RESPONSIBLE AI USE POLICY

1. OBJECTIVE, SCOPE, AND REFERENCES

1.1. OBJECTIVE

This policy establishes the principles, guidelines, and controls for the ethical, legal, secure, transparent, and responsible use of Artificial Intelligence (AI) tools and technologies across all PROGUIDE projects and services, in compliance with the requirements of the ISO/IEC 42001 standard (Artificial Intelligence Management System) and applicable legal regulations.

1.2. SCOPE

This policy applies to all PROGUIDE employees, contractors, and third parties who use, develop, or deliver any Artificial Intelligence tool, system, or model as part of their work activities. This encompasses both the use of third-party SaaS applications and the design, training, and implementation of custom models.

1.3. REFERENCE DOCUMENTS

ISO/IEC 42001:2023 – Artificial Intelligence Management System (AIMS)
ISO/IEC 22989:2022 – Artificial Intelligence Concepts and Terminology [Reference Glossary]
ISO/IEC 27001:2022 – Information Security
ISO 9001:2015 – Quality Management
Personal Data Protection Law 25.326 (Argentina) and Regulatory Decree 1558/2001
Intellectual Property Law 11.723 (Argentina)

[ISO/IEC 42001 Requirement: 2]

2. GUIDING PRINCIPLES OF THE SGIA

All personnel within the organization, regardless of their role, must guide their actions according to the following fundamental principles of the AI Management System:

2.1. RESPONSIBILITY AND HUMAN OVERSIGHT

The final decision and responsibility regarding AI-generated results are subject to human oversight.
AI is a support tool, not a substitute for professional judgment.
For high-risk systems, effective human oversight mechanisms and the capacity for real-time

intervention must be ensured.

2.2. EQUITY AND NON-DISCRIMINATION

- The use of AI that may perpetuate or amplify biases (an inclination or partial preference that is not entirely objective), resulting in discrimination (unfairness or unjust treatment) based on race, gender, age, religion, sexual orientation, or any other protected characteristic, is prohibited.
- Training or interaction data must be rigorously evaluated.

2.3. TRANSPARENCY AND EXPLAINABILITY

- It must be clearly documented when and how AI is used in a project.
- Any AI system in production must include mechanisms that allow for a clear explanation of how a specific recommendation or result was reached.

2.4. SECURITY, ROBUSTNESS, AND RELIABILITY:

- AI solutions must be tested to ensure their robustness against attacks, unforeseen failures, or performance degradation, implementing continuous monitoring to detect deviations.

[ISO/IEC 22989: 5.15.2 / 5.15.3]

3. SENIOR MANAGEMENT'S INSTITUTIONAL COMMITMENTS

3.1. FRAMEWORK FOR ESTABLISHING AI OBJECTIVES

PROGUIDE's senior management defines the objectives for the AI Management System, comprehensively classifying them according to the business's three operational dimensions (Use, Development, and Delivery). These objectives serve as the basis for designing and monitoring specific process indicators.
To ensure the effectiveness and continuous improvement of the AI Management System, the metrics, calculation formulas, targets, and responsible parties associated with each of these objectives are formally consolidated in the AI Objectives Dashboard.

3.2. COMMITMENT TO CONTINUOUS IMPROVEMENT

PROGUIDE's Senior Management assumes the ethical and institutional commitment to maintain, audit, and continuously improve the Artificial Intelligence Management System (AIMS), ensuring that controls evolve in step with technological advancements in the market.

3.3. RESOURCE ALLOCATION

Management commits to providing the necessary financial and technological resources (physical infrastructure, cloud computing resources, and secure licenses) as well as competent human resources for the implementation, maintenance, and continuous improvement of this management system, in accordance with the Human Resources management process.

4. DIMENSION I: AI USAGE GUIDELINES

4.1. SCOPE

For All Personnel: This dimension governs how any employee interacts with, consults, or uses third-party AI tools to optimize their daily tasks.

4.2. CATALOG OF AUTHORIZED AI TOOLS

The organization maintains a list of permitted AI tools that have been evaluated and approved for tasks involving information classified as Non-Sensitive or Public.
Any other AI tool that an employee wishes to use requires the prior completion of the evaluation and approval process with the AI Management System (SGIA) Manager.
The use of personal accounts for organizational activities is strictly prohibited. This commitment is undertaken by each employee upon digitally signing this Policy.
For tasks involving organizational information:

- A list of permitted AI tools—which have been evaluated and approved—is maintained.
- These tasks may only be performed using corporate accounts.

4.3. GUIDELINES FOR SAFE PROMPTING AND PROHIBITED USE

It is strictly prohibited to enter or mention the following data in any prompt, instruction, or query directed at a third-party AI system:

- Personally Identifiable Information (PII): First name, surname, national ID number (DNI), tax ID number (CUIL), health data, or any data identifying a natural person (in accordance with Law 25.326). If data processing is strictly necessary, such data must first be anonymized or pseudonymized.
- Access Information and Credentials: Passwords, passcodes, secrets, tokens, or API keys.
- Intellectual Property and Proprietary Code: Source code owned by a client or PROGUIDE, trade secrets, or strategic corporate information.
- Identifiable References: Client names, specific projects, or internal asset brands that could expose the organization's identity to third-party AI models lacking robust contractual data privacy agreements.

