Artificial Intelligence Governance Policy. V1.1

1. Purpose and Objective

The purpose of this AI Governance Policy ("Policy") is to establish the overarching governance framework for all AI systems and initiatives in the organisation. The Policy requires that AI be developed, deployed, and maintained ethically, transparently, and in alignment with the organisation's values, strategic priorities, and risk appetite. It defines organisational structures, roles, decision authorities, and oversight mechanisms to achieve responsible and effective AI governance. *(GL-1)*

2. Scope

2.1 Applicability. This Policy applies to all AI initiatives, projects, products, and services developed or utilised by the organisation, including but not limited to:

- Proprietary AI models built in-house.
- Third-party AI tools integrated into operational processes.
- Pilot or proof-of-concept AI deployments within any business unit.

All business units, teams, and individuals who plan, develop, manage, or support AI solutions must comply with this Policy to ensure consistent governance across diverse projects.

2.2 Exclusions. Certain low-risk or experimental AI activities may be granted limited exceptions if they do not pose significant material, legal, ethical, or operational risks. All requests for exceptions must follow the procedures outlined in Section 19 of this Policy.

2.3 Related Policies. This Policy complements and should be read in conjunction with the AI Governance Policy and any other corporate policies pertaining to data protection, information security, ethics, and compliance. *(GL-3)*

This Policy supports and is supported by the following additional policies, which you must consult where relevant:

- AI Risk Management Policy (RM-1)
- AI Model and Data Lifecycle Management Policy (LC-1)
- AI Incident Management and Response Policy (IM-1)
- AI Innovation and Responsible Use Policy

3. Definitions

For the purposes of this Policy, the following definitions apply in addition to definitions provided in the related policies:

1.1 Artificial Intelligence (AI): For the purposes of this policy, AI refers to any engineered or machine-based system that generates outputs—such as predictions, recommendations, or decisions—based on a set of objectives. These systems may operate with varying levels of autonomy. *(GL-1)*

1.2 AI Model: An AI model is any component that implements AI technology using computational, statistical, or machine-learning techniques to produce outputs from inputs. *(LC-2)*

1.3 AI System: Any software application employing Artificial Intelligence, generally comprised of a combination of models, datasets, interfaces and agents deployed on a computing infrastructure. *(GL-2)*

1.4 AI Incident: An AI incident refers to any event where an AI system operates outside its defined parameters, violates policy requirements, or potentially impacts stakeholders in unintended ways. All incidents must be documented and reviewed in accordance with Section 10. *(IM-1)*

4. Policy Statement

4.1 This policy establishes mandatory requirements for overseeing, directing, and controlling AI development and use within our organisation. It ensures that all AI initiatives are developed and deployed in a responsible, transparent, and ethical manner while supporting the business objectives and maintaining operational efficiency.

4.2 The organisation is committed to a structured, transparent, and accountable approach to AI governance. This Policy encourages innovation in AI by providing a safe and clearly defined framework for experimentation, development, and deployment.

5. Responsible AI Objectives

The objectives of our Responsible AI approach include:

5.1 System Trustworthiness and Reliability: All AI systems must maintain documented performance metrics with defined thresholds for accuracy and reliability. System owners are required to implement continuous monitoring protocols to detect and address model drift. *(GL-1, OM-1)*

5.2 Fairness and Bias Prevention: System owners must conduct bias impact assessments prior to deployment and on a quarterly basis thereafter. All AI systems shall undergo testing across diverse user populations and scenarios before approval for production. *(RS-5)*

5.3 Transparency and Explainability: Every AI system must provide explanations for its decisions that are appropriate to its intended audience. Comprehensive documentation and audit trails must be maintained for all significant system decisions and changes. *(RS-4, LC-4)*

5.4 Security and Privacy Protection: AI systems shall incorporate privacy-by-design principles and undergo thorough security assessments before deployment. System owners are required to conduct quarterly security reviews and maintain data protection measures that meet or exceed organisational standards. *(SE-3, PR-1)*

5.5 Social Impact: The AI Governance Committee will assess the broader societal implications of each AI system before deployment. System owners must implement mechanisms for stakeholder feedback and demonstrate how this input informs system development and operation. *(CO-2)*

