SOLEX ENERGY LIMITED

ARTIFICIAL INTELLIGENCE(AI)

ADOPTION & USAGE POLICY

(Reviewed & Adopted by the Board of Directors in its Meeting Dated May 16, 2026)

1800 572 8787 info@solex.in solex.in
REGISTERED & CORPORATE OFFICE:
SOLEX ENERGY LIMITED
8th Floor, 801-812, Rio Empire, Opp. RTO, Pal, Surat, Gujarat, India, 395009
CIN: L40106GJ2014PLC081036

ARTIFICIAL INTELLIGENCE(AI)

ADOPTION & USAGE POLICY

1. Purpose & Objectives

This Policy establishes a controlled, secure, and compliant framework for the use of Artificial Intelligence (AI) tools within Solex Energy Limited (Solex). It aims to:

- Ensure compliance with applicable data protection laws, including the Digital Personal Data Protection Act, 2023 (DPDP Act) and Information Technology Act, 2000.
- Align with SEBI regulations, including LODR and Prohibition of Insider Trading (PIT) Regulations
- Safeguard confidential, personal, and business-critical data
- Enable responsible, transparent, and auditable use of AI technologies

2. Scope

This Policy applies to:

- All employees (permanent, contractual, part-time, and interns), directors, consultants, advisors and third-party service providers of Solex
- All AI tools (internal or external), including but not limited to:
    - Chat-based AI tools
    - Document analysis platforms
    - Data analytics tools
    - Code generation systems

used for any Company business purpose, whether accessed via Company-issued devices, personal devices, or browser-based interfaces.

What this Policy covers

General-purpose AI assistants (e.g. ChatGPT, Claude, Gemini, Copilot); AI-powered coding assistants; AI tools embedded in SaaS platforms (ERP, CRM, HRMS, procurement); AI-driven quality inspection or predictive maintenance tools; and any internally developed AI/ML models processing Company data.

3. Definitions

Artificial Intelligence (AI): Any software or system capable of performing tasks that typically require human intelligence, including text generation, data analysis, and automation. **UPSI (Unpublished Price Sensitive Information):** Information that is not generally available and which upon becoming available is likely to materially affect the price of securities.

Restricted Data: Highly sensitive information including UPSI, personal data, financial information, and proprietary business data.

Shadow AI: Unapproved AI tools used without IT or management knowledge, posing uncontrolled data and security risks.

4. Guiding Principles

All AI usage at Solex shall adhere to the following principles:

- Data Minimization
- Purpose Limitation
- Confidentiality and Security
- Human Oversight
- Accountability and Auditability

5. Data Classification Framework

All data must be classified prior to any use in AI tools:

5.1 Public Data

- Publicly available information such as website content and marketing material
- Permitted for AI usage

5.2 Internal Data

- Internal communications and SOPs
- Permitted with caution and managerial discretion

5.3 Confidential Data

- Contracts, pricing information, internal reports
- Not permitted in external AI tools without explicit approval

5.4 Restricted Data (Strictly Prohibited)

The following data must not be used in any third-party AI tools:

- Unpublished Price sensitive Information-UPSI (financial results, expansion plans, etc.)
- Board and committee materials
- Employee personal data
- Customer and vendor sensitive data
- NDA-protected information
- Proprietary technical or manufacturing data

6. Permitted Use Cases

Employees may use AI tools for:

- Drafting generic communications, policies, and templates
- Public research and knowledge enhancement
- Summarizing non-confidential information

All outputs must be reviewed and validated by the user.

7. Prohibited Use Cases

The following activities are strictly prohibited:

- Uploading confidential or restricted data into AI tools
- Processing UPSI through AI platforms
- Using AI outputs without human validation
- Automated decision-making without oversight
- Sharing AI tool credentials
- Using any AI platform not listed in the policy ("Shadow AI")

8. AI Tool Approval Framework

No AI tool shall be used without prior approval.

