

PULSAR*GROUP

Artificial Intelligence (AI) Policy



Artificial Intelligence (AI) Policy

Content

[Content](#)

[Introduction](#)

[Policy Objectives](#)

[AI Infrastructure Providers](#)

[AI Model Rules](#)

[Expected AI Use Cases](#)

[AI Governance & Risk Management Practices](#)

[Risk Level Examples](#)

[AI System Lifecycle Management](#)

[AI Model Trials](#)

[AI Model Internal Tools](#)

[AI Models in Production](#)

[AI Monitoring](#)

[AI Failure & Incident Management](#)

[AI Training & Compliance](#)

[AI Risk Accountability Structure](#)

[Document Version Control](#)

Introduction

Pulsar Group is committed to the responsible and ethical use of artificial intelligence (AI). This policy establishes our approach to AI governance, ensuring compliance with legal and regulatory requirements, mitigating AI-related risks, and fostering trustworthy AI systems.

Policy Objectives

This policy aligns with ISO 42001 and the EU AI Act, ensuring responsible AI development and deployment through:

- **Risk-Based AI Management:** Categorise AI by risk level, with proportional oversight.
- **Human Oversight & Accountability:** Clear responsibilities for AI governance and risk mitigation.
- **Bias & Fairness:** Ongoing bias assessment and fairness evaluations.
- **Security & Data Protection:** Compliance with ISO 27001 and GDPR.
- **Transparency & Documentation:** Comprehensive AI system documentation, including lifecycle management and impact assessments.
- **Continuous Monitoring & Improvement:** Regular review and refinement of AI models.

AI Infrastructure Providers

When integrating AI capabilities into products, Pulsar Group prefers to use AI Infrastructure Providers rather than direct integration with an AI Model. These providers offer centrally managed platforms that host a variety of AI models, allowing the delivery of advanced functionality without the overhead of maintaining individual models internally.

This approach ensures seamless scalability, consistent performance, and automatic updates, with all model maintenance handled by providers. Consolidating Pulsar Group's use of AI models under supplier agreements, we reduce operational complexity, simplify compliance, and reinforce our commitment to strong data protection standards.

AI Model Rules

Any AI model integrated via an AI Infrastructure Provider shall not:

- 1) Use client data for secondary purposes e.g. training models
- 2) Retain client data for longer than 24 hours
- 3) Make automated decisions that could impact the rights & freedoms of individuals
- 4) Include High-Risk use cases of AI, e.g. creating individual profiles from facial recognition

Expected AI Use Cases

Expected use cases for utilising AI within Pulsar Group products include: Natural Language Processing, translation, entity extraction, and image tagging.

Any sentiment analysis within the products shall be based on an aggregated view of multiple posts & conversations. Sentiment analysis shall not track an individual's emotions over time.

AI Governance & Risk Management Practices

- All use cases shall be included in regular Data Processing Impact Assessments (DPIA) to ensure there are no high risks to an individual's rights and freedoms.
- AI governance, risk and compliance activity shall be integrated with the Pulsar Group Information Security Management System (ISMS), which is ISO 27001 certified.
- All AI Infrastructure Providers shall be documented within the ISMS and regularly reviewed to reflect changes in deployed AI and to ensure compliance with this policy.
- Collaboration with legal, data protection, and product teams is required to assess risk levels. AI risks will be categorised into low, medium, and high risk levels, with oversight proportional to the risk level.

Risk Level Examples

- **Low-Risk AI:** AI-powered spell checkers, chatbots and data analytics tools for non-sensitive data.

- **Medium-Risk AI:** Generative AI models trained on company proprietary data.
- **High-Risk AI:** AI-based processing of structured personal or sensitive data.
- **Critical-Risk AI:** AI involved in decision-making that impacts individuals; AI with a potential high societal impact.

AI System Lifecycle Management

AI system development must follow ISO 42001 best practices, including risk assessment, monitoring, and improvement. Each stage integrates relevant governance measures:

- **Concept & Design:** Risk analysis and compliance checks.
- **Development & Testing:** Bias testing, security assessments.
- **Deployment & Monitoring:** Continuous oversight, risk mitigation.
- **Retirement & Decommissioning:** Secure data removal and documentation.

AI Model Trials

- No CTO or legal approval is required to promote innovation.
- Must not include structured personal data confidential (e.g. client names/data).
- Trials should be isolated from production environments.

AI Model Internal Tools

- Includes general AI tools such as ChatGPT, Gemini in Google Workspace, or AI-driven analytics.
- Must not process sensitive or confidential information.
- Requires CTO and legal approval before adoption.

AI Models in Production

- Includes any AI Infrastructure Provider or AI Model directly integrated into company products.
- Compliance with this Policy must be demonstrated before deployment and documented in the ISMS.
- Requires CTO approval and legal review, including security and privacy assessments.

AI Monitoring

- AI systems must undergo periodic reviews addressing performance, trustworthiness, bias, and security concerns.
- AI system purposes should be continuously evaluated to align with societal values and organisational principles.
- AI reliability measures will be documented and assessed periodically.
- AI risk tolerance levels must be defined, with oversight allocated accordingly.
- Internal audits and external reviews will be conducted for any high-risk AI systems.
- Incident response plans will be developed and tested for AI-related failures.

AI Failure & Incident Management

- Pulsar Group shall produce clear procedures for identifying and evaluating AI failures.
- The Incident Response Plan must include AI system failures.
- AI-related incidents must be logged, investigated, and reported to AI Governance Team and/or the Security Team.
- If a failure or unexpected use case is identified, additional investigation, documentation, and approval shall be required, including:
 - External AI domain experts and special interest groups should be engaged to assess potential negative impacts.
 - AI documentation should include any assumptions, constructs, proxy targets and configuration results.
 - Feedback from internal and external stakeholders must be collected and analysed.

AI Training & Compliance

- All personnel must be informed of the legal and regulatory requirements specific to Pulsar Group's industry, sector, and AI application context.
- Compliance with the EU AI Act, UK AI regulations, GDPR, ISO 42001 (AI Management System – AIMS), and other relevant laws is mandatory.
- Training materials must outline best practices, potential risks, ethical considerations, compliance, and system limitations.

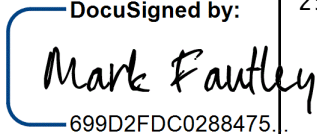
AI Risk Accountability Structure

- **CTO:** Owns all AI technologies and approves new AI models and vendors.
- **Legal & Compliance Team:** Conducts legal review, security, and privacy assessments before AI adoption.
- **AI Governance Team:** Oversees AI compliance and risk management.
- **Security Team:** Oversees ISMS integration and incident management.
- **Developers & Product Managers:** Ensure responsible AI design and implementation, monitoring and incident management.
- **Data Protection Officer (DPO):** Ensures compliance with GDPR and data protection laws.

Document Version Control

This policy shall be reviewed if required changes are identified to address an identified weakness, or a change in business activities which may affect the validity of this document.

The current version of this policy, together with its previous versions, shall be recorded below:

Version	Author	Approver	Signature	Date
1.0	Adam Palmer Head of Information Security & Privacy	Mark Fautley CFO	 DocuSigned by: <i>Mark Fautley</i> 699D2FDC0288475..	25/4/2025