6. Governance Structure

6.1 Executive Oversight: The Chief Technology Officer (CTO) shall serve as chair of the AI Governance Committee, which meets monthly to set strategic direction, approve major AI initiatives, and define risk thresholds. *(GL-1, GL-3)*

6.2 Operational Management: The AI Operational Committee, consisting of the AI Governance Lead, two Senior Engineers, and a Risk Specialist, convenes bi-weekly to oversee AI developments, monitor performance, and manage operational risks. Issues exceeding routine parameters are escalated to the AI Governance Committee. *(RM-4, RO-2)*

6.3 Decision Authority:
A three-tier decision framework is established:

- **Tier 1:** Technical teams manage routine operational decisions within documented parameters. This includes day-to-day model monitoring, model and data lifecycle management, and incident response ensuring all actions stay within the boundaries set by organisational policies. Teams must escalate risks, issues and decisions app *(GL-2)*
- **Tier 2:** The Operational Committee reviews and approves significant changes to existing systems. This committee must evaluate potential impacts on performance, compliance, or user experience and confirm alignment with established risk tolerances before granting approval. The Committee must also evaluate the ethical and societal implications of AI initiatives, in coordination with stakeholders. *(RM-3, RO-1)*
- **Tier 3:** The AI Governance Committee sets policy and approves major AI initiatives, defines risk thresholds, reviews incidents and emerging risks, provides final review and approval of new system deployments and high-impact model usage. The Committee receives reports from the Operational Committee and other stakeholders to ensure policy alignment. (GL-3). The AI Governance Committee must also evaluate the ethical and societal implications of AI initiatives, in coordination with stakeholders.

7. Roles and Responsibilities

- **Chief Technology Officer (CTO):** Provides executive oversight, chairs the Governance Committee, and approves final policy changes. (GL-1). Ensures alignment of AI governance directives with corporate strategy.
- **AI Governance Lead:** Coordinates the implementation of the AI governance framework across the organisation. (GL-2). Acts as the central point of contact for governance-related queries, facilitates the work of the Governance and Operational Committees, maintains the policy framework, and drives education and capability uplift in AI governance practices. Supports cross-functional alignment on risk and assurance expectations and ensures traceability of controls across the AI system lifecycle.
- **System Owners:** Ensure lifecycle compliance, maintain system documentation, and report issues to the Operational Committee. (LC-2). Serve as primary contacts for audits or queries related to their systems.
- **Legal and Compliance:** Advise on legal and regulatory requirements and evaluate third-party AI procurement for legal risk. (RO-1). Must be consulted before finalising contracts with external AI vendors or services.
- **Data Protection Officer (DPO):** Oversees data privacy controls and ensures GDPR and similar regulatory compliance. (PR-1). Coordinates with the Operational Committee on data handling concerns post-deployment.
- **Internal Audit:** Conducts independent audits of AI compliance and system behaviour across lifecycle phases. (AA-1). Reports findings to the Governance Committee, providing unbiased assessments.
- **Engineers and Data Scientists**: Ensure AI systems are developed in accordance with this Policy, including related policies (LC-3). Responsible for documentation of training data sources, model design rationale, performance metrics, and ethical considerations. Must collaborate with System Owners to support audit readiness and explainability requirements.

8. Risk Management

The Organisation adopts a structured approach to managing risks associated with AI systems. This Policy defers to the AI Risk Management Policy for detailed procedures but establishes the following overarching governance expectations:

8.1 Risk Policy Application. All AI systems are subject to the organisation's AI Risk Management Policy, which defines the processes for identifying, classifying, mitigating, and monitoring AI-specific risks. (RM-1).

8.2 Risk Appetite and Tolerance Alignment. AI initiatives must align with the organisation's declared AI risk appetite and tolerance thresholds. High-risk systems must demonstrate appropriate mitigation measures and be escalated to the Risk Management Committee for approval. (RM-1, RM-2)

8.3 System Classification. AI systems must be categorised according to their risk profile using the framework set out in the Risk Management Policy. Classification governs the level of governance, oversight, and control required across the system lifecycle. (RM-2)

8.4 AI Governance Committee Oversight. The AI Governance Committee retains oversight responsibility for risk-related escalations and reviews summary reports from the Risk Management Committee on adherence to risk thresholds and emerging issues. (GL-1)

