ARTIFICIAL INTELLIGENCE POLICY

1 PURPOSE

This Artificial Intelligence Policy ("Policy") aims to ensure the ethical, secure, lawful, and transparent use of AI within AMG in order to safeguard corporate data and maintain customer trust and regulatory compliance. It is relevant for all AMG employees globally as part of AMG Critical Materials N.V. and its group companies ("AMG"). Additionally, we expect our partners along AMG's value chain to support and respect AMG's principles in this matter.

In addition to the Policy, this document includes an example setup for AI-Governance and key cornerstones for AI general use guidelines.

2 SCOPE AND APPLICABILITY

This Policy is applicable to AMG and all its group companies. Every AMG employee, contractor and third-party service provider is expected to exhibit conduct that reflects this Policy during work, when representing AMG, on or off the work site, as well as in interactions with AMG external business partners and stakeholders. Service providers must comply with this Policy through contractual agreements (e.g. data processing agreements). This Policy is also considered a guideline to all our partners along the value chain to meet AMG's expectations regarding artificial intelligence.

The Policy applies to all AI-supported tools, whether internally developed, cloud-based, or integrated into third-party solutions regardless of hosting or deployment model. This Policy is a baseline AI Policy for all business units, but it can be extended, refined, or replaced by a business unit specific AI policy, provided that a local policy must conform legally to the local jurisdiction and aligned with GISO and/or CFO of AMG-NV Critical Materials.

AMG is firmly committed to full compliance with all national rules and regulations applicable to AMG's group companies. Where the requirements of such national legislation are stricter than this Policy or set additional requirements, the relevant stricter or additional rules of such national legislation shall prevail.

3 ROLES AND RESPONSIBILITIES

- The Management Board has adopted this Policy for all employees of the AMG Group and is accountable for the implementation of this Policy. It shall review this Policy and the implementation of this Policy regularly in consultation with the Supervisory Board.
- IT/Information security departments of the AMG group companies are responsible for Policy implementation and compliance and group-wide monitoring and reporting.
- All AMG employees are responsible to adhere to the principles as set forth in this Policy.

4 ANNEXES

Within Annex A, B and C we provide templates for the implementation of AI tooling.

- ✓ Annex A is a template addressing asset management;
- ✓ Annex B is a risk assessment template for consuming AI services;
- ✓ Within Annex C we provide a simple template for AI related incident reporting, recommended is using the existing IT/Information Security Incident Management process and extend it to AI;

Annex D shows a mapping from AI Governance to ISO27001:2002 controls. If an organization is aiming for/has already an ISO27001 certification, it is beneficial to integrate AI Governance directly into the ISO control framework to avoid duplicate work; and Annex E shows an example implementation of AI Governance and Annex F offers guidelines for setting AI Strategy.

5 DEFINITIONS

- **Artificial Intelligence (AI):** technologies imitating human cognitive abilities (e.g. reasoning, learning, decision-making).
- **AI Tool:** software trained using AI methods to generate predictions, recommendations, content, or decisions.
- **AI System:** machine-based system operating with varying autonomy, potentially adaptive post-deployment, producing outputs influencing physical or virtual environments.
- **Large Language Model:** AI model trained on text data to understand and generate human language.
- **Generative AI:** AI capable of creating new content (text, images, audio, code).
- **FOSS: f**ree and Open-Source Software
- **ISMS:** Information Security Management System**.**
- **Business Unit Level AI Governance Team:** Each Business Unit is expected to establish a local AI Governance Team responsible for evaluating, approving, and monitoring AI tool use within that Business Unit. Recommended composition includes representation from Business Unit IT and Information Security, a Legal/Compliance representative, and the business/process owner sponsoring the relevant AI use case.

