Artificial Intelligence Policy

1. Introduction

Artificial Intelligence (AI), including machine learning, generative AI, autonomous agents, and large language models (LLMs), is increasingly embedded within SunExpress operations and third-party services.

AI presents significant opportunities to enhance operational efficiency, customer experience, and decision-making. However, it also introduces risks related to data protection, model reliability, bias, regulatory compliance, and operational integrity.

This policy establishes a risk-based, controlled, and responsible approach to the adoption and use of AI across SunExpress.

2. Purpose

This policy aims to:

- Enable the safe and responsible use of AI
- Establish a risk-based governance framework aligned with ISO 27001 risk management principles
- Ensure compliance with KVKK, GDPR, and emerging regulations (including EU AI Act principles)
- Protect customers, employees, and company data
- Promote accountability, transparency, and human oversight

3. Scope

This policy applies to all uses of Artificial Intelligence across SunExpress, including:

- Generative AI (e.g., copilots, chatbots)
- Autonomous AI agents
- Machine learning and predictive models
- AI capabilities embedded in third-party systems, SaaS platforms, and cloud services

It covers the use, development, procurement, and integration of AI solutions, whether internally developed or externally provided, including those accessed via enterprise platforms, APIs, or end-user tools.

This policy applies to all employees, contractors, and third parties acting on behalf of SunExpress.

SunExpress

4. AI Governance Framework

4.1 Risk-Based Classification

All AI use cases must be classified according to their potential impact, following a risk-based approach that is consistent with relevant regulations and legislation. This classification should consider the likelihood and severity of risks associated with each AI deployment, including impacts on data privacy, business operations, customer experience, and compliance requirements.

The risk assessment must be conducted before implementation and regularly reviewed as part of ongoing governance.

AI use cases should be categorised into risk levels—such as Low, Medium, High or Critical — based on criteria including, but not limited to:

- The nature and sensitivity of data processed (e.g., personal, confidential, or public information).
- The degree of autonomy and decision-making capability of the AI system.
- The potential for business, customer, or societal impact, including ethical concerns.
- Regulatory requirements, including data protection laws (such as the GDPR), sector-specific legislation, and international standards.
- The involvement of third-party systems, SaaS platforms, or cloud services.

This framework ensures SunExpress meets its legal and regulatory obligations while promoting responsible, transparent, and ethical AI adoption across the organisation.

Risk Level	Description	Examples	Governance Requirement
Low	No classified data (internal use, confidential or strictly confidential) or personal data, and/or no business or customer impact	Drafting, research, productivity tools	Pre-approved usage
Medium	Internal use with limited impact and human validation	Internal copilots, analytics	Business approval + registration
High	Use of personal or sensitive data, or operational/financial impact	Customer-facing AI, decision support	Mandatory InfoSec & DPO review required. Risk Committee on escalation
Critical	Safety, regulatory, or critical operational impact	Flight operations, safety-critical systems	Risk Committee & Executive Oversight

4.2 Governance Model

The federated, risk-based model adopted ensures decision-making and oversight are distributed across relevant business and technical functions, with responsibilities assigned according to the level of risk associated with each AI use case.

By combining decentralised accountability with robust risk management, the framework supports both innovation and compliance, ensuring that AI systems are deployed safely and responsibly throughout the organisation.

Stakeholder	Role
Business Owner	• Accountable for AI use, outcomes, and risk acceptance • Responsible for ensuring classification • Responsible for compliance with this policy
Technical Custodian/Owner (IT / Relevant Technology Function)	• Responsible for implementation, integration, and operational management • Ensures alignment with enterprise architecture
Information & Cyber Security	• Defines security requirements and provides independent oversight • Reviews and approves "Critical" or "High"-risk use cases • Monitors compliance and risk exposure
Data Protection Officer (DPO)	• Advisory for KVKK and GDPR compliance • Reviews AI use involving personal data
Risk Committee	• Provide oversight for "Critical" and "High" risk escalated use cases

5. AI Use Requirements

5.1 Acceptable Use

Acceptable use of AI requires users to act responsibly by following all relevant organisational policies and adhering to applicable laws and regulations. Individuals must be mindful of the potential risks associated with AI, including the possibility of generating false or misleading information and inadvertent disclosure of sensitive data.

