AI Governance Policy

September 2026
Version 1.0
ReNew Energy Global Plc and its subsidiaries (“ReNew”)

Artificial Intelligence (AI) Governance Policy

S. No.	Type of Information	Document Data
1	Document Title	ReNew - Artificial Intelligence (AI) Governance Policy
2	Document Superseded	NA
3	Document Revision No	1.0
4	Document Approver	Board of Directors, ReNew Energy Global Plc

Contents

1. Objective 4
2. Scope & Applicability 4
3. Reference Standards & Alignment 4
4. AI lifecycle and Governance Principles 4
5. AI Risk Classification and Approval 5
6. Data Governance for AI 5
7. Third-Party and Vendor AI 5
8. AI Incident Management and Non-Compliance 5
9. Monitoring, Audit, and Continuous Improvement 5
10. Enterprise AI Governance Committee (AIGC) 6
11. Roles and Responsibilities 6

1. Objective

This policy establishes a comprehensive governance framework for the responsible, secure, ethical, and compliant use of Artificial Intelligence (AI), including Generative AI, across ReNew Energy Global Plc and its subsidiaries ("ReNew"). The policy ensures AI adoption supports business objectives while safeguarding information assets, stakeholders, and regulatory obligations.

2. Scope & Applicability

2.1. This policy applies to ReNew, and all AI systems developed, procured, deployed, or operated by ReNew, including machine learning, predictive analytics, optimization, and Generative AI systems.

2.2. It applies to all employees, contractors, consultants, and third parties across IT, OT, and business functions.

3. Reference Standards & Alignment

3.1. This policy aligns with global standard for AI governance (ISO 42001, NIST AI, EU AI Act. OWASP LLM Top 10), ReNew HR Policy, ReNew ISMS and cybersecurity frameworks.

4. AI lifecycle and Governance Principles

4.1. AI use shall be lawful, transparent, fair, secure, privacy-preserving, and subject to human oversight (humans-in-the-loop), throughout its lifecycle as per the 8 stages use case lifecycle principles of the AIGF and be subjected to regular audits and assessments.

4.2. Any AI system producing outputs that affects employees, customers, or safety-critical operations must have a documented, tested human override procedure. This is mandatory for High/Critical risk tier AI systems.

4.3. ReNew shall pay special attention to ensuring that artificial intelligence systems do not harm health or safety or have a negative impact on intellectual property rights. AI shall be used as a tool in service of the people, fully respecting human dignity and the environment. AI systems developed shall produce outputs which are explainable and traceable.

4.4. ReNew shall also maintain that any stakeholders interacting with AI systems are informed when interacting with AI systems, and AI generated outcomes shall be appropriately identifiable.

4.5. AI must not be used to make or support decisions that discriminate against individuals based on characteristics. ReNew shall encourage employees to actively question AI outputs that appear to treat people differently without justification.

4.6. ReNew shall endeavour to ensure that it provides mandatory training to all employees and stakeholders so as to ensure AI literacy across the organization, especially on aspects required to understand the risks implicit in the use of AI, such as legal and ethical considerations, behavioral aspects and best security practices, to enable the end users of AI tools to use them safely as per established guidelines.

4.7. ReNew shall maintain that any AI system being used is aligned with the established purpose for which it was deployed, avoiding unnecessary or excess risks, therefore, the application of AI systems must remain within reasonable limits to achieve the specific objective that it was intended for, without excessive or unnecessary usage that might go beyond the original established objective.

5. AI Risk Classification and Approval

5.1. AI use cases shall be classified as Low, Medium, or High risk based on impact and complexity.

5.2. High-risk AI systems require approval from the Enterprise AI Governance Committee (AIGC), and All AI system inputs, outputs, decisions, and override events should be logged with immutable timestamps which are accessible to CISO, Legal, and Internal Audit on demand.

6. Data Governance for AI

6.1. AI systems shall be developed from and contain data from datasets that are developed in accordance with data privacy and protection provisions and process data that is approved and complies with standards of quality established by ReNew and accepted by international standards of quality and integrity, as well as respecting intellectual property rights.

6.2. Use of personal or sensitive data requires mandatory prior approval from Legal and Information Security.

7. Third-Party and Vendor AI

7.1. All third-party AI solutions shall undergo mandatory security, privacy, environmental, and legal due diligence prior to deployment as per the guidelines established by AI Governance Framework.

8. AI Incident Management and Non-Compliance

8.1. AI-related incidents including but not limited to misuse of AI by using its designated scope, inputting confidential company/customer/personal data into unapproved tools, or deliberate exfiltration of data using AI tools shall be reported, investigated, and managed under ReNew's incident response and management processes as guided by ReNew's HR Disciplinary Policy, following the escalation mechanism established under the AIGF.

8.2. ReNew shall maintain that any AI usage inside the organization which violates its code of conduct, applicable law or code of ethics shall be reported through appropriate channels:

- Manipulative or deceptive practices that influence user behavior without informed consent
- Exploitation of vulnerabilities of individuals or groups
- Social scoring or profiling leading to unfair disadvantage

9. Monitoring, Audit, and Continuous Improvement

9.1 AI systems shall be periodically reviewed through methods such as internal/external assessments, audits, and other evaluation mechanisms to assess performance, bias, model drift, and security vulnerabilities. These risks shall be mitigated through measures such as penetration testing, encryption, secure coding practices, and prompt shields, with appropriate measures to ensure the traceability of AI tools and systems in place.

9.2 ReNew shall maintain a mandatory live inventory of all AI systems, models, and tools in use across the organization.

9.3. This policy shall be reviewed annually or upon significant regulatory, technological, or business change.

10. Enterprise AI Governance Committee (AIGC)

10.1. The Enterprise AI Governance Committee (AIGC) shall be the apex governance body responsible for oversight, governance, and risk management of AI at ReNew.

10.2. The AIGC shall be chaired by the Chief Digital and Information Officer (CDIO) and shall include representatives from IT, Information Security, Legal & Compliance, Risk, HR, and key Business Functions on a need basis.

10.3 The AIGC is responsible for approving high-risk AI use cases, overseeing AI-related risks and incidents, establishing accountability, ensuring regulatory and ISO alignment, and reporting AI risk posture to senior management and the Board.

10.4 The organisation remains committed to the responsible, secure, and compliant adoption of AI technologies. All AI-related activities shall be governed through approved policies, ethical oversight mechanisms, security controls, and applicable regulatory requirements.

11. Roles and Responsibilities

11.1. Roles and responsibilities for AI governance are defined through a formal RACI model and supporting governance artefacts maintained by the AIGC.

12. Review

This policy shall be reviewed annually or as major changes occur.