QUALITY MANAGEMENT SYSTEM POLICY

Proguide Global Services is a business consulting firm driven by the quality and professionalism of our team and focused on our primary objective: becoming a solid strategic partner for our clients. To this end, we effectively manage quality and information security, ensuring confidentiality, integrity, and availability.

VISION

To be the most innovative regional service consultancy regarding products and services for a more efficient and sustainable world.

MISSION

- Conduct activities within the framework of an integrated management system, ensuring the quality of our services and products while complying with applicable legal requirements.
- Bring diverse perspectives and life experiences to our teams, viewing diversity as an integral part of the organization, and prioritizing talent, skills, and qualifications above all else.
- Continuously improve both the services we offer—through the ongoing enhancement of our processes—and the quality management of our operations.
- Strengthen our market image and add value to our services by meeting the needs and expectations of our clients and prospective customers.

INFORMATION SECURITY POLICY

PURPOSE

The information security management system preserves the confidentiality, integrity, and availability of information through the application of a risk management process and provides interested parties with confidence regarding the proper management of risks.
The purpose of this policy is to establish an information security management framework within the organization to ensure the confidentiality, integrity, and availability of information assets.

SCOPE

This policy applies to all employees, contractors, suppliers, and third parties covered by the IMS who have access to the company's information assets. It encompasses all information systems, networks, applications, physical locations, and any other means used to process, store, or transmit information.

Our scope associated with the SGI
“Custom Software Development and Maintenance.”

INFORMATION SECURITY PRINCIPLES

Our Information Security Policy is based on the principles of information security:
Confidentiality: Information is accessible only to authorized persons.
Integrity: Information is accurate and complete, and processing methods are correct.
Availability: Information is available to authorized users when needed.

INFORMATION SECURITY OBJECTIVES

- Protecting Information: We protect information by ensuring the confidentiality, integrity, and availability of all information managed within the organization.
- Managing Risks: We manage risks by identifying, assessing, and mitigating those related to information security.
- Responding to Incidents: We respond to incidents using effective procedures for the detection, notification, and management of information security incidents.
- Training and Raising Awareness: We ensure that all employees understand and comply with information security policies and procedures through continuous training and awareness-raising.

- Maintaining Business Continuity: We implement and maintain business continuity and disaster recovery plans to minimize the impact of disruptions and ensure information availability.
- Continuous Improvement: We continuously review and improve the information security management system to adapt to changes in the environment, technologies, and threats.

RESPONSIBILITIES

Senior Management: Responsible for ensuring support and commitment to information security, providing necessary resources, and approving and periodically reviewing the information security policy.
Technology Manager: Responsible for the implementation and management of the Information Security Management System (ISMS).
Employees: Responsible for complying with information security policies and procedures, reporting security incidents, and participating in required training.

RISK MANAGEMENT

We conduct periodic risk analyses to identify, assess, and manage any potential threats to information security. This process enables us to better understand the vulnerabilities to which we are exposed and make informed decisions on how to address them.
Once risks are identified, we implement specific, appropriate controls to mitigate their impact and likelihood of occurrence.
These controls are not limited to technology; they also encompass organizational, human, and procedural measures that strengthen our comprehensive risk management approach.
Furthermore, we regularly review the effectiveness of these controls, ensuring they remain aligned with evolving threats and changes in the business environment. This proactive approach allows us to maintain a secure and resilient environment, tailored to our business needs and the demands of our clients and stakeholders.

ACCESS CONTROL

We ensure that access to information assets is strictly controlled and granted only upon authorization, always aligned with business needs and based on specific user roles. We adopt the principle of least privilege, meaning each user has access only to the information and resources necessary to fulfill their responsibilities, thereby minimizing the risk of unnecessary or improper access.
To ensure security, we employ robust authentication methods, including strong passwords and multi-factor authentication. These mechanisms add extra layers of protection, reducing the likelihood of unauthorized access even if credentials are compromised.

Furthermore, we have implemented both physical and logical access controls. Physical controls restrict access to our facilities and to devices that store or process sensitive information, while logical controls focus on protecting systems and networks through firewalls, encryption, and permission-based access policies. This comprehensive approach to access control allows us to safeguard the integrity, confidentiality, and availability of information, maintaining a secure environment for our critical assets.

SECURITY INCIDENT MANAGEMENT

We have established a detailed procedure for managing information security incidents, ensuring that each incident is handled efficiently and systematically. All incidents, regardless of their magnitude, are reported immediately and managed in accordance with this procedure, which outlines clear stages ranging from initial detection to final resolution and subsequent analysis. This process enables us not only to respond rapidly to threats but also to learn from each incident, thereby strengthening our defenses and preventing similar future events. Comprehensive documentation and tracking of every incident ensure a complete overview of vulnerabilities and necessary corrective measures, thereby maintaining our organization's security and resilience. This procedure includes incidents associated with artificial intelligence systems.