4.4. REPORTING ETHICAL CONCERNS AND AI INCIDENTS

- Technical Incident Channel: Incidents must be reported immediately to Support_IT@proguidemc.com.
- Types of AI incidents:
  - Loss of active corporate access
  - Suspected corporate information leakage
  - Cybersecurity incidents
  - Use of unauthorized AI tools or access via personal accounts
- Mechanism for Ethical and Bias Concerns: Employees are required to confidentially report any behavior observed in internal or third-party AI systems that conflicts with core values, or that involves harmful demographic biases or discriminatory outputs (unfairness). Ethical reports will be analyzed by the AI Management System (SGIA) Manager and addressed in accordance with the Code of Conduct.

5. DIMENSION II: AI DEVELOPMENT GUIDELINES

5.1. SCOPE

For Technical Teams: This dimension applies exclusively to the Engineering, Data Science, MLOps, and Security teams involved in the design, customization, training, or integration of AI models.

5.2. CUSTOM SOFTWARE DEVELOPMENT (AI-ASSISTED)

- Optimization, Not Blind Generation: AI coding assistance tools will be used for optimization tasks (autocompletion, refactoring, unit test generation, preliminary documentation) and never for the mass generation of complex business logic without technical oversight.
- Mandatory Code Validation: Code developed with AI assistance must undergo the same rigorous human review process (code review), including automated security vulnerability scanning and quality testing (unit and integration tests).

5.3.DATA GOVERNANCE: ORIGIN, QUALITY AND PRIVACY

Development teams must implement and document the provenance of information for model training:

- Data Traceability (Data Lineage) [Control Annex A.7.1]: A formal record will be maintained that certifies the legal origin of all data sets (datasets) used to train, validate or test AI models.
- Mitigation of Biased and Low Quality Data [Control Annex A.7.2]: A quality control process will be applied to the data sets that evaluates and mitigates statistical bias that may cause algorithmic unfairness.

5.4. MODEL LIFECYCLE GOVERNANCE (MLOPS)

For any AI system developed or customized in-house, technical teams must document and audit every phase of its lifecycle in accordance with ISO/IEC 22989 standards:

- Exploration and Design: Initial assessment of technical feasibility and ethical alignment, and definition of business success metrics.
- Training and Validation: Formal separation and methodological safeguarding of training data, validation data, and test data. Data origins and the evaluations conducted to mitigate dataset bias must be rigorously documented.
- Deployment: Controlled implementation using secure architectures and strict access control policies for containers and models.
- Monitoring and Retirement: Definition of formal processes for retiring or retraining models when significant losses in accuracy or security are detected.

5.5. ALGORITHMIC IMPACT ASSESSMENT (AIA)

For all AI systems internally classified as critical—based on criteria evaluated in the asset inventory template—an AIA must be conducted prior to their deployment into production. This assessment must comprehensively document:

- The system's detailed purpose and flow map.
- The provenance and integrity of the training data.
- The assessment of potential biases and corresponding mitigation controls.
- The designed explainability mechanisms.
- The level of human oversight and the ability to halt the system in the event of failure.

- Risk analysis and contingency plans regarding attacks or drift.

5.6. MODEL CARDS
- Model Card: Any proprietary model deployed to production must have a corresponding, up-to-date Model Card.
- Evidence Repository: To ensure traceability, Model Cards shall be formally stored in the project management tool.

5.7. CONTINUOUS MONITORING IN PRODUCTION
Automated alerts and metrics will be established to detect deviations in AI performance:
- Variable and Input Drift: Detection of statistical changes in training variables.
- Data Drift: Changes in the natural distribution of input data in production.
- Concept Drift: Changes in real-world environments that shift the model's logical boundaries.
- Fairness Metrics: Periodic monitoring for bias affecting sensitive demographic groups protected by law.

5.8. SECURE DECOMMISSIONING AND DISABLING OF AI SYSTEMS
When a model is withdrawn from production or replaced:
- Associated APIs and endpoints shall be securely disabled to prevent accidental use of a degraded system.
- A procedure for the secure digital erasure and sanitization of model data and components shall be applied to comply with confidentiality agreements and applicable personal data protection laws.

6. DIMENSION III: PRODUCT DELIVERY AND RELEASE GUIDELINES (FOR PROJECT LEADERS AND PMS)

This chapter governs contact with external clients, the legal provision of deliverables, and the mitigation of professional liabilities arising from the release of AI-assisted services.

6.1. AUTHORSHIP OF AI OUTPUT AND COPYRIGHT (LAW 11.723)
Under Argentina's Intellectual Property Law (Law 11.723), raw content generated exclusively by AI may not enjoy full protection in the absence of sufficient human intervention.
- Legal Consequence: If a deliverable (code, design, report, analysis) is provided to the client as direct, raw AI output without substantial editing, such content lacks clear ownership; consequently, third parties may freely copy or use it, and PROGUIDE would be unable to assert copyright claims.
- Delivery Control: Any product, deliverable, or service intended for a client must be reviewed, edited, and substantially adapted by the responsible human professional prior to delivery. The delivery of direct, raw AI outputs without human intervention is expressly prohibited.