6 AMG'S COMMITMENT TO ARTIFICIAL INTELLIGENCE

6.1 Guiding Principles

- **Human Oversight & Accountability:** AI supports decisions; ultimate responsibility lies with humans.
- **Transparency:** AI functionality and outputs must be explainable and labeled where applicable.
- **Fairness:** No discrimination on the basis of protected characteristics; bias must be identified and mitigated.
- **Data Privacy & Security:** All AI usage must comply with GDPR and internal information security standards.

- **Safety & Robustness:** AI must be resilient against errors, attacks, and misuse.
- **Sustainability:** AI should be deployed in an energy-efficient manner where feasible.
- **Governance:** The Business Unit Level AI Governance Team must include and actively involve IT and Information Security as mandatory members into AI related projects from project inception through decommissioning.

6.2 Data Protection & Confidentiality Rules

- **No confidential company data** should be used in public AI tools unless a contractual data protection agreement exists, risk owner and governance team have signed off.
- **No personal data** in public AI unless lawful basis, DPIA (Data Protection Impact Assessment), and risk owner approval are in place.
- **Customer data** must be anonymized/pseudonymized before AI use unless written consent is obtained.
- All AI-generated content must be **reviewed before use** and **labeled** when shared externally.

6.3 Intellectual Property & Copyright

- Assume AI-generated content **may not be copyright-protected**.
- Validate that AI outputs do not infringe third-party copyrights, End User Agreements or violate open-source licenses (FOSS scanning required).
- Training data legality must be verified when developing AI models.
- Do not use AI-generated code without any cross-validation in customer projects.

6.4 AI Tool Approval & Risk Management

- All AI tools must be **evaluated and approved** by the Business Unit Level AI Governance Team before use.
- **Risk evaluation** must document:
  - Tool name, provider, version
  - Intended use case
  - Data involved
  - Risk classification under EU AI Act (prohibited, high-risk, low risk)
  - Security controls
- **Security team/Head of IT** must be involved for new AI tool onboarding.
- **Each Business Units Approved AI tools** must be listed in a **local central registry** (e.g., SharePoint/FreshService).

6.5 AI Integration into own products

- **Legal conformance:** It must be ensured that own developments adhere to local product liability acts, safety and security standards and conform to the licenses/End User License Agreement of the used tools are published with.
- **Certifications:** Industry specific certification of products with integrated AI functionality is highly recommended.

- **Sustainable Product Development:** Automatically generated program code must be reviewed and if necessary improved in a way that makes maintenance of the code possible. Avoid *throw away* code.

6.6 EU AI Act Compliance

- **Prohibited AI**: Not allowed under any circumstance (see Art. 5 AI Act).
- **High-risk AI**: Requires documented risk management, human oversight, transparency, data quality controls, and CE conformity assessment.
- **Low-risk AI**: Must comply with transparency obligations (e.g., user disclosure, "AI-generated" label).

6.7 Security & Incident Handling

- AI usage must follow existing **ISMS processes** for vulnerability management and incident response.
- AI-related incidents (security breaches, data leaks, policy violations) must be reported to the GISO and CFO immediately.

6.8 Documentation & Review

- All AI usage decisions, risk assessments, and tool approvals must be documented.

7 MONITORING AND GRIEVANCES

We expect all employees to comply with this Policy. If any employee is found to have exhibited inappropriate conduct or behavior in breach of this Policy, AMG reserves the right to take action, in particular, but not conclusively to take disciplinary actions including dismissal.

Employees who believe they have been subjected to any kind of behavior or acts that conflict with this Policy should seek assistance from a supervisor, upper management, or otherwise in accordance with our Speak Up & Reporting Policy. Confidentiality, non-retaliation, and remedy will be maintained in accordance.

Comments from AMG's own workforce of workers employed in AMG's value chain regarding this Policy are highly welcomed and can be addressed through AMGs websites and contact information.

8 TRAINING

AMG periodically provides training to relevant AMG employees and regularly reviews this Policy to ensure compliance with all applicable laws and regulations. Training will take place in the following manner:

- Any tool access requires mandatory AI awareness training before tool access.
- All new employees take the mandatory and locally provided online training course which reflects the organizations AI tooling and strategy.

