Artificial Intelligence Governance Policy. V1.0

1. Definitions

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: An AI system encompasses any data system, software, hardware, application, tool, or utility that operates wholly or partially using AI technology. *(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)*

2. Purpose and Scope

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 maintaining operational efficiency. The objectives of our Responsible AI approach include:

2.1 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)*

2.2 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)*

2.3 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)*

2.4 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)*

2.5 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)*

3. Governance Structure

3.1 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)*

3.2 Operational Management: The AI Operational Committee, consisting of the AI Technical 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 Governance Committee. *(RM-4, RO-2)*

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

- **Tier 1:** Technical teams manage routine operational decisions within documented parameters. *(GL-2)*

- **Tier 2:** The Operational Committee reviews and approves significant changes to existing systems. *(RM-3, RO-1)*
- **Tier 3:** The Governance Committee provides final approval for new system deployments and major architectural changes. *(GL-1, GL-3)*

4. Data Management

Our data management practices ensure that all data is collected, validated, and maintained according to stringent standards described in the Model and Data Lifecycle Standard.

4.1 Data Governance: The Data Governance team is responsible for establishing and maintaining quality standards for all AI training and operational data. Processes for data collection, including consent management, must be implemented. The AI Technical Lead oversees quarterly data quality assessments. *(LC-1)*

4.2 Data Lifecycle Management:
System owners shall document procedures for data retention, archival, and secure disposal in line with organisational and regulatory requirements. All AI systems must have access controls to limit data availability to authorised personnel. *(LC-2, LC-4)*

5. Risk Management

Effective risk management is central to our AI governance framework. We ensure that risks are identified, assessed, and mitigated continuously according to the Risk Management Policy which should be read in conjunction with this Policy.

5.1 Assessment Requirements: Every new AI system must undergo a formal impact assessment before deployment. System owners shall conduct quarterly risk reviews and maintain continuous monitoring protocols. (RM-1, RM-4)

5.2 Risk Thresholds: The AI Governance Committee shall establish risk thresholds for all AI systems. High-risk systems require Committee approval for any significant changes, and system operation must be paused immediately if critical risks are detected. *(RM-2, RM-3)*

6. Procurement Standards

6.1 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)*

6.2 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)*

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

6.4 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)*

7. Regulatory Compliance

7.1 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)

7.2 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)

7.3 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)

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

8. Model Operations

8.1 Performance Monitoring: System owners shall establish performance thresholds for each AI model, including metrics for accuracy, fairness, and drift. Automated monitoring systems must trigger alerts within 15 minutes of threshold violations. *(OM-1)*

8.2 Model Maintenance: The AI Technical Lead shall define criteria for model retraining. Models must be retrained when performance degrades or at set intervals, with all updates subjected to documented testing and approval. *(OM-1, LC-2)*

8.3 Version Control: Comprehensive version control must be maintained for all models, training data, and documentation. Each production model requires a unique identifier linked to its training data and parameters. Quarterly audits of version control are mandatory. *(LC-4, LC-5)*

8.4 System Retirement: System owners shall develop decommissioning plans that address data archival, stakeholder notification, and transition procedures. Retirement plans require approval by the AI Governance Committee and must be reviewed within 30 days of decommissioning. *(LC-4)*

9. Training Requirements

9.1 Employee Training: All personnel involved in AI development or deployment must complete role-specific training programs. Training materials shall be updated quarterly to ensure teams maintain current certifications and knowledge. *(RS-1, PR-1)*

9.2 Competency Management:
Human Resources shall maintain defined competency requirements for all AI-related roles and conduct annual assessments. *(RS-1)*

10. Documentation and Compliance

10.1 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)*

10.2 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)*

11. Project Management

11.1 Lifecycle Governance: Project teams must secure documented approval at each major lifecycle stage. The AI Operational Committee shall review design documents, test results, and deployment plans before work proceeds, maintaining a complete audit trail of all decisions. *(LC-5)*

11.2 Change Management: All significant changes to AI systems require prior approval from the Operational Committee. Teams must document the rationale, test results, and risk assessments associated with each change. Emergency changes must undergo a post-implementation review within 24 hours. *(LC-5)*

12. Incident Management

12.1 Incident Response:
Teams must initiate incident response procedures within 30 minutes of detecting an AI incident. The AI Technical Lead shall assess incident severity and escalate issues according to predefined thresholds. *(IM-1)*

12.2 Incident Documentation:
Detailed incident logs—including detection methods, response actions, and resolution steps—must be maintained. The AI Governance Committee shall review all critical incidents within 24 hours, and incident metrics shall be integrated into quarterly risk assessments. *(IM-2)*

13. Human-AI Interaction

13.1 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)*

13.2 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)*

14. Stakeholder Engagement

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

14.2 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. Ethics and Impact Assessment

15.1 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)*

15.2 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)*

15.3 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)*

15.4 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. Policy Review

19.1 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)

19.2 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]
