INFORMATION SECURITY POLICY

INDEX

1. OBJECTIVE

The Information Security Policy establishes the reference framework by which SGF Global implements the minimum security standards to adequately protect its information and cybersecurity assets and promote the achievement of the organization's strategic objectives in this area, such as:

- Ensure the confidentiality, integrity, and availability of confidential client and candidate information by implementing appropriate security controls to prevent unauthorized disclosure.
- Ensure strict compliance with applicable laws and regulations regarding privacy, data protection and information security, while strictly adhering to all contractual obligations established with our customers to ensure the confidentiality and security of stored data managed by our organization.
- Identify and manage the risks and opportunities that can impact information security and have an impact on the organization.
- Implement and operate information security processes, controls, and other measures to address risks and take preventive and/or corrective actions to mitigate them.
- Ensure the protection and security of information assets according to their confidentiality and criticality; keep assets current and classified.
- Implement and maintain an ISMS that meets the requirements of ISO 27001 to ensure that information assets are properly protected and managed.
- Establish appropriate access controls to ensure that only authorized personnel have access to confidential and sensitive information, and that privileges are assigned in an appropriate and controlled manner.
- Information security policies, procedures and standards must be followed by all SGF Global employees.
- Employee training and awareness of information security best practices to reduce internal threats and improve security culture.
- Ensure that any breach or disruptive event is managed effectively and quickly with an information security incident response plan.

2. SCOPE

This Information Security Policy applies to everyone employed and/or contracted by SGF Global, and to any vendor, third party or interested party that has access to the systems and/or information of the company.

3. REFERENCES

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems - Requirements.
- ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls.

4. RESPONSIBILITIES

The approval of the Information Security Policy is made by the Director, any changes, corrections, or updates must be proposed in the Information Security Committee (ISC) and/or approved by the General Manager and communicated to all users, suppliers and stakeholders of SGF Global through the various means at its disposal.

Senior management should provide guidance and support for information security management in accordance with business requirements and applicable laws.

SGF Global's Information Security Committee (ISC) should establish clear guidelines to support information security through the implementation and maintenance of security policies throughout the organization. This committee should be a multidisciplinary group with representatives from various areas of the organization.

It is also the responsibility of the Information Security Committee (ISC) to identify, update, and document all regulatory and legal requirements and to identify controls to meet those requirements.

Laws and regulations should be identified when acquiring and implementing cryptographic controls, licenses, auditing tools, conversation recordings, and other regulated items.

SGF Global employees' personal information must be protected according to local laws.

If an amendment or change to the General Policy is required, its implementation and subsequent compliance must be reviewed by the Information Security Committee (ISC) and/or the Director of SGF Global.

In addition, an individual responsible for information security at SGF Global has been designated as the Information Security Officer (OSI), who in turn reports to the Director. This person is responsible for maintaining the level of security required by the organization, as well as the security of the various computer systems and telecommunications networks supported. In this capacity, the OSI works to prevent improper or unlawful behavior by the various users of IT resources and by external users who access the Company's resources.

These responsibilities include legal and ethical obligations regarding the proper functioning and protection of SGF Global's information, as well as the management of the various interests pursued by SGF Global.

The Information Security Officer (ISO) will be a member of the Information Security Committee (ISC) and will have primary responsibility for documenting, updating, and implementing the Security Policy. Likewise, the ISO will periodically evaluate the effectiveness of these policies and determine modifications whenever deemed necessary to ensure the protection of information and related assets at SGF Global.

5. VOCABULARY

- **Availability:** The property of information to be accessible and usable when needed by an authorized entity.
- **Codification:** The process of encoding sensitive information to prevent it from reaching unauthorized persons.
- **Confidentiality:** The property of information not being available for disclosure to unauthorized individuals, entities, or processes.
- **Control:** Policies, procedures, practices, and organizational structures designed to keep information security risks below acceptable risk levels.
- **Encryption:** Is the process of making information considered important unreadable. Once encrypted, the information can only be read by applying a key.
- **Information Security Incident:** A breach or threat that affects the confidentiality, availability, integrity, and continuity of services provided.
- **Integrity:** The property of data, systems, and processes that ensures that information remains complete, accurate, and free from unauthorized changes over time.
- **Risk:** The possibility that a specific threat will exploit a vulnerability to cause loss or damage to an information asset. It is typically viewed as a combination of the likelihood of an event and its impact.
- **Threat:** A potential cause of an unwanted event that could cause damage to a system or organization.
- **Vulnerability:** A weakness in a system or asset that can be exploited to cause damage.

