AI USE CASE INTAKE & APPROVAL WORKFLOW

1. PURPOSE OF THIS WORKFLOW

This workflow ensures that all AI use cases introduced in the organisation go through:

- Proper evaluation
- Privacy and security review
- Ethical review
- Risk scoring
- Governance approval
- Documentation requirements
- Safe deployment

It prevents unapproved or unsafe AI from entering the enterprise environment.

2. SCOPE

This workflow applies to:

- Internal AI/ML models
- GenAI/LLM use cases
- Third-party AI tools / SaaS
- API-based AI services
- Vendor/supplier AI systems

3. END-TO-END WORKFLOW OVERVIEW

Below are the seven stages of Lifecycle:

1. Use Case Submission (Intake)
2. Preliminary Screening
3. Feasibility & Data Assessment
4. Detailed Risk Assessment (Fairness, Privacy, Security, Ethical)
5. Model Development & Validation
6. Governance Approval & Sign-off

7. Deployment & Continuous Monitoring

4. WORKFLOW DIAGRAM (TEXT FLOWCHART)

User / Business Team

↓

1. Use Case Intake Form Submitted

↓

AI PMO Reviews for Completeness

↓

2. Preliminary Risk Screening (AI PMO + AI Risk)

|

↳ Low Risk → Fast-Track Approval

|

↳ Medium/High Risk → Full Assessment Required

↓

3. Data Assessment (DPO + Data Steward)

↓

4. Detailed Risk Assessment

- **Fairness Assessment**
- **Privacy Assessment**

- **Security (MITRE ATLAS)**
- **Explainability Assessment**

↓

AI Risk Issues RAG Scoring Issued

↓

5. Model Development & Validation

- **Bias Testing**
- **Explainability Testing**
- **Adversarial & Safety Testing**

↓

6. Model Approval Stage

- **AI PMO**
- **AI Risk Manager**
- **Security Lead**
- **DPO**
- **Compliance**
- **AI Governance Board (High Risk Only)**

↓

7. Deployment (Controlled)

↓

Continuous Monitoring + AI Audit Log

5. STAGE DETAILS

5.1 Stage 1 — Use Case Intake

Responsible: Business Owner, Product Manager

Required Document: AI Use Case Intake Form

Includes:

- Problem statement
- Expected value
- Data sources
- Risk indicators
- AI fit justification
- Alternatives considered

5.2 Stage 2 — Preliminary Screening

Responsible: AI PMO + AI Risk Manager

Tasks:

Validate if the use case involves:

- Sensitive data
- Decisions affecting individuals
- Automation of judgments
- Regulated domains

Outcome:

- Low risk → Fast-track
- Medium risk → Full review
- High risk → AI Governance Board involvement

5.3 Stage 3 — Data Assessment

Responsible: Data Protection Officer (DPO), Data Steward

Deliverables:

- Data Card
- Privacy requirements
- Sensitive attributes evaluation
- Data quality & representativeness check

5.4 Stage 4 — Detailed Risk Assessment

Responsible: AI Risk Manager, Security, Fairness Lead

Includes:

5.4.1.1 Fairness Assessment:

- Group fairness
- Bias risk scoring
- Ethical impact

5.4.1.2 Privacy Assessment:

- PDPA/GDPR applicability
- Minimisation
- Lawful basis
- PII protection

5.4.1.3 Security Assessment:

- Input attacks
- Training data attacks
- Model attacks
- Output attacks

5.4.1.4 Explainability Assessment:

- SHAP/LIME feasibility
- User explanation needs
- Regulatory requirements

Deliverables: AI Risk Assessment Form

5.5 Stage 5 — Model Development & Validation

Responsible: Data Science Team + Independent Validator

Includes:

- Model training
- Validation report
- Red-teaming
- Adversarial testing
- Safety testing
- Bias & explainability tests

Deliverables:

- Updated Model Card
- Validation Report
- Security Test Report

5.6 Stage 6 — Governance Approval

Responsible:

- AI PMO
- AI Risk Manager
- Security Lead
- DPO
- Compliance
- AI Governance Board (for High-Risk)

Required Template: AI Model Approval Form

Approval routes:

- Low risk → AI PMO + Risk Manager
- Medium risk → Add Security + DPO review
- High risk → Governance Board review

5.7 Stage 7 — Deployment & Monitoring

Responsible: Model Owner, AI PMO, Security

Includes:

- Access control
- API/use restrictions
- Logging
- Monitoring thresholds
- Human-in-the-loop where required
- Required Template: AI Audit Log

Monitoring tracks:

- Drift

- Bias
- Security events
- Performance degradation
- Hallucination (for LLMs)

6. RISK ROUTING MATRIX

Risk Area	Low	Medium	High
Fairness	PMO	AI Risk	AI Board
Security	PMO	Security Lead	AI Board
Privacy	PMO	DPO	DPO + Board
Explainability	PMO	Risk + PMO	AI Board
Safety	PMO	Safety + PMO	AI Board
Legal Impact	PMO	Legal + Risk	Legal + Board

7. ROLES & RESPONSIBILITIES (RACI)

Deliverable	Business	PMO	AI Risk	DPO	Security	Board
Use Case Intake Form	R	A	C	C	I	I
Data Card	C	A	C	R	I	I
Model Card	R	A	C	C	C	I
Risk Assessment	C	A	R	C	C	I
ATLAS Threat Assessment	C	A	C	I	R	I
Model Approval	R	A	C	C	C	A
Monitoring	R	A	C	C	R	I

8. REQUIRED DOCUMENTS AT EACH STAGE

Stage	Required Documents
Intake	AI Use Case Intake Form
Screening	Preliminary Risk Checklist
Data Assessment	Data Card
Risk Assessment	Model Card, AI Risk Assessment Form, ATLAS Assessment
Validation	Validation Report
Approval	AI Model Approval Form
Monitoring	AI Audit Log