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.

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 standard, guaranteeing that our security processes and controls remain consistent with the requirements of this international certification. These audits allow us to identify and rectify 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 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). 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. 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.

The General Management

SEPTEMBER 2026

CODE: PSGC VERSION: 05

PROGUIDE