8.5 Delegated Implementation. The Risk Management Committee is accountable for operationalising risk management activities, including risk reviews, control validation, and continuous improvement of the risk framework. This includes maintaining the AI Risk Register and ensuring lessons learned are integrated into practice. (RM-3, RM-4)

9. Model & Data Lifecycle Management

AI initiatives must conform to the requirements set out in the AI Model and Data Lifecycle Management Policy, which defines the operational controls for model and data governance from inception to retirement. The following overarching statements provide governance-level direction:

9.1 Model Lifecycle Ownership. All AI models—whether developed internally or acquired from third parties—must comply with formal lifecycle requirements, including data sourcing, model validation, deployment protocols, and decommissioning. Oversight responsibilities are assigned to Model Owners and reviewed by the AI Operational Committee. (LC-1, LC-2)

9.2 Documentation and Traceability. Lifecycle documentation must be complete, version-controlled, and centrally retained. This includes data descriptions, validation results, deployment logs, and performance monitoring records, enabling auditability and traceability across the AI system's lifecycle. (LC-4)

9.3 Approval and Oversight of High-Impact Models. High-impact or novel models require formal validation and may only be deployed following review by the AI Governance Committee. The AI Operational Committee is responsible for validating standard models and ensuring ongoing operational compliance. (GL-3, RM-3)

9.4 Monitoring and Feedback Integration. Deployed AI systems must be continuously monitored for performance, fairness, and compliance. Where issues arise or drift is detected, retraining or rollback actions must follow the same controls and documentation as original deployments. (OM-1, RM-4)

9.5 Model Retirement Obligations. All models must be formally retired when obsolete, ensuring proper archival, deletion, and transition steps. Lessons learned during decommissioning must be documented to support continuous improvement across future initiatives. (LC-2, RM-4)

9.6 Escalation and Enforcement. Non-compliance with lifecycle controls—such as skipping validation, omitting monitoring, or failing to manage datasets responsibly—will trigger review by the AI Governance Committee and may result in rollback, access restrictions, or disciplinary action. (AA-1)

10. Incident Management and Response

The Organisation requires that all AI incidents—defined as events in which an AI system behaves in a way that is unsafe, unintended, or in breach of policy—be managed in accordance with the AI Incident Management and Response Policy. The following governance requirements are binding on all teams developing, deploying, operating, or overseeing AI systems:

10.1 Mandatory incident activation and escalation. All AI incidents rated Level 3 (High) or Level 4 (Critical) must trigger formal response activation within 30 minutes of confirmation. The AI Technical Lead is responsible for convening the Incident Response Team and ensuring containment actions begin immediately. Critical incidents must be escalated to the AI Governance Committee and Chief Technology Officer without delay. (IM-1, IM-2)

10.2 Responsibility for Detection and Logging. System Owners must ensure that monitoring systems are in place to detect anomalies, drift, or misuse consistent with expected AI failure modes. All suspected incidents must be recorded in the AI Incident Register, including a preliminary severity rating and triage decision. Failure to log incidents may constitute a governance breach. (IM-1)

10.3 Root Cause Analysis and Remediation. All incidents rated Moderate or higher must undergo formal root cause analysis, led by the AI Technical Lead and supported by affected teams. Findings must be documented in a Post-Incident Report, including timeline, system impacts, contributing factors, and corrective actions. These reports must be reviewed by the AI Operational Committee and submitted to the AI Governance Committee for all Level 4 incidents. (IM-2)

10.4 Control Improvement and Knowledge Integration. Remediation is not complete until systemic improvements are implemented. Responsible teams must update controls, checklists, monitoring thresholds, or training procedures as identified through investigation. For Level 3–4 incidents, a structured lessons-learned workshop is mandatory, and outputs must be embedded into lifecycle policies, audit criteria, and future risk assessments. (IM-3)

10.5 Governance Committee Oversight and Accountability. The AI Governance Committee retains accountability for the integrity of incident response across the Organisation. It must review all critical incident reports, endorse systemic remediations, and escalate to Executive Leadership or the Board as required. The AI Operational Committee is responsible for tracking lower-severity incidents and verifying timely resolution of all recommended actions. (GL-3, IM-2)

11. Responsible Use and Training Requirements

All personnel must adhere to the Organisation's expectations for responsible AI use, as defined in the AI Innovation and Responsible Use Policy. This section establishes mandatory governance obligations related to training, competency, and oversight of day-to-day AI usage across the Organisation.

