1. PURPOSE

1.1 This policy establishes clear, ethical, and responsible guidelines for the use of artificial intelligence (AI) technologies within the organization, ensuring that AI use aligns with applicable legislation, information security standards, and institutional values.

2. SCOPE

2.1 This policy applies to all company personnel, including employees, contractors, service providers, and third parties who use or interact with AI systems in the workplace.

3. RESPONSIBILITY

3.1 Users are responsible for following this policy when using AI to perform their duties.

3.2 MADATA is responsible for evaluating cases in which GCC's institutional artificial intelligence tool does not meet the user's functional or operational requirements It is the responsibility of a member of the Extended Leadership Team or a Corporate Business Leader to approve users who, due to the nature of their position, require cell phone service.

3.3 The IT Committee is responsible for reviewing and authorizing cases in which the use of an AI tool other than the institutional one is requested.

3.4 Corporate and Divisional SLT are responsible for authorizing extraordinary cases.

4. DEFINITIONS

4.1 Artificial Intelligence (AI): Technology capable of emulating human reasoning to perform tasks.

4.2 Corporate and Divisional SLT: Key figures relevant to the analysis and evaluation of specific issues.

4.3 LFPDPPP: Federal Law on Protection of Personal Data Held by Private Parties.

5. CONTENT

5.1 AI should be used as a support tool, not as a substitute for human judgment. This means that any consultation should be purely informative, avoiding decisions based solely on artificial intelligence.

5.2 Data Protection and Security All use of AI must comply with the LFPDPPP and internal information security policies.

5.3 In order to ensure information security, operational integrity, and regulatory compliance, only tools authorized by GCC are permitted for use.

5.4 The use of external or unauthorized solutions is strictly prohibited.

5.5 In cases where the institutional tool does not meet the user's functional or operational requirements, the use of an external tool may be considered, provided that it is evaluated and authorized by the appropriate authorities. Any acquisition, licensing, or enabling of these solutions must be managed in accordance with policy PO-DTI-TI-32 CONTROL OVER AUTHORIZED/UNAUTHORIZED

LICENSED SOFTWARE, ensuring compliance with institutional standards for security, privacy, and control are met.

5.6 Uses of AI

5.6.1 Automating repetitive tasks, improving productivity, or facilitating decision-making, always under human supervision.

5.6.2 Assisting in writing, programming, information analysis, or translation, as long as no sensitive information is involved (Reference to Policy).

5.6.3 Organizing tasks, dates, and reminders.

5.6.4 Creating document templates.

5.7 It is prohibited to use AI for:

5.7.1 Processing, entering, or disclosing confidential, sensitive, or protected information (PO-DTI-TI-49 INFORMATION CLASSIFICATION POLICY)

5.7.2 The use of personal email accounts to access, contract, or register on artificial intelligence platforms other than the authorized institutional tool is strictly prohibited.

5.7.3 Making automated decisions in sensitive processes, such as performance evaluations, hiring, or sanctions Generating false, misleading, discriminatory, or defamatory content

5.7.4 Generating false, misleading, discriminatory, or defamatory content

5.7.5 Using AI to surveil, record, or monitor individuals without consent or legal authorization.

5.7.6 Completely replacing human oversight in critical or high-impact processes

5.8 Consequences for Non-Compliance

5.8.1 The misuse of artificial intelligence may result in warnings or administrative sanctions in accordance with the current Cybersecurity Consequences Matrix.

5.9 Development of AI applications

5.9.1 All development of applications that integrate AI must:

5.9.1.1 Be evaluated and approved by Madata and the IT Committee.

5.9.1.2 Conduct a privacy and security impact assessment.

5.9.1.3 Comply with principles of ethical design, transparency, and explainability.

5.9.1.4 Apply secure development methodologies and algorithmic bias testing.

5.9.1.5 Document its architecture, data sources, functionalities, and restrictions.

5.9.1.6 Ensure the traceability of automated decisions and human review mechanisms.

6. PROCEDURE

N/A

7. REFERENCES

PO-DTI-TI-32 CONTROL OVER AUTHORIZED/UNAUTHORIZED LICENSED SOFTWARE.

PO-DTI-TI-49 INFORMATION CLASSIFICATION POLICY.

8. APPENDIX

N/A

9. DOCUMENT REVISION DATE

Revision No.	Date	Changes Description
0	June 2025	Original Document.

10. AUTHORIZATIONS

Elaborated	Reviewed	Authorized
	Maria Elena Rojas/Internal Control	Ramón Velazco Unzueta / Corporate Controller