Charter Document
AI Modernization Leadership Team
Legacy Enterprise Class Data Center
January 2026

1. Purpose

The AI Modernization Leadership Team provides strategic oversight, architectural governance, and cross-functional alignment for the multi-year AI modernization initiative. The team ensures that all decisions reinforce long-term operational, safety, and modernization objectives while enabling a scalable, secure, interoperable, and vendor-neutral AI ecosystem.

2. Mission

To guide the design, deployment, and lifecycle management of the enterprise AI ecosystem by establishing standards, managing risk, and ensuring alignment across IT, OT, operations, data, cybersecurity, and compliance functions.

3. Scope of Authority

The Leadership Team is authorized to:

- Define and enforce the vendor-neutral reference architecture
- Approve use cases, prioritization, and deployment sequencing
- Establish data governance, security, and interoperability standards
- Oversee vendor selection and ensure vendor accountability
- Resolve cross-functional conflicts and escalate major risks
- Ensure alignment with the enterprise modernization roadmap
- Govern the AI lifecycle, including MLOps and model deployment

The team holds decision-making authority over architecture, standards, and strategic direction for all AI initiatives.

4. Responsibilities

Strategic Responsibilities

- Maintain the long-term vision for AI modernization
- Ensure alignment with operational, safety, and business objectives
- Prioritize use cases based on value, feasibility, and risk

Architectural Responsibilities

- Maintain the vendor-neutral reference architecture
- Define edge, core, and cloud roles and boundaries
- Ensure interoperability across systems and vendors

Operational Responsibilities

- Validate operational readiness for deployments
- Ensure solutions integrate with yard, wayside, and locomotive workflows
- Oversee change management and workforce impact

Data & AI Responsibilities

- Govern data quality, lineage, and retention
- Oversee model lifecycle, drift monitoring, and retraining
- Ensure MLOps practices are standardized and repeatable

Cybersecurity & Compliance Responsibilities

- Enforce zero-trust principles
- Maintain OT/IT segmentation
- Ensure FRA, DOT, TSA, and internal compliance requirements are met

Risk & Value Responsibilities

- Identify and mitigate technical, operational, and vendor risks
- Track ROI and long-term value realization
- Ensure financial transparency and budget alignment

5. Team Composition

The Leadership Team includes representatives from:

- Strategic Owner / Chair
- Operations
- IT & Infrastructure
- OT & Industrial Systems
- Data & AI
- Cybersecurity
- Compliance & Safety
- Finance & Value Realization

Each representative is accountable for decisions within their domain and for contributing to cross-functional governance.

6. Operating Model

Meeting Cadence

- Bi-weekly leadership team meetings
- Monthly executive steering updates
- Quarterly architecture and roadmap reviews

Decision-Making

- Consensus-driven decision process where possible
- Chair holds final authority when consensus cannot be reached
- Major decisions documented and communicated to stakeholders

Documentation

- Architecture standards
- Governance policies
- Risk registers
- Roadmaps and deployment plans
- Vendor performance evaluations

7. Success Criteria

The Leadership Team is successful when:

- The AI ecosystem is scalable, secure, and interoperable
- Deployments improve safety, reliability, and operational efficiency
- Vendor lock-in is avoided and competitive flexibility is maintained
- Data governance and MLOps practices are standardized
- Risks are proactively managed and mitigated
- The initiative delivers measurable long-term value

8. Charter Review

This charter will be reviewed periodically to ensure continued alignment with evolving operational needs, the technology landscape, and the enterprise modernization strategy.