SAMPLE AI Governance Policy

FOR INFORMATIONAL USE ONLY *

Bank Name:

Effective Date:
Approved By:

Purpose - This policy establishes governance for AI/ML systems to ensure safe banking practices, regulatory compliance, effective risk management and ethical AI use.

Scope - Applies to all AI/ML models, generative AI tools, automated decision systems, employees and third-party vendors.

Governance Structure - Board approves strategy and oversees risk. Management implements controls. AI governance committee reviews use cases. Model risk management validates models.

Risk Classification - AI systems classified as high, moderate or low risk based on customer and regulatory impact. Controls scale accordingly.

Model Lifecycle Governance - Includes approval, development/acquisition, validation, deployment, monitoring and decommissioning of AI systems.

Fair Lending and Bias - Requires bias testing, explainability and compliance with fair lending laws for customer-impacting models.

Data Governance - Data must be accurate, controlled and traceable with lineage and access restrictions.

Third-Party Risk - Vendors must undergo due diligence, contractual controls and ongoing monitoring.

Generative AI Controls - Restricts sensitive data input, requires human review and monitors hallucination risks.

Security and Privacy - Requires encryption, access controls and cybersecurity compliance.

Documentation - Maintain model documentation, validation reports, monitoring logs and change history.

Training - Employees must be trained on AI use, risks and data privacy.

Audit - Internal audit reviews governance periodically and policy reviewed annually.

Incident Management - AI incidents must be reported, investigated and remediated.

Enforcement - Non-compliance may result in disciplinary action or system suspension.

***This sample AI governance policy is being provided for INFORMATIONAL USE ONLY to assist members as they develop their own policy. The layout and sections used are for demonstration purposes only. Member banks should include appropriate personnel from compliance, legal, etc., as they develop their own policy.**

SAMPLE AI Governance Standards

FOR INFORMATIONAL USE ONLY *

Bank Name:

Effective Date:
Owner:

Applicability - These standards apply to all AI/ML systems and generative AI capabilities used by or on behalf of the bank, including internally developed solutions and third-party services.

Risk Classification

- Each AI system must be assigned a risk tier (high/moderate/low) prior to development, acquisition or material change.
- Risk tiering must consider customer impact, regulatory exposure, decision criticality, automation level, use of sensitive data and operational resilience.
- Risk tiering and the rationale must be documented and approved by the AI governance committee before work begins.

Lifecycle Controls and Change Management

- AI systems must follow an approved lifecycle: intake, design, build/acquire, validate, deploy, monitor and retire.
- No customer-impacting or high-risk AI system may be used in production without independent validation and documented approval to deploy.
- Material changes (data sources, features, model logic, thresholds, vendor version changes, intended use or deployment context) require re-assessment of risk tier and re-approval prior to implementation.

Fair Lending, Bias and Explainability

- Customer-impacting AI systems must undergo fairness and bias testing appropriate to the use case and risk tier, including pre-deployment and periodic post-deployment testing.
- Where decisions affect customers, the bank must be able to provide a meaningful explanation of key factors driving outcomes, consistent with applicable law and policy.
- Issues identified through testing must be remediated, documented and re-tested prior to deployment.

Data Governance

- Data used for training, testing or operating AI systems must be authorized, fit for purpose and subject to data quality controls.
- Data lineage, ownership, access controls and retention requirements must be documented for each system.
- Use of non-public, customer or confidential information in generative AI tools is prohibited unless explicitly approved and protected by appropriate technical controls.

Third-Party and Vendor Controls

- Third-party AI solutions must complete due diligence and risk assessment prior to procurement and periodically thereafter.
- Contracts must address data protection, confidentiality, incident notification, service availability, model/version change notifications and audit/monitoring rights consistent with bank requirements.
- Third-party AI systems must be monitored for performance and risk in the same manner as internally developed solutions, commensurate with risk tier.

Security, Privacy and Resilience

- AI systems must meet the bank's cybersecurity requirements, including least-privilege access, encryption in transit and at rest (where applicable), logging and vulnerability management.
- Privacy requirements must be addressed through data minimization, appropriate notices/consents (as applicable) and secure handling of personal information.
- High-risk AI systems must have defined operational controls for availability, backup/rollback and incident response.