BUSINESS CONTINUITY

We have implemented Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) designed to ensure that, in the event of an interruption, information availability and the operation of our critical services are maintained or restored quickly and effectively. These plans cover a wide range of potential scenarios—from technical failures to natural disasters—and detail the steps to be taken to minimize the impact on our operations and protect the interests of our clients and stakeholders.
The BCP is structured to ensure that essential business functions continue to operate with minimal disruption, while the DRP focuses on recovering technology infrastructure and restoring data. Both plans are regularly reviewed and updated to reflect environmental changes, emerging threats, and lessons learned from exercises and simulations. This way, we are prepared to handle any contingency, ensuring our organization's resilience and the continuity of the services we provide.

LEGAL AND REGULATORY COMPLIANCE

We strictly comply with all applicable laws and regulations regarding information security, ensuring that our practices remain aligned with current legal and regulatory standards. This commitment not only enables us to operate within the legal framework but also reinforces the trust our clients and partners place in our ability to handle information securely and responsibly.
We conduct periodic audits to verify and ensure ongoing compliance with the ISO 27001 and ISO/IEC 42001 standards, guaranteeing that our security processes and controls remain aligned with the requirements of these international certifications. These audits allow us to identify and promptly

correct any deviations, ensuring that our policies and procedures not only meet current expectations but also anticipate future challenges and regulatory changes.

TRAINING AND AWARENESS

We provide regular training to all employees, ensuring they understand and adhere to the information security policies and procedures we have established. These training sessions cover not only technical aspects but also address the importance of security in day-to-day operations, helping employees recognize and handle potential threats.
Furthermore, we actively promote a culture of information security throughout the organization. This involves not only training but also continuous awareness-raising regarding the importance of protecting our assets and sensitive data. Through campaigns, communications, and leading by example, we foster an environment where every team member feels responsible for and committed to security, thereby ensuring that information protection is a priority shared by all.

REVIEW AND IMPROVEMENT

We conduct periodic internal audits and senior management reviews to evaluate the effectiveness of our Information Security Management System (ISMS) and of our Artificial Intelligence Management System (AIMS). These review processes enable us to identify areas for improvement and ensure that our practices and controls remain effective and aligned with our security objectives. Based on the results of these audits and reviews, as well as changes in the risk landscape, we implement continuous improvements to the ISMS and in the AIMS. This approach allows us to proactively adapt to new threats and challenges, constantly strengthening our defenses and response capabilities.

COMMUNICATION

We ensure that this security policy is clearly communicated to all employees and relevant stakeholders, guaranteeing that they understand its importance and their responsibilities. Furthermore, we keep the policy readily available and accessible throughout the organization, making it easy for anyone to consult it whenever necessary. This commitment to transparency and effective communication reinforces our security culture and ensures that everyone is aligned with our information protection objectives and practices.

ARTIFICIAL INTELLIGENCE POLICY

PURPOSE

The Artificial Intelligence Management System (AIMS) establishes the framework for PROGUIDE to use, develop, and integrate artificial intelligence systems in an ethical, legal, secure, transparent, and responsible manner, in accordance with the ISO/IEC 42001 standard and applicable legislation. The AIMS is part of the Integrated Management System, alongside quality management and information security management.

SCOPE

This policy applies to all employees, contractors, and suppliers covered by the Integrated Management System (IMS) who use, develop, or deliver artificial intelligence tools, systems, or models within the scope of "Custom Software Development and Maintenance," specifically in the following roles:

- Internal use of artificial intelligence as a support tool in the design, development, and maintenance processes for custom software.
- Internal use of artificial intelligence as a support tool in the organization's administrative and internal management processes.
- Integration of artificial intelligence-based and data-driven systems into custom software solutions for clients.

ARTIFICIAL INTELLIGENCE PRINCIPLES

Our Artificial Intelligence Policy is founded on the following principles:
Accountability and Human Oversight: AI-assisted decisions and outcomes are subject to human oversight. AI serves as a supporting tool and does not replace professional judgment; responsibility for every outcome always rests with an identifiable individual, and all results are subject to review for compliance with applicable legal requirements.
Fairness and Non-Discrimination: We do not use AI that could perpetuate or amplify biases leading to unfair treatment based on race, gender, age, religion, sexual orientation, or any other protected characteristic.
Transparency and Explainability: We document when and how AI is used, and we ensure that systems in production are capable of explaining how they arrive at their results.
Security, Robustness, and Reliability: We test AI systems against attacks, unforeseen failures, and performance degradation, and we monitor them continuously to detect any deviations.
Privacy and Data Protection: We protect personal data and confidential information processed using AI tools or systems, in accordance with Law 25.326, our Information Security Management System (based on the ISO/IEC 27001 standard), and our agreements with clients.
Efficiency and Responsible Resource Use: We use AI to enhance productivity and the quality of our services, employing authorized tools and ensuring the rational use of resources.
Continuous Improvement: We continuously review and improve our Artificial Intelligence

management system to adapt to changes in the environment, technologies, and potential threats.

