Vice President – AI/ML — Job Description

Designation: Vice President – AI/ML

Compensation: Commensurate with experience

Educational Qualification

1. B.Tech./B.E. in Computer Science, Information Technology, Artificial Intelligence, or a related engineering discipline (Must have)
2. M.Tech./M.S. in AI/ML, Computer Science, Data Science, or a related field strongly preferred; Ph.D. in a relevant field desirable
3. Certifications (Desirable): Cloud/architecture professional (AWS/Azure/GCP), MLOps/LLMOps, or programme-management certifications (PMP, PRINCE2, SAFe)

Experience

1. 15+ years of experience in AI/ML, software, or data engineering, with a substantial record of senior technical and organisational leadership
2. Proven experience leading the design, delivery, and operation of AI/ML, Generative AI, or large-scale data-intensive systems in production
3. Extensive people-leadership experience, having led multi-disciplinary engineering and data-science organisations, including managers and technical leads
4. Track record of delivering large, multi-workstream technology programmes to schedule and budget, with accountability for outcomes, quality, reliability, and cost
5. Demonstrated experience owning technology strategy and architecture for an enterprise or platform operating at scale
6. Experience building and scaling high-performing teams, including talent acquisition, capability development, and the management of delivery partners and vendors
7. Strong, current technical grounding in AI/ML and modern software architecture, with the standing to set technical direction and make model and architecture decisions
8. Prior Government/PSU experience is not essential; the ability to operate within public-sector requirements for data protection, sovereign infrastructure, procurement, and audit is expected

Key Responsibilities

Programme Leadership & Strategy

1. Set the vision, strategy, and delivery roadmap for AI/ML services across Digital India platforms and cross-ministerial systems
2. Lead the end-to-end delivery of the programme's portfolio of AI use cases across the capability teams, ensuring timely, high-quality, and measurable outcomes
3. Establish and run programme governance — planning, prioritisation, risk management, and delivery reporting — and present progress and outcomes to NeGD leadership
4. Own the programme budget and cost governance, ensuring efficient use of compute, infrastructure, and manpower against the approved envelope

Technical & Architectural Direction

1. Own the AI/ML technical strategy and target-state architecture across capability teams — Document Intelligence; Conversational & Multilingual AI; Predictive Analytics; Visual AI & Identity Verification; Agentic AI & Workflow Automation; and Fraud & Anomaly Detection

2. Set standards for model selection and build-versus-buy decisions, including the use of open-source and sovereign models, fine-tuning, retrieval-augmented generation, and prompting
3. Act as the design authority for the programme, approving reference architectures, integration standards, evaluation frameworks, and inference and deployment patterns
4. Ensure reusable AI components — APIs, SDKs, model cards, and templates — are produced to a common standard and published for cross-ministry reuse

Organisation & Delivery

1. Mentor the AI teams and the capability-pod leadership, scaling the organisation in line with validated demand
2. Direct and coordinate the programme's functional and technical resources as a single, integrated delivery organisation
3. Establish the operating model, engineering standards, and delivery culture for a fast-growing national AI capability
4. Establish MLOps/LLMOps practices — model lifecycle management, evaluation, monitoring for drift and quality, and reliable, cost-effective inference at production scale

Empanelment, Procurement & Partnerships

1. Govern the engagement of empanelled agencies at the discovered L1 rate card across resource, project, and turnkey modes — including agency selection, performance management, acceptance, and service levels
2. Manage relationships with technology, model, and infrastructure providers, including commercial terms, performance, and risk

Governance, Security & Responsible AI

1. Ensure all AI systems are delivered in line with the Responsible AI framework — risk assessment, human oversight, explainability, evaluation, and audit
2. Ensure security and data protection by design across the programme, in line with MeitY security standards, CERT-In directions, and the Digital Personal Data Protection Act, 2023
3. Ensure the appropriate use of sovereign infrastructure and coordinate with other MeitY agencies where relevant

Technical Competencies

1. **AI/ML & Generative AI:** Strong command of the modern AI stack — large language models, transformer architectures, generative AI, natural language processing, agentic AI, retrieval-augmented generation, computer vision, and classical and predictive machine learning
2. **MLOps & LLMOps:** Model lifecycle management, training and inference pipelines, model registries, evaluation harnesses, monitoring for drift and quality, and reliable production deployment
3. **Solution & Platform Architecture:** Microservices, event-driven and API-based design, model gateways, and multi-cloud, on-premise, and sovereign deployment patterns
4. **Generative AI Systems:** Retrieval-augmented generation pipeline design, vector databases and semantic search, prompt and evaluation strategies, and output safety and guardrails
5. **AI Evaluation & Assurance:** Evaluation frameworks, benchmarking, and red-teaming for accuracy, fairness, robustness, and safety
6. **Cloud & Inference Infrastructure:** Cloud architecture, identity and access management, GPU/accelerator utilisation, scalability and reliability, and observability

7. **Cost Governance:** Unit economics and cost management for compute, training, and inference, and forecasting against a programme budget
8. **Programme & Delivery Management:** Programme governance, portfolio prioritisation, budgeting, risk management, and multi-workstream delivery
9. **Security, Data Protection & Responsible AI:** Access control, encryption, audit, the Digital Personal Data Protection Act 2023, CERT-In directions, MeitY security standards, and the IndiaAI Responsible AI framework
10. **Organisational Leadership:** Organisation design, hiring and capability development, performance management, and the management of delivery partners and vendors
11. **Communication & Stakeholder Engagement:** Executive communication of strategy, progress, and risk; leading technical reviews; and building alignment across technical and functional teams