

Corporate Policy on the Use and Development of Artificial Intelligence

1. Objective

Establish the principles, guidelines, responsibilities, controls, and restrictions for the use, acquisition, development, training, implementation, and operation of Artificial Intelligence (AI) systems within the organization, ensuring:

- Information protection and cybersecurity.
- Regulatory and contractual compliance.
- Respect for people's rights and data privacy.
- Mitigating operational, ethical, and reputational risks.
- Transparency, traceability and human oversight of AI systems.
- The responsible and sustainable use of AI technologies.

2. Scope

This policy applies to:

- All business units and subsidiaries of Grupo México Transportes (GMXT).
- All employees, directors, contractors, suppliers and authorized third parties.
- Any AI tool, model, platform, or service used or developed by GMXT, including:
 - Generative AI.
 - Machine Learning.
 - Predictive models.
 - Intelligent automation.
 - In-house trained models.
 - SaaS services with AI capabilities.
 - APIs and third-party platforms, such as those that process:
 - Database with internal, non-public information.
 - Data sources: cameras, telephony, video conferencing, telemetry, GPS.
 - Structured or unstructured information.
 - Unpublished or unauthorized third-party information.
- In the case of technological infrastructure, the following environments are included:
 - Productive.
 - Development.
 - Testing.
 - Sandbox.
 - Cloud and on-premise.

3. Guiding Principles

Grupo México Transportes, as an organization, adopts the following principles for the responsible use of AI:

3.1. Human Supervision

Any decision derived from the result of the use and/or application of AI that may affect people, customers, employees, suppliers, regulatory compliance, security, finance, GMXT's infrastructure, civil areas, natural ecosystems or compromise the future environment without sustainable elements, must have human supervision and validation.

AI

- It is not a substitute for human responsibility.
- Cannot make irreversible autonomous decisions.
- It must allow for intervention, correction and reversal.
- It must have traceability of its decisions, use and management of each application.
- It should never threaten the safety or life of people.
- GMXT shall be the property of any development, initiative, product, service or project developed, designed or executed by employees, executives, directors, suppliers or third parties who provide services to GMXT.

3.2. Transparency and Understanding

All developments, systems, efforts and activities that use Artificial Intelligence (AI) must:

- Document the logic, purpose, and scope.
- Allow for a reasonable explanation of expected outcomes and decision-making.

- Maintain traceability of information input, models, and results.
- Be able to be fully identified as AI systems.
- All AI models must be tested and validated by the Digital Transformation Directorate before implementation.
- The responsible technical-functional team and the Management of the area with the greatest impact on the use of the model must verify the reasonableness, consistency and veracity of the results generated.
- High-impact models will require approval from the General Management and the Technical Committee.
- Employees will be able to develop and test AI solutions with authorization from their Directorate and validation from the Digital Transformation Department.
- The contracting, rental, acquisition or use of AI tools will require prior evaluation and certification from the Digital Transformation Department.

It is forbidden to use models with a high degree of opacity in critical processes without exception and to have considered the points of transparency and understanding established above.

3.3. Privacy and Data Protection

Any implementation of Artificial Intelligence must comply with the normative and regulatory framework currently applicable to Grupo México Transportes:

- Regulation of the Railway Sector
 - Railway Service Regulatory Law and its Regulations.
 - Official Mexican Standards (NOMs) of the SCT
 - Rail Transportation Regulatory Agency (ARTF) Regulations.
 - Federal Railroad Administration (FRA) regulations for sections operated in

the United States.

- Safety, Environmental and Labor Standards
 - Federal Labor Law.
 - General Law of Ecological Balance and Environmental Protection (LGEEPA).
 - STPS Standards.
- Fiscal and Customs Framework
 - Federal Tax Code (CFF).
 - Customs Law.
 - Income Tax Law (ISR).
- Corporate Governance and Ethics.
 - CNBV Provisions.
 - Securities Market Law.
 - GMXT Corporate Governance Manual.
 - GMXT Code of Ethics.
- The Federal Law on the Protection of Personal Data in Possession of Private Parties (LFPDPPP).
- Confidentiality agreements with partners, customers and suppliers.

