AI ACCEPTABLE USE & DATA SECURITY POLICY (AUP)

Effective Date: December 9, 2025

Owner: IBS Ventures (SMC-Pvt) Ltd. - Governance, Security & Compliance team

Applies To: Inspurate Employees, Contractors, Interns, Partner Companies, External Vendors, and Clients

1. Overview

At IBS Ventures, we use Artificial Intelligence (AI) to accelerate development, enhance creativity, and improve operational efficiency. But AI also brings new forms of risk — operational, cybersecurity, privacy, and legal.

This AI Acceptable Use & Data Security Policy defines how IBS Ventures manages and governs AI systems to protect internal assets, client data, partner and vendor information, shared infrastructure, and intellectual property. Security is non-negotiable, and trust is one of our core service values.

2. Recent Global AI Security Failures (Cited References)

1. Google Gemini Deletes Developer's Entire Local Drive

Source: CyberNews, "Deeply sorry: Gemini deletes developer's drive" (Nov 2024)

2. ChatGPT Leak Exposed Payment Information (OpenAI Breach, March 2023)

Source: OpenAI Security Incident Report (March 2023)

3. Samsung Employees Uploaded Sensitive Source Code to ChatGPT

Source: Forbes / Bloomberg (April 2023)

4. AI Coding Assistants Introducing Critical Vulnerabilities

Source: Stanford HAI Study — "Asleep at the Keyboard? Assessing the Security of AI-Generated Code" (2023)

5. Data Poisoning Attacks on AI Systems

Source: MIT Technology Review (2024)

© IBS Ventures (SMC-Pvt) Limited

3. Who This Policy Applies To

This policy governs AI use by IBS Venture employees, contractors, interns, consultants, clients, partners, vendors, and technology collaborators.

4. IBS Ventures Security Commitment

IBS Ventures commits to:

- Zero tolerance for data exposure.
- Zero use of client data in public AI systems.
- Zero autonomous execution by AI tools on any production environment.
- Full alignment with global security and data protection laws.

5. Core Principles

- Human accountability always.
- Zero trust for AI output; everything must be verified.
- No confidential data in public LLMs.
- AI is the copilot; humans are the decision-makers.

6. Software Development Standards

Mandatory Sandboxing:

AI tools must run only in isolated environments such as Docker containers, VMs, or Codespaces. AI must never access local drives or production systems.

Human-in-the-Loop Enforcement:

No AI-generated command involving deletion, database operations, network calls, or permission changes may be executed without human approval.

Credential Hygiene:

No keys, tokens, secrets, or connection strings may be shared with AI tools.

© IBS Ventures (SMC-Pvt) Limited

7. Data Privacy & Legal Compliance

We align with:

- GDPR (EU)
- CCPA (California)
- UK GDPR
- Pakistan's PDPA draft
- ISO 27001
- SOC 2
- Banking & FinTech client requirements

*See Annexure A for explanation of each

Data Classification Model:

Public, Internal, Confidential, Client Confidential, Restricted.

8. Cybersecurity Requirements

- Device encryption, updated OS, EDR enabled.
- MFA required; password manager required.
- No public WiFi without VPN.
- AI agents may not scan networks or access client infrastructure.
- Phishing and social engineering checks required.

9. Approved & Prohibited AI Tools

Approved:

ChatGPT Enterprise, GitHub Copilot Enterprise, Cursor (sandboxed), Windsurf (sandboxed), Replit AI (containerized), Lovable (containerized), Local encrypted LLMs.

Prohibited:

Auto-GPT, BabyAGI, Devin-style autonomous agents, Gemini Turbo autonomous modes, browser plugins with session-wide monitoring.

© IBS Ventures (SMC-Pvt) Limited

10. Incident Reporting Protocol

If an AI system deletes files, exposes data, sends unauthorized requests, or behaves unpredictably:

1. Stop the process.
2. Disconnect the device/container.
3. Report to Inspurate Governance & Security.
4. Document steps leading to the incident.

11. Policy Review Cycle

This policy is reviewed quarterly based on new AI threats, legal updates, client obligations, and industry best practices.

© IBS Ventures (SMC-Pvt) Limited

Acknowledgment

I acknowledge that I have read, understood, and agree to comply with the **IBS Ventures (SMC-Pvt) Limited AI Acceptable Use & Data Security Policy**.

