**AI Risk Management Policy**

# Policy Objective

The purpose of this AI Risk Management Policy is to ensure that all Artificial Intelligence (AI) systems developed, deployed, or used by the organization are safe, secure, fair, transparent, and aligned with both organizational goals and applicable laws and regulations. The policy provides a structured approach to managing AI-related risks while promoting innovation, accountability, and trust.

# Scope

This policy applies to all AI systems, applications, and tools developed, acquired, or deployed within the organization. It covers internal and external use cases, third-party AI services, and partnerships where AI technologies are integrated into organizational processes or customer-facing products.

# Governance Structure

Effective governance is essential to managing AI risks. The following roles and responsibilities are defined:

**- Executive Leadership:** Approves the AI Risk Management Policy and oversees strategic alignment.

**- AI Governance Committee:** Provides oversight, risk review, and ensures compliance with standards and regulations.

**- AI Risk Owners:** Assigned individuals responsible for identifying, assessing, and mitigating risks in their respective domains.

**- All Employees:** Must adhere to the policy and report potential AI-related risks or incidents.

# Risk Categories

The organization recognizes that AI systems may introduce unique risks. The following categories are prioritized for effective governance:

**a) Ethical and Bias Risks**AI systems may unintentionally reflect or amplify bias in training data, leading to unfair outcomes such as discrimination against individuals based on gender, race, or socioeconomic status. Ethical risks also include lack of transparency, explainability, or accountability in AI decision-making. Left unmanaged, these risks can harm customer trust, violate regulations, and damage the organization’s reputation.  
*Mitigation includes*: bias testing, fairness audits, ensuring diverse training datasets, and embedding human oversight in sensitive decisions.

**b) Operational and Technical Risks**Operational risks arise from failures in the design, deployment, or functioning of AI systems. If not managed effectively, these risks may disrupt business processes, reduce efficiency, and lead to financial or reputational damage.

Key Operational Risk Areas:

* **System Downtime & Performance Issues:** Unexpected outages, scaling problems, or resource bottlenecks that impact availability.
* **Model Versioning:** Inadequate version control may result in multiple, inconsistent models being deployed, reducing reliability and traceability.
* **Data Lineage:** Lack of transparency over the origin, transformation, and usage of data may compromise trust, accountability, and compliance.
* **Change Management:** Uncontrolled updates to datasets, algorithms, or system configurations can introduce errors or misaligned outputs.
* **Third-Party Dependencies:** Reliance on external AI tools or APIs introduces risks if vendors fail to maintain security, uptime, or compliance.

*Mitigation includes*: adoption of MLOps practices, proper documentation of data lineage, robust version control systems, staged deployment pipelines, fallback/manual processes, and well-defined change approval workflows.

**c) Security and Privacy Risks** AI systems may become targets for cyber threats such as adversarial attacks, data poisoning, model theft, or unauthorized access to sensitive data. Security vulnerabilities can compromise both the integrity of AI models and the privacy of user data, leading to legal and compliance violations.  
*Mitigation includes*: applying encryption and access controls, regular penetration testing, monitoring for adversarial inputs, and aligning with the organization’s overall cybersecurity framework.

### **d) Strategic and Business Risks**

AI adoption may expose the organization to broader business and strategic challenges. Over-reliance on a single AI vendor may cause **vendor lock-in**, increasing costs and reducing flexibility. Misalignment of AI strategy with business objectives may lead to wasted investment, operational inefficiencies, or loss of competitive advantage. Poorly governed AI initiatives may also harm stakeholder confidence and shareholder value.

**Mitigation includes:** diversifying AI providers, aligning AI strategy with corporate goals, conducting cost–benefit analyses, and ensuring board-level oversight of major AI initiatives.

### **e) Regulatory and Reputational Risks**

Failure to comply with emerging AI regulations (e.g., EU AI Act, GDPR, PCI DSS, or industry-specific standards) can result in significant fines, sanctions, or litigation. Beyond legal penalties, organizations risk reputational harm if AI systems are perceived as unsafe, biased, or misused. Publicized failures can erode trust among customers, regulators, and the public.