Prohibited:

- Entering sensitive, confidential, or regulated data into unauthorized public tools.
- Use personal information without legal basis or appropriate consent.
- Reuse personal data for training without formal authorization.

3.4. Security and Cybersecurity

Every AI system must incorporate security controls aligned with corporate cybersecurity policies.

Minimum controls include:

- Identity and access management.
- MFA for admins.
- Encryption in transit and at rest.
- Activity monitoring and logging.
- Vulnerability management.
- Model integrity validation.
- Protection against prompt injection, data poisoning, and model theft.
- Segregation of environments.

3.5. Bias Prevention and Ethical Use

AI models will need to be designed and operated by minimizing:

- Discrimination.
- Unjustified biases.
- Undue exclusion.
- Disproportionate impacts.

To maintain correct ethical use and continuously optimize the operation while minimizing bias, the following should be carried out on a recurring basis:

- Periodic bias assessments.
- Statistical validations.
- Multidisciplinary reviews.
- Continuous monitoring of results.

3.6. Responsibility and Accountability

Responsibility for AI-generated outcomes will always fall on people or areas designated by the organization.

AI:

- It cannot be held legally responsible.
- It is not a substitute for formal approvals.
- It does not replace regulatory controls.

Each AI system, application and/or tool must have:

- Business Owner.
- Technical Lead/Owner.
- Security Lead/Owner.
- Compliance Lead/Owner.

The Digital Transformation Department, through the IA Squad Team, will be responsible for the evaluation, certification and monitoring of the use, quality, reliability and purpose of the Artificial Intelligence (AI) tools, services and solutions used in GMXT. Likewise, it will supervise the validity of the certifications granted and will establish, in coordination with the corresponding areas, the costs, storage schemes, operation and responsibilities associated with the internal and external digital environments owned by GMXT.

3.7. Sustainability

The organization must promote:

- Efficient use of computational resources.
- Selection of energy-efficient models.
- Inference and Training Optimization.
- Environmental Impact Assessment of AI-Intensive Loads.

4. Classification of AI Systems

AI systems will be classified according to their level of risk:

LEVEL	DESCRIPTION	EXAMPLES
Low	No relevant impact on people or critical decisions	Internal assistants, draft generation
Medium	Administrative or analytical support	Demand forecasting, document automation
High	Financial, operational, legal, regulatory, or human impact	Credit risk, operations optimization, HR, fraud, health
Forbidden	Unauthorized Use	Mass biometric surveillance, social scoring

5. Permitted Uses for AI

The organization considers the use of AI tools to be suitable for:

- Automating administrative tasks.
- Reading assistance and document analysis.
- Data analysis.
- Optimization of the core processes of the operation.
- Optimization of financial, administrative and support processes.
- Code generation and optimization under human review.
- Review, optimization, and identification of vulnerabilities to improve cybersecurity controls.
- Operational Support.
- Supervised customer service.
- Anomaly detection.
- Advanced analytics.

Any AI use case, tool, service, or model not covered by this policy shall, without exception, require prior authorization and certification from the Digital Transformation Department.

The above as long as:

- Approved controls are in place.
- Regulatory limits are respected.
- The information used is authorized.
- Have human oversight in development and validation.

6. Restricted Uses

The development of AI systems requires formal authorization from the AI and Risk Committee when one or more of the following situations arise:

- Use of sensitive data.
- Models trained on sensitive information.
- AI with an impact on work decisions.
- Generative AI connected to regulated information.
- Self-learning models in production.
- Any AI system, tool, service or model that, in the opinion of the IA Squad Team, presents potential direct or indirect risks that require assessment and authorization by the AI and Risk Committee.