I understand that:

- I am responsible for all actions taken using AI tools under my login or device.
- I will not input client data, confidential information, or credentials into any public AI system unless explicitly approved.
- I will use AI tools only within IBS Ventures approved environments and follow sandboxing, review, and security procedures.
- I will not allow AI agents to run autonomously or execute commands without human verification.
- I will immediately report any suspected data exposure, security incident, or AI malfunction to IBS Ventures Governance & Security Team.
- I will follow applicable data protection, cybersecurity, and legal compliance requirements including GDPR, CCPA, UK GDPR, PDPA, ISO 27001 principles, and SOC 2 practices.
- Violations of this policy may result in access restrictions, disciplinary action, contract termination, or legal consequences depending on severity.

By continuing to work with Inspurate Business Services as an employee, contractor, partner, or vendor, I confirm my commitment to uphold this policy and protect the confidentiality, integrity, and security of Inspurate and its clients.

Name: _____

Role / Company: _____

Signature: _____

Date: _____

© IBS Ventures (SMC-Pvt) Limited

ANNEXURE DATA PROTECTION, CYBERSECURITY, AND LEGAL COMPLIANCE

This annexure provides expanded detail on the compliance frameworks referenced in the IBS Ventures AI Acceptable Use & Data Security Policy. All team members, contractors, partners, vendors, and clients must follow these standards when interacting with Inspurate systems or data.

A. GDPR — EU GENERAL DATA PROTECTION REGULATION

- Lawful processing of personal data.
- Data minimization: collect only what is necessary.
- Purpose limitation: use data only for the purpose collected.
- Data subject rights: access, correction, portability, deletion.
- Security safeguards: encryption, access control, breach protection.
- Cross-border transfer rules: Standard Contractual Clauses.
- No personal data may be uploaded to public AI tools.

B. CCPA — CALIFORNIA CONSUMER PRIVACY ACT

- Rights: to know, access, delete, and opt out of data selling.
- Transparency obligations regarding data collection and usage.
- Requirement to maintain reasonable security practices.
- Prohibition on selling personal data without explicit notice.
- No personal or identifiable data may be shared with public AI systems.

C. UK GDPR

- Similar to EU GDPR: lawful, fair, transparent processing.
- Accuracy and up-to-date data requirements.
- Restrictions on automated decision-making.
- Safeguards for international transfers.
- Mandatory security controls for personal data.

D. PAKISTAN PDPA — PERSONAL DATA PROTECTION ACT (DRAFT)

- Consent-based processing of personal information.
- Purpose specification and restricted use.
- Possible data localization requirements.
- Mandatory breach notifications.
- Rights of individuals to access and correct personal data.
- Obligation to secure data with appropriate safeguards.

© IBS Ventures (SMC-Pvt) Limited

E. ISO 27001 — INFORMATION SECURITY MANAGEMENT PRINCIPLES

- Access control: MFA, least privilege, role-based permissions.
- Asset management: inventory and classification.
- Cryptographic controls: encryption at rest and in transit.
- Operations security: patching, malware protection, logging.
- Supplier security: assess and manage third-party risk.
- Incident response: documented and tested procedures.
- Business continuity: backup and recovery planning.

F. SOC 2 — TRUST SERVICE CRITERIA

- Security: protection from unauthorized access.
- Availability: system uptime and reliability.
- Processing integrity: accurate and authorized data processing.
- Confidentiality: protection of sensitive information.
- Privacy: handling personal data in line with declared policies.
- Emphasis on logging, monitoring, and auditability.

G. COMMON REQUIREMENTS ACROSS ALL FRAMEWORKS

- Strong access control.
- Encryption and secure storage.
- Data minimization principles.
- Clear purpose limitation.
- Timely breach reporting.
- Vendor and supplier compliance.
- No uploading sensitive or personal data into public AI systems.

H. WHAT THIS MEANS FOR IBS VENTURE TEAM MEMBERS, CONTRACTORS, PARTNERS, AND VENDORS

- Do not upload confidential or client data to public AI tools.
- Follow sandboxing, encryption, and access control practices.
- Report data incidents immediately.
- Follow the Inspurate AUP when coding, designing, communicating, or analyzing data.
- Align with these global principles regardless of region or role.

© IBS Ventures (SMC-Pvt) Limited