Responsible Artificial Intelligence Governance

[AI-Generated Image]

As Thai Union Group expands its use of digital technology, artificial intelligence (AI) is increasingly applied to improve productivity, decision support and operational efficiency across our business units. This growing reliance brings a corresponding exposure to risks relating to data privacy, information security, bias and misuse. Thai Union therefore governs the adoption, development and operation of AI through a defined framework of standards and guidelines, designed to ensure that AI is used responsibly, securely and under clear human accountability.

Responsible AI Governance Framework

The adoption, development and operation of AI is governed by the Digital Technology Standard DTS-10 Artificial Intelligence and by the AI/ML Model Development Guideline and the Agentic Application Development Guideline, which sit beneath the Group Information Security Policy and the Group Acceptable Use Policy.

Responsible AI Measures

Approved AI tools and controlled access

Only company-approved AI applications that have been vetted for security and compliance may be used with Thai Union data. Unauthorized AI tools, including public chatbots and image or code generators, are prohibited, and the use of unapproved AI applications is monitored and blocked through application security controls. Tool access and licensing require line manager approval through the Group service catalogue, and access to approved platforms is controlled through single sign-on, multi-factor authentication and role-based access control. Personal, confidential and proprietary data must not be entered into AI systems that have not been vetted by the company, and employees are required to mask or anonymize personal data before any use with external models.

Boundaries on AI use and human oversight

AI may not be used for harmful or unethical purposes. Manipulation, exploitation and unauthorized surveillance are prohibited, and high-risk applications such as those supporting hiring or medical decisions require additional approval and oversight. AI applications and agents are classified into three governance tiers according to data sensitivity, enterprise system integration and deployment scope; those addressing human resources, legal or financial topics, integrating with core enterprise systems, or published to external channels require the highest tier of review, including security assessment. Every AI-generated artefact has a named human owner accountable for it, autonomous agents operate under a Zero Trust model with least privilege and least agency, and high-risk or irreversible actions require explicit human confirmation.

Transparency and labelling of AI-generated content

Thai Union requires AI-generated material to be identifiable and attributable to a named person. Every AI-generated artefact, including code, configuration, prompts, flows, agents and reports, must have a named human owner who has reviewed and understood it and accepts responsibility for it, and accepting AI output without review is prohibited. Thai Union is developing mechanisms to label AI-generated content and AI-influenced outputs, so that users can identify when they are engaging with AI-generated material rather than human work product. This capability is planned for phased introduction across AI-enabled tools and channels.

Auditable logs are maintained for AI-assisted development, recording prompts, code changes, human approvals, design references, tools, frameworks and model versions, so that AI-generated content can be traced from requirement through to deployment. For generative AI, Thai Union applies grounded generation with citation and attribution so that the sources supporting an output are visible to the user, and AI agents may not be configured to impersonate other systems. For decisions supported or materially influenced by an AI system, human review and sign-off is required as a control point under Thai Union's AI governance framework. Thai Union is evaluating mechanisms to proactively inform affected individuals when a decision has been materially influenced by an AI system. Where AI output influences a business decision, the user remains accountable for validating that output before it is relied upon.

Monitoring, drift detection and retraining

Production models are monitored continuously for accuracy, latency and throughput. Data drift and model drift are detected, alerts are raised on performance degradation, and retraining is triggered through managed pipelines when drift exceeds defined thresholds. New models are tested against the production model before replacement, all versions are tracked with rollback capability maintained, and complete lineage from data to model to prediction is retained as an audit trail. Generative AI applications are additionally monitored for hallucination, unsafe outputs and retrieval failure, and a documented incident response plan covers AI-related failures including model drift, safety issues and data leakage.

Fairness, bias and model risk assessment

Training, validation and test datasets must reflect the target population, use cases and key subgroups, with assumptions, exclusions and limitations documented and reviewed before model approval. Model testing covers performance, robustness and bias, and each production model has a Model Card recording its purpose, limitations, subgroup evaluation results, safety testing and revision history. A documented Model Risk Assessment covering harm analysis, privacy, bias, intellectual property and security is approved before production. Duties are segregated across development, validation and deployment, with independent validation for high-impact models and periodic control testing thereafter. In addition, Thai Union's guidelines require back-testing through cross-validation on unseen data to mitigate model bias and support model validation activities. The implementation of these controls is currently at an early stage and is being progressively rolled out across AI and ML use cases. This includes the continued development and operationalization of fairness, bias, and model governance controls in line with Thai Union's evolving AI governance framework.

Appeals and recourse for AI-driven decisions

Thai Union recognizes that Artificial Intelligence (AI) systems may support recommendations, analysis, automation, and decision-making processes. However, AI does not replace human accountability. All high-impact AI-generated outputs and automated actions remain subject to appropriate human review and oversight prior to implementation.

Employees, and third parties may raise concerns regarding AI-generated outputs, recommendations, or automated actions through established operational and service management channels. Reported concerns are reviewed by the relevant business, technology, security, or governance functions to assess accuracy, appropriateness, compliance, and potential impacts. Corrective actions, including modification, suspension, or withdrawal of AI-enabled functionality, may be implemented where required.

Thai Union promotes a Human-in-the-Loop approach for high-risk or irreversible actions, ensuring that human judgment remains central to decision-making processes.

Training and awareness

Thai Union has initiated AI usage training as part of its AI governance program. The AI Standard and requirements for responsible AI usage have been communicated to key user groups through workshops and online sessions, and awareness communications have been shared with all employees. Training materials and communication records are maintained as evidence. The training program is being progressively expanded to a broader employee population.

Environmental and sustainability impact of AI

Thai Union is committed to the responsible and efficient use of Artificial Intelligence technologies. When designing and deploying AI-enabled solutions, the organization seeks to optimize resource utilization, reduce unnecessary processing activities, and maximize business value while minimizing operational overhead.

Thai Union promotes the use of approved enterprise AI platforms, cloud-native services, and controlled development environments to support efficient resource consumption and secure operations. AI solutions are designed with governance controls, monitoring mechanisms, and usage restrictions to prevent excessive or unnecessary utilization of computational resources. For AI applications, this includes a short-circuit breaker that limits AI processing beyond a defined threshold, helping to prevent excessive use of compute resources.

Where applicable, Thai Union leverages the sustainability initiatives, operational efficiencies, and environmental commitments of its strategic cloud service providers to support responsible digital transformation. AI-enabled solutions are also expected to contribute to productivity improvements, process automation, and reductions in manual effort across the organization.

Standards alignment and governance assurance

Thai Union's AI governance framework is based on AI governance best practice, including OECD AI Principles, NIST AI Risk Management Framework, the EU Artificial Intelligence Act, and AI provider guidelines.

Thai Union is committed to ensuring that AI systems operate in a transparent, accountable, and responsible manner. AI technologies are designed to support human decision-making rather than replace human judgment. All AI-generated artefacts, applications, workflows, configurations, and recommendations must have a designated human owner who is responsible for reviewing, understanding, and approving their use.

Thai Union applies Human-in-the-Loop controls for AI-enabled activities that may introduce elevated business, operational, compliance, privacy, or security risks. High-risk actions and automated processes are subject to appropriate review, approval, and monitoring before implementation.

Thai Union also maintains auditability and traceability throughout the AI lifecycle through documentation, logging, model lineage, change control, and governance oversight processes.

Reference policies and documents

- Group Information Security Policy;
- Group Acceptable Use Policy;
- DTS-10 Digital Technology Standards - Artificial Intelligence;
- AI/ML Model Development Guideline;
- Agentic Application Development Guideline;
- Cybersecurity Governance