7. Prohibited Uses

The use of AI is strictly prohibited in the following cases:

7.1. Prohibited Practices

- Psychological or behavioral manipulation.
- Exploiting human vulnerabilities.
- Social scoring.
- Unauthorized mass biometric surveillance.
- Emotional recognition without legal basis.
- Illegal or discriminatory profiling.

7.2. Security & Data

- Using AI to evade security controls.
- Malware or attack generation.
- Training with stolen or unauthorized data.
- Sharing sensitive information with public AI.

7.3. Critical Autonomous Operation

- Autonomous legal or financial decision-making without human oversight.
- Deploying models without validation.
- Automatic modification of models in production without formal governance.

8. AI Corporate Governance

8.1. AI Committee

The organization will establish an Artificial Intelligence Committee made up of representatives from the following areas of specialty and directions:

- Technology – Digital Transformation Directorate
- Cybersecurity – Digital Infrastructure Directorate
- Risk Management – Finance Directorate
- Compliance – Legal Directorate
- Legal – Legal Directorate
- Audit – Audit Directorate
- Business Functions – General Administration Directorate, General Operations Directorate, General Commercial Directorate
- Data Protection – Legal Directorate

The functions of the Committee are:

- Approve AI initiatives.
- Assess risks.
- Authorize exceptions.
- Monitor compliance.
- Review incidents and biases.

9. Roles and Responsibilities

The organization must communicate the role and responsibilities to the organization's collaborators in terms of the development and use of AI:

ROLE	RESPONSIBILITY
Users	Responsible Use and Policy Compliance
Process Owners	Validate results and risks
Digital Transformation	Development and technical validation of AI applications in accordance with this policy
Digital Infrastructure	Infrastructure and operation
Cybersecurity	Protection and monitoring
Legal	Regulatory Compliance
Audit	Independent verification
IA Committee	Governance and approval
IA Squad Team	Specialized AI team with technical and certification authority

10. Requirements for new AI developments

From the point of view of Information Technologies, all development must include:

10.1. Documentation

- Development Objective, Model and/or System.
- Description of the dataset used.
- Description of the variables considered.
- Defining Metrics.
- Risks identified.
- Known scope and limitations.

10.2. Validation

- Technical validation.
- Functional testing.
- Bias assessment.
- Accuracy validation.
- Cybersecurity assessment.
- UAT Testing.
- Business approval.

10.3. Monitoring

- Model drift.
- Accuracy.
- Incidents.
- Misuse.
- Anomalous behaviors.

11. Third-Party Management

Any supplier of Grupo México Transportes that develops and/or makes use of AI tools must:

- Comply with corporate security requirements.
- Enable risk assessment.
- Establish the required confidentiality agreements.
- Define and communicate the processing of the data used.
- Inform the location of the storage and processing of information.
- Ensure the non-misuse of information.

12. Incident Management

Any AI-related incidents should be reported immediately to:

- Cybersecurity.
- Risks.
- Compliance.
- IA Squad Team.

These incidents include, but are not limited to, events of:

- Information leakage.
- Biases detected.
- Critical erroneous results.
- Misuse.
- Model engagement.
- Unauthorized access.

13. Audit & Compliance

The organization may at any time:

- Audit any AI system.
- Request technical and documentary evidence.
- Suspend high-risk models.
- Revoke access.
- Applying disciplinary sanctions.

14. Training

Any employee who uses AI tools, models, or capabilities must be trained on:

- Risks.
- Privacy.
- Security.
- Biases.
- Responsible use.
- Permitted limits.

15. Sanctions

Failure to comply with this policy may result in:

- Suspension of access.
- Disciplinary measures.
- Contractual termination.
- Legal actions.
- Regulatory reports.

16. Relationship to Other Policies

This policy complements the current policies of Grupo México Transportes:

- Information Security Policy.
- Personal Data Protection Policy.
- Technology Risk Policy.
- Code of Ethics.
- Safe Development Policy.
- Supplier Management Policy.

17. Validity and Revision

This policy shall:

- Get checked at least once a year.
- Update on relevant regulatory or technological changes.
- Be approved by Senior Management and the corresponding Committee.