AI POST-DEPLOYMENT MONITORING
POLICY QUICK START GUIDE

AI post-deployment monitoring ensures that AI systems maintain their accuracy, ethical standards, and compliance during real-world applications. This policy framework provides a strong structure to minimize risks while enhancing the value of AI.

Responsible Function	Purpose	Artifacts	Repository	Dependencies
1. AI Governance Framework Policy				
Description: Defines the structure, roles, processes, and responsibilities for AI governance, ensuring AI systems align with organization goals, ethics, and regulations.				
AI Governance Council / Compliance	Establish accountability for monitoring AI performance, ethics, and compliance.	Governance Charter Policy Documents	Governance Repository *(eg: SharePoint, GRC System)*	**Upstream:** Enterprise Risk Management Policy **Downstream:** Monitoring Policies
2. AI Model Performance Monitoring Policy				
Description: Outlines processes for real time monitoring of model accuracy, reliability, and data integrity to detect and address issues like drift or anomalies post-deployment.				
Data Science/ ML Operations	Ensure AI models maintain accuracy and reliability in real-world environments.	Performance Dashboards Drift Reports	ML Model Registry Monitoring Dashboard	**Upstream:** AI Governance Framework **Downstream:** Retraining Policy
3. Ethical Bias and Fairness Policy				
Description: Defines the processes and criteria for evaluating, identifying, and mitigating biases in AI systems to ensure fair, equitable, and ethical outcomes across all applications and stakeholders.				
AI Ethics Office/ Compliance	Promote fairness, ethical alignment, and trust in AI systems.	Bias Audit Reports Mitigation Plans	Compliance Document Repository	**Upstream:** AI Governance Framework **Downstream:** Performance Monitoring Policy
4. Regulatory Compliance Monitoring Policy				
Description: Defines methods to monitor AI systems for ongoing compliance with evolving laws and industry regulations.				
Compliance/ Legal	Maintain legal and regulatory adherence to avoid penalties and reputational risks.	Compliance Checklists Audit Logs	Compliance Database Legal Vault	**Upstream:** Regulatory Framework **Downstream:** Audit Policy

LEETECH VENTURES

www.LeeTechVentures.com
admin@LeeTechVentures.com

AI POST-DEPLOYMENT MONITORING

POLICY QUICK START GUIDE

Responsible Function	Purpose	Artifacts	Repository	Dependencies
5. AI Security and Resilience Policy				
Policy Description: Establishes security controls and practices to monitor AI systems for adversarial attacks or vulnerabilities.				
IT Security/ Infosec Team	Protect AI systems from cyber threats, adversarial inputs, and data manipulation.	Vulnerability Reports Security Logs	Cybersecurity Tools Data Vault	**Upstream:** Security Policies **Downstream:** Incident Response Policy
6. AI Retraining and Updates Policy				
Policy Description: Specifies guidelines for retraining AI models to address performance degradation, drift, or bias.				
Data Science/ ML Operations	Sustain model relevance, accuracy, and performance over time.	Retraining Logs Updated Models	ML Model Registry Monitoring Dashboard	**Upstream:** Performance Monitoring Policy **Downstream:** Bias and Fairness Policy
7. Human-in-the-Loop (HITL) Oversight Policy				
Policy Description: Defines scenarios where human validation and oversight are required for AI decisions post-deployment.				
Operations/ Domain Experts	Ensure AI decisions align with real-world expectations and business goals.	HITL Reports Decision Validation Logs	AI Governance Repository	**Upstream:** Governance Framework **Downstream:** Ethics Policy
8. AI Documentation and Auditability Policy				
Policy Description: Provides guidelines for maintaining audit trails, logs, and documentation for AI systems post-deployment.				
Compliance/ IT Operations	Improve transparency, accountability, and regulatory readiness for audits.	Audit Trails Version Control Logs	Audit Repository Document Management System	**Upstream:** Compliance Policy **Downstream:** Monitoring Policies

www.LeeTechVentures.com
admin@LeeTechVentures.com

AI POST-DEPLOYMENT MONITORING
POLICY QUICK START GUIDE

Responsible Function	Purpose	Artifacts	Repository	Dependencies
9. AI Stress Testing and Scenario Analysis Policy				
Policy Description: Requires testing AI systems under simulated extreme, adversarial, or edge-case conditions.				
IT Operations/ Data Science	Identify vulnerabilities, assess resilience, and improve AI robustness.	Stress Test Reports Scenario Analysis Logs	Resilience Testing Folder/ System	**Upstream:** Security Policy **Downstream:** Retraining Policy
10. Cross-Functional Collaboration Policy				
Policy Description: Facilitates collaboration among data, legal, ethics, and security teams for holistic AI oversight.				
AI Governance Council	Ensure all risks—ethical, operational, regulatory, and security—are addressed collaboratively.	Meeting Minutes Collaboration Reports	Governance Repository	**Upstream:** Governance Framework **Downstream:** All Other Policies

Key Notes:

1. Order Sequence: Policies are prioritized to align governance structures (Policy 1) before addressing operational, ethical, regulatory, and security risks.

2. Storage Locations: Policies, artifacts and deliverables are stored in **centralized repositories** such as GRC (Governance, Risk, and Compliance) systems, model registries, or secure vaults for traceability.

3. Interdependencies: Policies are designed to **build on one another**—governance frameworks underpin all monitoring activities, while security, retraining, and stress testing feed into AI operational resilience.

This quick start guide offers a foundational framework to implement Lean AI Governance and enable effective AI Post-Deployment Monitoring. It is not exhaustive and should be tailored to specific organizational needs and regulations.