8.1 Approval Criteria

- Data storage and processing location
- Data usage for model training
- Security certifications (e.g., ISO 27001, SOC 2)
- Data retention and deletion policies

8.2 Approval Authority

Approval must be jointly provided by:

- IT Department
- Compliance/Legal Department

9. Control Requirements

9.1 Access Controls

- Role-based access to AI tools
- Restricted access for sensitive functions

9.2 Data Protection Controls

- Prohibition on sharing restricted data
- Mandatory anonymization where applicable

9.3 Audit Logging

- Maintain logs of AI tool usage
- Periodic review by Compliance

9.4 Data Retention

- Ensure vendors do not retain or reuse Solex data
- Ensure deletion capabilities are available to specified individual

9.5 Vendor Safeguards

All vendors must contractually agree to:

- No use of Solex data for training models
- Strict confidentiality obligations
- Timely breach notification
- Data deletion upon completion, termination or on request
- Audit rights for Solex

9.6 Incident Response

In case of data exposure:

1. Immediately notify Compliance and IT team
2. Identify impacted data
3. Inform senior management
4. Assess regulatory reporting requirements
5. Document and remediate the incident

10. SEBI Compliance Safeguards

- AI tools must not process UPSI (Unpublished Price Sensitive Information)
- Compliance with Prohibition of Insider Trading (PIT) Code of Conduct must be ensured
- AI usage must not bypass Structured Digital Database (SDD) requirements

11. Employee Responsibilities

All users must:

- Use AI tools responsibly and ethically
- Avoid uploading restricted data
- Verify AI-generated outputs
- Report any misuse or incidents

Non-compliance may result in disciplinary action.

Penalty Matrix (Graded Violations)

Non-compliance with this Policy shall attract disciplinary action based on severity, intent, and impact. The Company reserves the right to escalate actions depending on regulatory exposure.

Level	Nature of Violation	Examples	Action
Level 1 (Minor)	Unintentional / Low Risk	Using AI without approval for generic tasks, minor procedural lapses	Verbal / Written Warning, Mandatory Retraining
Level 2 (Moderate)	Negligence / Repeated Breach	Uploading internal or confidential data (non-critical), repeated violations of policy	Written Warning, Access Restriction, HR Disciplinary Action
Level 3 (Major)	Serious Misconduct	Uploading restricted data, NDA breach, failure to report incident	Suspension of access, Formal Disciplinary Proceedings
Level 4 (Critical)	Regulatory / High Impact Breach	Sharing UPSI, personal data breach, financial data leakage	Termination, Legal Action, Regulatory Reporting (DPDP/SEBI)

Additional provisions:

- Any violation involving **UPSI or personal data** shall be treated as **Level 4 (Critical)** irrespective of intent.
- Repeated violations will automatically escalate to the next severity level.
- The Company may initiate **civil and/or criminal proceedings** where applicable.

12. Governance Structure

Function	Responsibility
Compliance	Policy ownership, regulatory alignment
IT	Tool security, access control, audits, monitoring
HR	Training and awareness

13. Training and Awareness

- Mandatory training for all employees
- Specialized training for Sales, Purchase, Finance, Compliance, and senior management

14. Review and Amendments

This Policy shall be reviewed periodically by the Compliance Department and updated as required to reflect legal, regulatory, or technological changes.

Employee AI Usage Declaration

All employees, consultants, and contractual staff using AI tools must sign the following declaration:

AI USAGE DECLARATION

I, _____, hereby acknowledge that I have read and understood the Solex AI Adoption & Usage Policy.

I confirm that:

1. I will use AI tools only for permitted purposes as defined in the Policy.
2. I will not upload, share, or process any Confidential or Restricted Data (including UPSI, personal data, financial data, or NDA-protected information) on any external AI platform.
3. I will ensure that all AI-generated outputs are reviewed, validated, and approved before use in any official capacity.
4. I understand that any misuse of AI tools may lead to disciplinary action, including termination.
5. I will immediately report any accidental data exposure or policy breach to the Compliance and IT teams.

I agree to comply with all provisions of the Policy and any updates issued from time to time.

Employee Name: _____

Employee ID: _____

Department: _____

Signature: _____

Date: _____