QUALITY MANAGEMENT SYSTEM POLICY

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

VISION

To be the regional services consultancy with the greatest innovation in products and services for a more efficient and sustainable world.

MISSION

- Develop activities within the framework of an integrated management system, ensuring the quality of our services and products.
- Contribute perspectives and life experience to our teams, understanding diversity as a whole within the organization. Value talents, skills, and training above all else.
- Continuously improve both the services we offer, based on the continuous improvement of our processes, and the management quality of our operations.
- Maintain the work dynamic within the framework of compliance with all corresponding legal requirements and other applicable derivatives.
- Consolidate our image in the market and add value to our services by meeting the needs and expectations of our clients and prospects.

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 stakeholders with confidence in the appropriate 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 SGI who have access to the company's information assets. It covers 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 following Information Security principles:
Confidentiality : Information is accessible only to authorized individuals.
Integrity: Information is accurate and complete, and its processing methods are correct.
Availability: Information is available to authorized users when needed.

INFORMATION SECURITY OBJECTIVES

- Protect Information: We protect information by ensuring the confidentiality, integrity, and availability of all information we manage in the organization.
- Risk Management: We manage risks by identifying, evaluating, and mitigating those related to information security.
- Responding to Incidents: We respond to incidents using effective procedures for detecting, reporting, and managing information security incidents.
- Training and awareness: We ensure that all employees understand and comply with information

security policies and procedures through continuous training and awareness.

- Maintain 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 continually 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 the necessary resources and carrying out the approval and periodic review of the information security policy.
Technology Manager: Responsible for the implementation and management of the information security management system (SGI).
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 information security threats. This process allows 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 and appropriate controls to mitigate their impact and likelihood of occurrence.
These controls are not limited to technology but also include organizational, human, and procedural measures that strengthen our comprehensive approach to risk management.
In addition, 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 the needs of our business and the demands of our customers and stakeholders.

ACCESS CONTROL

We ensure that access to information assets is strictly controlled and authorized only, always aligned with business needs and based on specific user roles. We adopt the principle of least privilege, meaning that each user only has access to the information and resources necessary to fulfill their responsibilities, thus minimizing the risk of unnecessary or improper access.
To ensure security, we use strong authentication methods, including strong passwords and multi-factor authentication. These mechanisms add additional layers of protection, reducing the possibility of unauthorized access even if credentials are compromised.
In addition, we have implemented both physical and logical access controls. Physical controls limit

access to our facilities and 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 in an efficient and structured manner. All incidents, regardless of their magnitude, are reported immediately and managed according to this procedure, which includes clear stages from initial detection to final resolution and subsequent analysis. This process not only allows us to respond quickly to threats but also to learn from each incident to strengthen our defenses and prevent similar events in the future. Thorough documentation and follow-up of each incident ensure we have a complete view of vulnerabilities and the necessary corrective measures, thus maintaining the security and resilience of our organization.

BUSINESS CONTINUITY

We have implemented business continuity (BCP) and disaster recovery (DRP) plans designed to ensure that, in the event of a disruption, the availability of information 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 customers and stakeholders. The BCP is structured to ensure essential business functions continue to operate with minimal disruption, while the DRP focuses on the recovery of the IT infrastructure and data restoration. Both plans are regularly reviewed and updated to reflect changes in the environment, new threats, and lessons learned from exercises and simulations. This way, we are prepared to face any contingency, ensuring the resilience of our organization and the continuity of the services we offer.

LEGAL AND REGULATORY COMPLIANCE

We rigorously comply with all applicable laws and regulations regarding information security, ensuring that our practices are always aligned with current legal and regulatory standards. This commitment not only allows us to operate within the legal framework but also reinforces the confidence of our customers and partners in our ability to handle information securely and responsibly.
We conduct periodic audits to verify and ensure ongoing compliance with ISO 27001, ensuring that our security processes and controls remain in line with the requirements of this international certification. These audits allow us to identify and correct any deviations in a timely manner, 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 follow our established information security policies and procedures. These trainings not only cover technical aspects but also address the importance of security in everyday life, helping employees recognize and manage potential threats.
In addition, we actively promote a culture of information security throughout the organization. This involves not only training but also ongoing awareness of the importance of protecting our assets and sensitive data. Through campaigns, communications, and daily example, we foster an environment in which every team member feels responsible and committed to security, ensuring that information protection is a shared priority for everyone.

REVIEW AND IMPROVEMENT

We conduct periodic internal audits and senior management reviews to assess the effectiveness of our Information Security Management System (SGSI). These review processes allow 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 environment, we implement continuous improvements to the SGSI. 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, ensuring 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 review whenever needed. This commitment to transparency and effective communication reinforces our security culture and ensures everyone is aligned with our information protection goals and practices.

The General Management

APRIL 2025

CODE: PSGC VERSION: 04

PROGUIDE