ARTIFICIAL INTELLIGENCE OBJECTIVES

Based on the principles, and for each of the scopes defined in this policy, we establish the following objectives:

SCOPE	PRINCIPLE OF POLICY	OBJECTIVE
Internal use of AI as a support tool for administrative and internal management processes.	Security, Robustness, and Reliability	Ensure that staff use exclusively corporate accounts and authorized tools from the official catalog for company tasks.
Internal use of AI as a support tool for administrative and internal management processes.	Security, Robustness, and Reliability	Ensure that AI-based tool providers comply with security and privacy agreements.
Internal use of AI as a support tool for administrative and internal management processes.	Security, Robustness, and Reliability	Ensure that no personal data, credentials, or confidential information are exposed.
Internal use of AI as a support tool for administrative and internal management processes.	Transparency and Explainability	Ensure comprehensive training and annual awareness-raising for all employees regarding the principles for the safe and ethical use of AI.
Internal use of AI as a support tool for administrative and internal management processes.	Efficiency and Responsible Use of Resources	Increase the productivity of the development team.
Internal use of AI as a support tool for administrative and internal management processes.	Efficiency and Responsible Use of Resources	Optimize software development costs through the efficient and controlled use of artificial intelligence tools for application development.
Internal use of AI as a support tool for administrative and internal management processes.	Privacy and Data Protection	In accordance with Law 25.326, the Information Security Management System as per the ISO/IEC 27001 standard, and agreements with our clients.
Integración de sistemas basados en IA y datos en soluciones de software a medida para clientes.	Responsibility and Human Oversight	Any AI system intended for customers must include a mechanism that identifies a party responsible for the outcomes, as well as a reminder for all users regarding the limitations of the AI's reasoning.
Integración de sistemas basados en IA y datos en soluciones de software a medida para clientes.	Responsibility and Human Oversight	Any AI system in production can be stopped or routed for human intervention.
Integración de sistemas basados en IA y datos en soluciones de software a medida para clientes.	Equity and Non-Discrimination	Ensure that the AI systems we integrate do not discriminate.
Integración de sistemas basados en IA y datos en soluciones de software a medida para clientes.	Transparency and Explainability	The use of AI, as well as an explanation of the interpretation of the results, is documented.
Integración de sistemas basados en IA y datos en soluciones de software a medida para clientes.	Privacy and Data Protection	In accordance with Law 25.326, the Information Security Management System as per the ISO/IEC 27001 standard, agreements with our clients, and the Data Management Procedure for AI
Integración de sistemas basados en IA y datos en soluciones de software a medida para clientes.	Security, Robustness, and Reliability	AI incidents are detected and contained in a timely manner.
Integración de sistemas basados en IA y datos en soluciones de software a medida para clientes.	Security, Robustness, and Reliability	Ensure that the AI systems released are robust according to the acceptance criteria.

The indicators, targets, and individuals responsible for each objective are managed via the AI Objectives Dashboard, which is periodically reviewed by Management.

MANAGEMENT COMMITMENTS

- Establishing, communicating, and reviewing artificial intelligence objectives.
- Complying with legal, regulatory, and contractual requirements applicable to the use and development of artificial intelligence, as well as the requirements of the ISO/IEC 42001 standard.
- Providing the necessary financial, technological, and competent human resources to implement, maintain, and improve the AI Management System (AIMS).
- Continuously improving the AIMS, ensuring that its controls evolve in step with technological advancements.

RESPONSIBILITIES

Top Management: Responsible for approving this policy, allocating necessary resources, authorizing the release of systems classified as "High" or "Very High" risk, and reviewing the performance of the AIMS.
AIMS Manager: Responsible for implementing and maintaining the AIMS, managing the Statement of Applicability, and coordinating internal audits and the monitoring of objectives.
Data Scientist: Responsible for reviewing AI-related risks and designing training and testing experiments.
Employees and Contractors: Responsible for adhering to the AI Responsible Use Guidelines, reporting incidents and ethical concerns, and participating in required training.

AI RISK AND IMPACT MANAGEMENT

We identify, assess, and address risks associated with AI systems throughout their entire lifecycle, including their impact on individuals and society. Before deploying any system, we conduct an impact assessment.

ASSOCIATED DOCUMENTS

This policy is further detailed in the AI Responsible Use Guidelines, the AI Development Operating Model, and the procedure for the "Artificial Intelligence System Lifecycle Integrated into Software Development."

MANAGEMENT BOARD

NOVEMBER 2026

CODE: PSGC VERSION: 06

PROGUIDE