architecture for all customer data?
- ✓ Have you conducted a vulnerability assessment in the past 6 months?
- ✓ Are AI models tested against adversarial or data poisoning attacks?
- ✓ Is sensitive data encrypted at rest and in transit?
- ✓ Do you maintain role-based access controls across systems?
- ✓ Is there an incident response plan with assigned responsibilities?
- ✓ Are third-party APIs and integrations security-audited?
- ✓ Do you maintain compliance documentation for applicable data protection laws?
- ✓ Are federated or decentralized systems assessed for model leakage risks?
- ✓ Is board-level cyber risk awareness formally documented?

If you answered 'No' to three or more items, your organization may be exposed to preventable cyber and AI-related risks.

Contact A-CiL for a structured Cyber Risk or AI Security Audit.

trustaspiration@gmail.com

7044567467 | 9836310643