AI must be used:

- In alignment with SunExpress policies and legal obligations
- With awareness of limitations such as inaccuracies and hallucinations
- In a manner that does not introduce unacceptable risk

5.2 Human Oversight

Human oversight is essential whenever AI is deployed, particularly in scenarios where decisions have significant impacts. This ensures that AI-generated recommendations are carefully reviewed and assessed by qualified professionals before any actions are taken.

AI systems must not be solely relied upon for:

- Decisions affecting customers or employees
- Financial or operational decisions
- Safety-critical outcomes

5.3 Safeguards for Decision-Making

Whenever artificial intelligence is utilised to assist with or guide decisions that have an impact on individuals, it is crucial to ensure that such use is accompanied by robust safeguards. This approach helps to prevent the risk of unjustified or unchallengeable automated decisions and ensures that the decision-making process remains transparent and accountable.

Where AI is used to support or inform decisions affecting individuals:

- Appropriate safeguards must be implemented
- Outputs must be validated prior to action
- Decisions must remain explainable where required
- Individuals must not be subject to unjustified or unchallengeable automated decisions

5.4 Fairness and Responsible Use

All AI applications must be designed and managed to uphold ethical principles, promote transparency, and maintain accountability throughout their lifecycle.

AI must not be used in a manner that results in:

- Unlawful discrimination
- Unfair bias
- Unjustified adverse impact on individuals

6. AI Risk Management

AI risks must be assessed and managed in alignment with ISO 27001 risk management processes and integrated into the enterprise risk management system (STREAM).

6.1 Risk Categories

AI risk assessments must consider:

- Data protection and privacy risks
- Model accuracy and hallucination risk
- Bias and fairness concerns
- Regulatory and legal exposure
- Operational dependency and over-reliance
- Third-party and supply chain risks

7. AI Use Case Registration (AI Inventory)

All "Medium", "High" and "Critical" risk AI use cases must be recorded in a register of AI use cases.

7.1 Registration Triggers

Recording in the AI inventory or register is required when:

- Procuring AI-enabled solutions
- Implementing new AI use cases
- Integrating AI via APIs or third-party platforms
- Using generative AI with business or personal data

7.2 Minimum Information Requirements

Each registered or recorded use case must include:

- Business Owner.
- Technical Custodian/Owner.
- Use case description.
- Data classification (including personal data).
- Risk classification.
- Technology/provider.
- Decision impact level.

8. Data Protection and Security

8.1 Use of Public AI Services

Classified business data and personal data must not be submitted to public or non-approved AI tools unless:

- Explicitly approved by the data owner.
- Compliant with KVKK and GDPR.
- Appropriate safeguards are in place.

8.2 Approved AI Services

SunExpress will maintain a list of approved AI tools and platforms. Use of non-approved AI tools requires assessment and approval.

8.3 Data Protection Controls

Where applicable:

- Data must be classified prior to AI use.
- Data Loss Prevention (DLP) controls must be enforced.
- Monitoring and logging should be implemented.

9. Third-Party and Supplier AI

Supplier-provided AI features must be evaluated using established procurement procedures involving supplier assurance.

Suppliers are required to inform SunExpress of any incorporation of AI within their offerings.

All contracts must stipulate provisions relating to:

- Safeguarding data.
- Implementation of security measures.

- Clear disclosure of AI usage.

10. Monitoring, Assurance, and Review

All AI use cases should undergo regular reviews to ensure ongoing suitability and compliance.

Use cases identified as critical or high-risk must be subject to continuous monitoring with particular attention to the following factors:

- Their operational performance and reliability.
- Potential risks and exposure to threats.
- Adherence to regulatory and organisational compliance requirements.

Any incidents involving AI must be promptly reported and managed in accordance with established incident management protocols.

11. Exceptions

All deviations or exceptions from SunExpress policies or standards must receive prior approval from Information Security. This must be done through a documented procedure that ensures every exception and instance of non-conformance is tracked and reported accordingly. The handling of exceptions must:

- Be thoroughly documented
- Receive approval from Information & Cyber Security
- Include clear documentation of risk acceptance

12. Non-Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

13. Policy Maintenance

The Information & Cyber Security team holds responsibility for the following:

- Overseeing the ongoing maintenance and revision of this policy
- Ensuring the policy remains consistent with advancements in technology and regulatory changes
- The policy will be subject to review each year, or whenever there are substantial changes to AI implementation or relevant regulations.

Signed

Marcus Schnabel
CEO

Tuncay Eminoglu
Deputy CEO