Documentation, Monitoring and Auditability

- Each AI system must maintain sufficient documentation to support governance, validation, audit, and regulatory review, including purpose, design, data sources, limitations, approvals, and change history.
- Performance and stability monitoring must be implemented with thresholds and escalation paths aligned to risk tier.
- AI systems must be included in the bank's inventory and be available for audit and examination.

***This sample AI governance standards are being provided for INFORMATIONAL USE ONLY to assist members as they develop their own standards. The layout and sections used are for demonstration purposes only. Member banks should include appropriate personnel from compliance, legal, etc., as they develop their own standards.**

SAMPLE AI Governance Procedures

FOR INFORMATIONAL USE ONLY *

Bank Name:
Effective Date:
Owner:

AI Use Case Intake and Approval

- Business owner submits an AI use case intake form, including purpose, intended users, decisions supported and customer impact.
- Risk/Compliance completes an initial screening (regulatory, privacy, security, operational, reputational) and assigns a preliminary risk tier.
- Data owner confirms data availability, authorization and quality constraints.
- AI governance committee reviews the intake package, confirms the risk tier, and approves, requests changes, or rejects the use case.
- Approved use cases are logged in the AI inventory and proceed to development/acquisition.

Model Development or Acquisition

- Define objectives, scope, success metrics and limitations to include any customer impact and decision authority.
- Identify data sources, complete data mapping, lineage documentation and data quality checks.
- Develop the model or perform vendor evaluation to include testing of functionality, performance and control features.
- Document methodology, features, assumptions, training approach and known limitations.
- Prepare an implementation package for independent validation.

Independent Validation

- Model risk management (or other independent function) reviews the model package and confirms validation scope based on risk tier.
- Perform testing of conceptual soundness, data quality, performance, stability, and fairness/bias and explainability (where applicable).
- Document validation results, issues and required remediation actions.
- Business owner remediates findings and provides evidence of closure.
- Validator issues a deploy/no-deploy recommendation and retains validation artifacts.

Deployment and Production Change Control

- Obtain deployment approvals (business owner, AI governance committee as applicable, information security and model risk management) per risk tier.
- Implement access controls, logging, monitoring and rollback procedures.
- Deploy the model to production through approved change management processes.
- Validate post-deployment performance and confirm monitoring is active.
- Notify impacted stakeholders and update the AI inventory with production details.

Ongoing Monitoring and Periodic Review

- Monitor performance, stability and data drift metrics at a frequency aligned to risk tier.
- Conduct periodic reviews to confirm the model remains fit for purpose, including fairness/bias testing for customer-impacting use cases.
- Investigate threshold breaches, anomalies or customer complaints; document findings and corrective actions.
- Escalate material issues to the AI governance committee and risk management.
- Revalidate models and re-approve as required for material changes or when performance degrades.

Incident Management

- Report suspected AI incidents (e.g., incorrect decisions, bias concerns, data leakage, security events, unexpected behavior) through the bank's incident process.
- Assess impact to include customer impact, regulatory impact, financial exposure and operational risk.
- Contain and remediate, which may include disabling the model, rolling back changes, or implementing compensating controls.
- Validate fixes and document root cause, corrective actions and communications.
- Close the incident after approvals and update the AI inventory and monitoring controls as needed.

Decommissioning and Record Retention

- Business owner submits a retirement request and confirms replacement plan (if applicable).
- Obtain approvals to retire based on risk tier and impacted processes.
- Remove/Disable production access and update downstream dependencies.
- Archive required documentation, approvals, monitoring history and incident records in accordance with retention requirements.
- Update the AI inventory status to "retired" and confirm completion.

***These sample AI governance procedures are being provided for INFORMATIONAL USE ONLY to assist members as they develop their own procedures. The layout and sections used are for demonstration purposes only. Member banks should include appropriate personnel from compliance, legal, etc., as they develop their own procedures.**