Department: CC-IT

ARTIFICIAL INTELLIGENCE USE, SECURITY, PRIVACY AND GOVERNANCE POLICY

POLICY DOCUMENTATION SYSTEM

Approved by:	Competent Authority
Date of Approval:	12.11.2026
Date of Initial Policy Issue:	12.11.2026
Revision number:	1.0
Revision date:	Not Applicable (Initial Issue)
Next Revision Due Date:	11.11.2027, or earlier upon material regulatory, technological or risk change

NTPC Limited

Brief Summary of the Policy

The Policy establishes NTPC's enterprise-wide framework for the responsible, secure, lawful and controlled adoption, development, procurement, deployment and use of Artificial Intelligence (AI). It applies across the AI lifecycle to employees, trainees, consultants, contractors, OEMs and service providers, and covers Generative AI, predictive AI, Large Language Models, AI assistants, Agentic AI, computer vision, AI-enabled cyber security, and AI embedded in enterprise or industrial systems. The core provisions of the Policy are summarized below:

1. Official work may use only NTPC-approved AI tools. Non-public, confidential, cyber-security, plant/OT, legally privileged or restricted information shall not be entered into public or unapproved AI services.
2. AI outputs must be independently reviewed for accuracy, completeness, security, privacy, legal compliance, intellectual property, bias and contextual suitability. AI does not replace human accountability or established approval processes.
3. AI involving plant or operational information shall remain outside the OT control environment and advisory in nature. Autonomous OT actions, control writes and AI-created connectivity to OT are prohibited.
4. AI systems shall follow security and privacy by design, least privilege, threat modelling, secure development, logging, monitoring, adversarial testing, vulnerability management, network segregation and controlled decommissioning.
5. Material AI use cases must be risk-classified, assigned an accountable owner and approved at the appropriate level. High-risk use includes plant-data or OT-adjacent applications, action-capable agents, significant personal-data processing and high-impact decisions.
6. Third-party AI procurement must address NTPC data ownership and confidentiality, processing location, prohibition on vendor model training without authorization, incident notification, audit rights, secure deletion, material changes and supply-chain transparency.
7. AI-related security, privacy, safety or misuse incidents must be reported immediately to CSOC. The Policy is subject to annual review and earlier review upon material regulatory, technological, architecture or threat changes.