11.1 Mandatory Training and Competency Requirements. All employees and contractors involved in the design, development, deployment, or use of AI systems must complete role-specific training on responsible AI use. Training must cover acceptable and prohibited use, privacy and security safeguards, fairness principles, and accountability for outputs. Human Resources, in coordination with the AI Governance Committee, is responsible for maintaining defined competency requirements for AI-related roles and ensuring these are assessed at least annually. (RS-1)

11.2 Policy Familiarity and Ongoing Awareness. All employees—regardless of technical background—must familiarise themselves with the AI Innovation and Responsible Use Policy prior to using AI tools for work purposes. Refresher training or updates must be completed when major policy changes occur or new tools are introduced. Managers are accountable for ensuring their teams understand and apply this Policy in day-to-day work. (RS-1, GL-3)

11.3 Use of AI Tools in Daily Work. Employees are permitted to use approved AI tools to support communication, ideation, coding, summarisation, and decision support—but must remain accountable for reviewing and validating all outputs. AI-generated content must not be treated as factually correct or confidential without human verification. Under no circumstances should employees allow AI systems to make final decisions in high-consequence domains (e.g., hiring, compliance, legal advice) without appropriate review and authorisation. (RS-5, RO-1)

11.4 Prohibited AI Practices. The use of AI systems to impersonate individuals, misrepresent content, expose sensitive data, or generate discriminatory, unsafe, or misleading outputs is strictly prohibited. Employees must not use unapproved or public AI tools to process internal, proprietary, or personally identifiable information unless those tools have been approved for secure use. (PR-1, RO-1)

11.5 Reporting and Escalation of Concerns. Any suspected misuse of AI, inappropriate outputs, or unapproved tool usage must be promptly reported to a manager or the AI Governance Committee. Good faith reporting is encouraged, and no employee will face adverse consequences for appropriately raising responsible use concerns. Escalation mechanisms must be accessible and well-publicised to support a culture of safe experimentation. (IM-3, GL-3)

12. Documentation and Regulatory Compliance

12.2 AI System Inventory. Every System Owner shall ensure their system is recorded within the central inventory of all AI systems, including those in development, production, or decommissioned. (GL-2) The inventory must contain: System name, owner, and purpose; current status and risk classification; date of last review. System Owners are responsible for updating this inventory in real time, especially after major changes or reclassifications.

12.1 System Documentation. Every AI system must maintain up-to-date documentation, including system specifications, risk assessments, performance metrics, and incident response procedures. Documentation must be reviewed quarterly and audited annually by the AI Governance Committee. *(LC-4)*

12.3 Compliance Monitoring: The Chief Compliance Officer shall designate an AI Compliance team responsible for monitoring applicable regulations and providing monthly updates to the AI Governance Committee. (RO-1)

12.4 Regulatory Impact Assessments: Quarterly regulatory impact assessments must be conducted for all AI systems. System owners must implement necessary compliance actions within 60 days unless an extension is granted. (RO-2)

12.5 Cross-Border Requirements: AI systems operating across multiple jurisdictions must comply with the most stringent applicable regulations. The AI Compliance team must approve all cross-border deployments. (RO-3)

12.6 Compliance Monitoring: The Compliance team shall conduct monthly reviews of system metrics and quarterly assessments of governance effectiveness. High-risk systems require annual external validation, with all findings documented to support ongoing compliance. *(AA-1)*

12.7 Compliance Reporting: The AI Compliance team shall produce monthly compliance status reports detailing metrics, gaps, and remediation efforts. (RO-4)

13. Procurement Standards

13.1 Vendor Assessment and Selection: The Procurement team shall assess all AI vendors against established technical and responsible AI criteria. Vendors must meet minimum standards in security, privacy, and model governance before approval. *(TP-1)*

13.2 Vendor Monitoring: System owners shall conduct quarterly performance reviews of all AI vendors, ensuring compliance with service level agreements and security requirements. Vendors are required to provide monthly performance reports and participate in quarterly review meetings. *(TP-2)*

14.3 Third-Party Validation: High-risk AI systems procured from vendors must undergo independent third-party validation before deployment. *(TP-2)*