- All new employees are being inducted by the local compliance officer once they start employment and are being advised about the application, amongst other policies, of the AMG Code of Business Conduct, Speak Up & Reporting Policy and this Policy.
- All AMG employees are trained regularly, at least every three years, either online or by way of onsite meetings to address new risks and regulatory updates. Designated groups of AMG Employees may receive regular specific training on the matters referred to in this Policy.

9 OTHER RELATED DOCUMENTS

Other AMG policies and AMG documents that are related to the topic of this Policy are, amongst others:

- AMG Speak Up & Reporting Policy
- AMG Code of Business Conduct
- AMG Supplier Code of Conduct

ANNEXES attached

Annex A – Approved AI Tools Register (Template)

Example for asset management of AI based tools:

Tool Name	Provider	Version	Deployment Type (Internal / Public / SaaS / On-Prem)	Primary Use Case	Data Types Processed	Risk Category (EU AI Act)	Approval Date	Risk Owner	Review Date
Example: Microsoft Copilot	Microsoft	2025.06	SaaS	Document drafting	Internal business docs (no personal data)	Low-risk AI (Transparency obligation)	2025-07-15	IT Director	2026-07-15
Example: Internal Chatbot X	In-house	v2.1	Internal	HR Q&A	Anonymized HR FAQs	Low-risk AI	2025-05-01	HR Manager	2026-05-01
Example: Predictive Maintenance AI	Siemens	v4.0	On-Prem	Maintenance scheduling	Sensor telemetry	High-risk AI (Industrial safety)	2025-08-10	Plant Manager	2026-08-10

Maintenance rule:

- Update whenever a tool is approved, updated, deprecated, or decommissioned.
- Include all AI tools regardless of whether they are standalone or embedded in other software.

Annex B – AI Risk Assessment Form (Aligned to the EU AI Act)

Section 1 – General Information

- Tool Name:
- Provider / Vendor:
- Version:
- Deployment Model:
- Owner / Department:
- Request Date:

Section 2 – Use Case Description

- Intended Use Case:
- Expected Business Benefit:
- Data Inputs: (e.g., anonymized text, images, telemetry, personal data)
- Expected Outputs: (e.g., recommendations, generated content, decisions)

Section 3 – Risk Classification (EU AI Act)

☐ **Prohibited AI** – If yes, STOP.
☐ **High-risk AI** – Document risk management plan, human oversight procedures, CE conformity assessment.

☐ **Low-risk AI** – Apply transparency requirements.
☐ **Other AI** – No specific AI Act obligations, but still subject to internal controls.

Section 4 – Risk & Security Controls

- Data Privacy Impact Assessment (DPIA) required? ☐ Yes ☐ No
- FOSS/Open-source license check performed? ☐ Yes ☐ No
- Access Controls defined? ☐ Yes ☐ No
- Output Review Process in place? ☐ Yes ☐ No
- Adversarial Attack Mitigation tested? ☐ Yes ☐ No

Section 5 – Approval Workflow

- Risk Owner Decision: ☐ Approved ☐ Approved with Conditions ☐ Rejected
- Approval Date:
- Reviewer Name / Title:

Annex C – AI Incident Report Template

Incident Summary

- Tool Involved:
- Date/Time Detected:
- Description of Incident:

Impact Assessment

- Data compromised:
- Business process impact:
- Regulatory implications (GDPR / AI Act):

Root Cause Analysis

- Technical cause:
- Process / human factors:

Corrective Actions

- Immediate containment:
- Long-term remediation:

Reporter Information

- Name:
- Department:
- Date of report:

Annex D - ISO 27001:2022 Annex A Control Mapping for AI Governance

ISO 27001 Control	Control Title	Policy / Annex Reference	Evidence / Implementation
A.5.1	Policies for information security	Unified AI Policy – Sections 1–12	Approved AI policy document signed off by management.
A.5.7	Threat intelligence	Annex B – AI Risk Assessment (Section 4 – Adversarial Attack Mitigation)	Risk analysis records for AI tools showing awareness of AI-specific threat vectors (data poisoning, model stealing).
A.5.23	Information security for use of cloud services	Unified AI Policy – Sections 5 & 7	Risk assessments for SaaS AI tools (e.g., Microsoft Copilot) with documented contractual safeguards.
A.5.32	Intellectual property rights	Unified AI Policy – Section 6 & Annex B	FOSS scanner reports, copyright review notes, AI-generated content labeling procedures.
A.5.34	Privacy and protection of personally identifiable information	Unified AI Policy – Section 5	DPIA records, consent logs, pseudonymization documentation for AI data inputs.
A.5.36	Compliance with policies, rules and standards	Unified AI Policy – Section 12 & Annex A	Policy compliance monitoring logs, approved AI tools register.
A.6.1	Information security roles and responsibilities	Unified AI Policy – Section 7 & 8	AI Governance Team charter, role descriptions for risk owners.
A.6.4	Disciplinary process	Unified AI Policy – Section 12	HR disciplinary policy referencing AI misuse consequences.
A.8.12	Data leakage prevention	Unified AI Policy – Section 5	Technical DLP controls and training records to prevent input of confidential data into public AI tools.
A.8.16	Monitoring activities	Annex A – AI Tools Register & Annex B – Review Dates	Scheduled AI tool reviews, audit logs of AI tool usage.

ISO 27001 Control	Control Title	Policy / Annex Reference	Evidence / Implementation
A.8.28	Secure development life cycle	Unified AI Policy – Section 6 & 8	AI in development documented in risk assessments, code scanning results, training data legality checks.
A.8.30	Outsourced development	Unified AI Policy – Section 2	Supplier contracts with AI compliance clauses.
A.8.33	Test data	Unified AI Policy – Section 5	Documentation showing anonymized or synthetic data used in AI testing.
A.8.35	Secure system architecture and engineering principles	Annex B – Risk Classification & Controls	Architecture reviews including AI security design principles.
A.8.37	Outsourced services	Unified AI Policy – Section 2 & Annex A	Third-party AI tool approvals with contractual obligations.