6.2. LIABILITY AND TRACEABILITY GUARANTEE (AI-ASSISTED DECISION-MAKING)
Artificial Intelligence serves strictly as a professional assistance tool. Civil and professional liability for the outcomes of each project rests at all times with the operational professional who supervises and validates those outcomes. The organization operating the system shall be liable to third parties who

may be adversely affected by AI-assisted decisions.

- Mandatory Validation Signature: Any relevant deliverable or decision suggested by an AI for a client project must be validated and documented by an identifiable PROGUIDE representative. This individual must sign the validation of the AI-assisted decision prior to its delivery to the client, thereby assuming the resulting professional liability and ensuring full process traceability.
- Prohibition of 100% Automated Decisions: Making final, critical decisions based exclusively on AI outputs without significant human intervention is strictly prohibited.

6.3. DATA SUBJECT RIGHTS (ARCO) IN AI SYSTEMS

For any AI service provided to clients that involves the processing of data belonging to end-users, contractors, or employees, compliance with Articles 14 through 16 of Law 25.326 must be ensured:

- A clear record of the lifecycle and storage of data used in the AI must be maintained.
- The systems provided must be designed to respond promptly to user requests to exercise ARCO rights: a maximum timeframe of ten (10) business days for exercising the right of access, and five (5) business days for requests to rectify, update, or delete data.

6.4. CONTROL OF INTERNATIONAL DATA TRANSFERS

When delivering solutions that integrate AI cloud services (such as APIs from OpenAI, Microsoft, or other international processors), project leaders shall verify that the provider has a valid Data Processing Agreement (DPA) in place containing contractual clauses equivalent to the standards of Argentina's Personal Data Protection Law (Article 12 of Law 25.326).

6.5. EVALUATION OF THIRD-PARTY AI PROVIDERS

Before contracting and integrating APIs, cloud computing infrastructure, or AI-based SaaS tools supplied by third parties, PROGUIDE will implement a technical and legal assessment to verify:

- Ethical Alignment: The provider's policy regarding the biased and discriminatory use of its systems.
- Information Security: Compliance with safeguarding standards such as ISO/IEC 27001 or SOC.
- Data Privacy: An explicit contractual commitment from the provider not to use data and prompts submitted by PROGUIDE to train or improve its general AI models.

7. SGIA GOVERNANCE, TRAINING, AND AUDITING

7.1. STATEMENT OF APPLICABILITY (SOA)

The SGIA Manager shall maintain the Statement of Applicability (SoA) updated and documented on an annual basis, detailing the controls implemented from the Annex A section of the ISO/IEC 42001 standard and the justification for excluding those not applicable to Proguide's business.

- ### 7.2. PORTFOLIO OF REFERENCED SUB-POLICIES AND PROCEDURES

This AI Governance Policy serves as the master framework for Proguide's AI Governance System (SGIA). Compliance with the following secondary artifacts is mandated for its detailed technical and administrative execution:

- PRO-SaaS-IA: Procedure for Acceptable Use of AI Tools and Secure Queries (Provides operational details for Chapter I, applicable to all personnel).
- PRO-MLOps-GVD: Procedure for Data Governance and Model Lifecycle Engineering (Provides operational details for Chapter II, applicable to developers).
- PRO-AIA-RSC: Procedure for Algorithmic Impact Assessment and AI Risk Management (Provides operational details for section C2.4, applicable to the Ethics Committee).
- PRO-DEL-HUM: Procedure for Validating Assisted Decisions and Releasing Products to Clients (Provides operational details for Chapter III, applicable to Project Managers).
- Compliance Matrix: maps each chapter to requirements, controls, or laws.

7.3. ANNUAL TRAINING AND AWARENESS

All organization personnel shall undergo a mandatory training program at least once a year covering:

- Principles for the safe and ethical use of AI within the organization.
- AI Management System (SGIA) practices.
- Development of technical competencies identified in performance evaluations.

7.4. INTERNAL AUDIT AND COMPLIANCE

The effectiveness of this policy and all its associated controls will be strictly monitored through annual internal audits of the SGIA, coordinated by the SGIAmanager in accordance with Clause 9.2 of the ISO/IEC 42001 standard. Any detected deviation will result in the opening of a Non-Conformity record and the immediate implementation of corrective actions.

8. POLICY ISSUANCE CONTROL AND SIGNATURES

This policy will be reviewed at least annually, or whenever significant changes occur in the organizational context, the applicable regulatory framework, or the requirements of the ISO/IEC 42001 standard, to ensure its continued effectiveness and suitability.
Note: This AI policy has been documented with the assistance of Artificial Intelligence tools under approved corporate licenses.

PREPARED BY: CECILIA MARCHETTI
REVIEWED BY: ALEJANDRA CARVAJAL / DALMA BUDING
APPROVED BY: VALERIA CARBALLUDE OR CRISTIAN VELIS
DATE: JUNE 25, 2026