14.4 Contractual Requirements: All contracts with AI vendors must include specific performance metrics, audit provisions, and incident response obligations. The Legal team shall review all contracts to ensure appropriate risk allocation and governance rights. *(TP-1)*

14. Human-AI Interaction

14.1 Disclosure Requirements: All AI systems must clearly disclose their automated nature to users, with user interfaces that detail capabilities and limitations in clear language. *(RS-4)*

14.2 Oversight Protocols:
System owners must establish oversight protocols that correspond to the risk level of each AI system. High-risk systems require active human monitoring during operation, and all oversight decisions must be documented. *(RS-1)*

15. Stakeholder Engagement, Ethics and Impact Assessment

15.1 Consultation Requirements: Before deploying new AI systems or making significant changes, system owners must consult with affected stakeholders and document all relevant feedback. *(CO-2)*

15.2 External Engagement: The organisation shall maintain active engagement with regulatory bodies, industry groups, and other relevant stakeholders. The AI Governance Committee is responsible for reviewing and approving public communications about AI systems. *(CO-2)*

15.3 Ethics Review Board: The organisation shall maintain an AI Ethics Review Board, composed of technical, legal, ethical, and domain experts. The Board must review all new AI systems and significant changes, documenting all decisions in an ethics review register. *(RS-5)*

15.4 Impact Assessment Process: System owners must conduct comprehensive impact assessments before deploying any AI system. The Ethics Review Board reviews these assessments and may require additional controls prior to approval. *(RS-2)*

15.5 Ethical Decision Framework: The Board shall maintain a documented ethical decision framework aligned with organisational values, ensuring that all AI initiatives are ethically justified. *(RS-4)*

15.6 Ongoing Impact Monitoring: System owners must continuously monitor deployed systems for unintended consequences and report any ethical concerns to the Ethics Review Board within 24 hours. *(RS-3)*

16. Testing and Validation

16.1 Testing Requirements: The AI Technical Lead shall establish comprehensive testing protocols covering technical performance, security, fairness, and ethical implications. Detailed test documentation must be maintained. *(AA-1)*

16.2 Validation Protocols: Independent validation teams shall review all high-risk AI systems prior to deployment. Validation confirms compliance with policy requirements and organisational standards, with outcomes and remediation actions documented. *(AA-2)*

16.3 Testing Environments: Separate environments for development, testing, and production must be maintained to ensure representative testing conditions while protecting sensitive data. The AI Technical Lead must approve all configurations.

16.4 Acceptance Criteria: The AI Operational Committee shall define specific acceptance criteria for each AI system. No system shall proceed to deployment without documented evidence that these criteria have been met.

17. Assurance and Audit

17.1 Internal Audit Processes: Regular internal audits must be conducted to verify compliance with this policy. These audits assess risk management, data governance, and operational procedures. *(AA-1)*

17.2 External Validation: High-risk AI systems shall undergo independent external validation annually to provide an objective assessment of system performance and compliance. *(AA-2)*

17.3 Audit Reporting and Remediation: All audit findings must be documented, with corrective actions tracked until resolved. The AI Governance Committee shall review audit reports quarterly. *(AA-3)*

18. Continuous Improvement and Change Management

18.1 Feedback Mechanisms: Establish formal channels for collecting feedback from technical teams, end users, and external stakeholders. This feedback informs ongoing policy adjustments. *(OM-3)*

18.2 Regular Reviews and Updates: The policy shall be reviewed annually, with ad hoc updates as necessary to address emerging challenges. *(OM-3)*

18.3 Integrated Change Management: All significant changes to AI systems must follow a documented change management process, with modifications logged and approved. *(LC-5)*

19. Exceptions and Exemptions

All requests for exceptions to this Policy must be documented and submitted to the CTO. Each request must include a clear justification of the business need, potential risks, alignment with the organisation's risk appetite, and any compensating controls to be implemented. The CTO may grant temporary or conditional exemptions at its discretion if the overall risk remains acceptable.

20. Policy Review

20.1 Formal Annual Review: The AI Governance Committee shall conduct a comprehensive review of this policy at least once per year. All proposed changes require CTO approval and must be communicated to all stakeholders. (OM-3)

20.2 Ad Hoc Updates: In addition to scheduled reviews, the policy shall be updated promptly when significant technological, operational, or regulatory changes occur.

Approved by:

[Name], Chief Technology Officer

Date:
[Date]