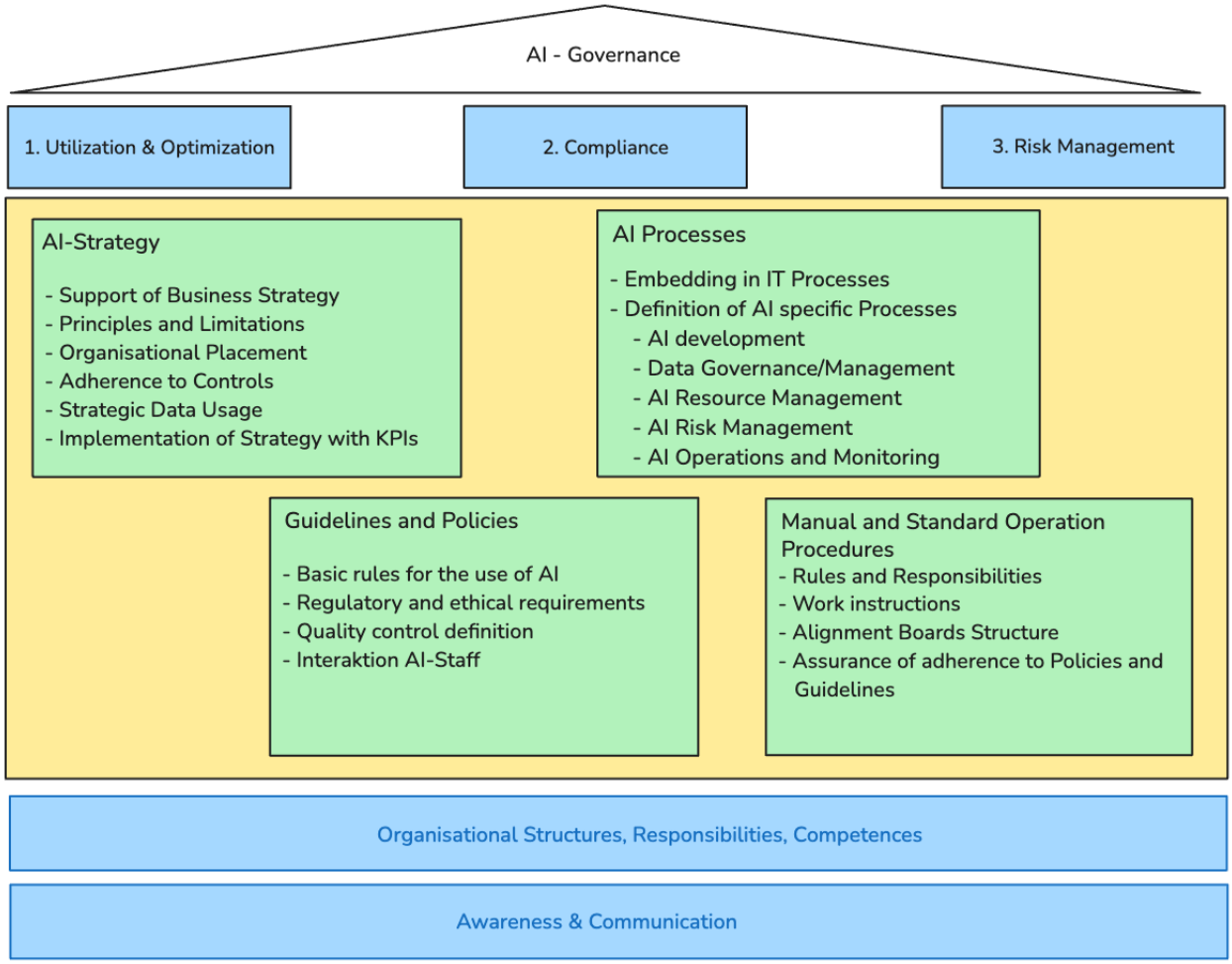
How to present to auditors

1. **Policy document** — Approved and version-controlled in your ISMS repository.
2. **Annex A** — AI Tools Register with “last review date” column to show ongoing governance.
3. **Annex B** — Sample completed risk assessment for a live AI tool.
4. **Annex C** — Example AI incident report (even if only a test exercise).
5. **Cross-reference table** (above) — Shows direct linkage to ISO 27001:2022 Annex A controls.

Note: This mapping means you can demonstrate **direct policy-to-control coverage** without extra documentation work.

It also shows the auditor that your AI governance is **integrated into the ISMS**, not a separate silo.

Annex E - Template Design and Setup of AI Governance



Annex F - AI Strategy

Strategy - Who is the owner of the AI topic and sets the strategy - Which limitations and ethical boundaries are set - Where is the AI topic embedded into the organization:

- How are internal and external regulations managed and controlled
- How can internal data and information be used for AI
- What are the KPIs to evaluate internal AI projects

Annex AI Guidelines and Rules for the use of AI

AI-Guiding Principles

- **Precision**: Exact, reproducible results by the AI model
- **Reliability**: AI models must not degrade over time
- **Robustness and Generalization Capabilities**: AI models must proof robustness
- **Resilience**: AI models must be resilient to external to the model influences
- **Fairness**: Be aware of Bias of any kind, test the AI systems to ensure no unwanted bias is present
- **Legal Conformance**: Operation of the AI is complying to local laws and regulations - **Explainability**: Transparency how the AI model generates its decisions