**Mitigation includes:** proactive monitoring of regulatory developments, periodic compliance audits, transparent reporting on AI practices, and crisis communication strategies to manage reputational impact.

# Risk Assessment Process

The organization follows a structured and measurable process to assess and manage AI-related risks.

**Note: The scoring model and methodology may vary**

**1. Identification** Risks are identified through multiple channels, including system audits, technical testing, stakeholder feedback, incident reports, and compliance reviews.

**2. Quantitative Evaluation** Each identified risk is scored using a **Likelihood × Impact score**, resulting in a **Risk Score between 1 and 25**.

* **Likelihood (1–5):** Probability of risk occurrence, from Rare (1) to Almost Certain (5).
* **Impact (1–5):** Severity of consequences, from Minor (1) to Critical (5).

**3. Risk Thresholds and Response Levels**

* **Low Risk:** Acceptable; monitor regularly, no immediate action required.
* **Medium Risk:** Requires mitigation planning within a defined timeline.
* **High Risk:** Requires immediate corrective actions and escalation to the AI Governance Committee.
* **Critical Risk:** Urgent executive review; AI system may be paused, restricted, or decommissioned until resolved.

**4. Prioritization** Risks are ranked by score, ensuring resources are allocated efficiently, with **Critical and High risks** addressed first.

**5. Documentation and Review** All risk evaluations, scoring, and mitigation measures are recorded in the **AI Risk Register** and reviewed at least quarterly to ensure transparency and accountability.

# Mitigation Strategies

To reduce AI risks, the organization adopts the following mitigation measures:

**- Data protection controls** including anonymization, encryption, and access restrictions.

**- Regular bias and fairness testing** of AI models.

**- Human-in-the-loop oversight** for high-risk AI decisions.

**- Incident response procedures** to manage and report AI-related issues.

**- Continuous monitoring and retraining of models** to prevent drift and performance decline.

**For a detailed breakdown of mitigation strategies, refer to the ‘Control Library’ document.**

# Implementation and Monitoring

The implementation of this policy will follow a phased approach, with timelines defined by the AI Governance Committee. Monitoring will be ongoing, with quarterly reviews conducted to evaluate policy effectiveness. Adjustments will be made in line with technological advancements, regulatory changes, and organizational needs.

## AI System Lifecycle Management

To ensure AI systems remain safe, reliable, and compliant, the organization manages them across their full lifecycle, from development through decommissioning.

## Lifecycle Phases

1. **Development:** All AI models must follow secure coding practices, data quality checks, and ethical design principles.
2. **Testing & Validation:** Before deployment, models undergo rigorous testing for accuracy, bias, security vulnerabilities, and regulatory compliance.
3. **Deployment:** Only approved models are deployed into production, with version control and rollback mechanisms in place.
4. **Monitoring & Maintenance:** Continuous monitoring detects drift, bias, or anomalies. Models are retrained or adjusted as required.
5. **Change Management:** Any updates to models, datasets, or parameters must go through a documented approval and testing process.
6. **Decommissioning:** Legacy or unused AI systems are safely retired, ensuring proper archiving of data and documentation for audit purposes.

This lifecycle approach ensures that risks are proactively managed at every stage, and that AI systems remain aligned with organizational values, regulatory requirements, and stakeholder expectations.

# Training and Awareness

All employees and stakeholders engaged in AI-related activities must undergo training on this policy, AI risks, and their roles in managing them. Training will be refreshed annually, and awareness campaigns will ensure continuous reinforcement.

# Compliance with Standards and Regulations

This policy aligns with international and industry best practices, including:

- NIST AI Risk Management Framework (RMF)

- ISO/IEC 42001: AI Management Systems

- ISO/IEC 3100: Risk Management

- Emerging global regulations such as the EU AI Act

The organization is committed to monitoring regulatory developments and updating this policy accordingly.

# **Review and Updates**

*This policy will be reviewed annually by the AI Governance Committee to ensure its relevance and effectiveness. Revisions will be made based on lessons learned, regulatory updates, and industry best practices*

**END**