6. POLICY DEVELOPMENT

6.1 Information Security Policy.

The purpose of SGF Global's Information Security Policy is to protect information assets from all internal and external threats, whether intentional or accidental.

It is the policy of the organization to ensure, among other things, the following principles:

- Confidentiality of information so that only authorized users have access.
- Integrity of information that is maintained to prevent unauthorized changes.
- Availability of information that is secured in accordance with business process requirements.
- Compliance with laws and regulations.
- Commitment to compliance with applicable information security requirements.
- Fulfill contractual obligations to our customers.
- Information security training, culture and awareness for all employees, contractors, customers, and suppliers.

6.2 Information Security Risk Management.

SGF Global creates a culture of information security risk management by establishing, formalizing, and implementing a risk assessment and response methodology.

All in-scope information assets should be evaluated periodically and/or when significant organizational changes occur, particularly by process owners, to determine the minimum controls necessary to reduce and maintain risk at acceptable levels.

The design, development and implementation of the controls required to minimize risk is the responsibility of the process owner, with the support of the various areas of the organization; in the case of assets, the owners of these assets will be responsible for identifying and mitigating the risks they may present.

The risk assessment will be carried out according to the methodology defined in SGF Global, it is important to clarify that the risks identified must always be managed.

6.3 Information and system access control.

Depending on the classification of SGF Global information, access controls must be established. The employees of SGF Global should only have access to the information that is necessary for them to carry out their job functions.

Access to information by third parties and interested parties should be granted only for the required functions and with mechanisms that ensure both the identity of those granting access and the confidentiality, integrity and availability of the information.

6.4 Information Security Incident Management..

A documented plan is in place for communicating, responding to, monitoring, and determining the root cause of the incident, including:

- ✓ Roles and responsibilities.
- ✓ Communication strategies and appropriate channels.
- ✓ Incident response procedures.
- ✓ Regulatory requirements.
- ✓ Recovery procedures.
- ✓ Backup Procedures.
- ✓ Evidence collection.

The organization has a trained and qualified team to monitor and respond to incidents, in addition to verifying alerts from SGF Global's security devices such as SIEM, IDS, firewalls, and others.

The Incident Plan should be tested at least annually and improvements made based on lessons learned from both simulated and actual incidents. All employees should be responsible for observing and reporting events, incidents, vulnerabilities and misuse of SGF Global's information assets in accordance with the established procedure.

6.5 Information Security Business Continuity.

It is the responsibility of the organization's management to approve a Business Continuity Plan that covers SGF Global's essential and critical activities, as any disruption in business processes will affect operations.

The plan should include controls designed to identify and mitigate risks, to limit the consequences of the various incidents and, ultimately, to ensure the immediate recovery of essential operations.

All information systems must have contingency plans and the necessary resources to ensure business continuity, as well as knowledge of the business continuity plans of suppliers that provide critical services to the organization, as a fundamental part of business support.

6.6 Information Security Training and Awareness.

With the support and advice of the Information Security Officer (ISO), the policy is approved by the Director and disseminated by the Information Security Committee (ISC).

The Information Security Management System (ISMS) and all managers, deputy managers and directors of the organization are responsible for disseminating this policy.

This document and the documents related to this system are available to the employees according to their level of classification and to the critical suppliers through what is established by each management responsible for that supplier and/or is determined in accordance with the NDA signed between both parties. In the same way, the policy will be available for the knowledge of employees, contractors, suppliers and interested parties through the means available within the organization.

All SGF Global employees and, when applicable, external employees (suppliers and stakeholders with critical functions), must receive training on security requirements, legal responsibilities and business controls, the consequences of non-compliance and the benefits of the Information Security Management System (ISMS), and the proper use of information processing assets and applications, on joining the organization and in accordance with the provisions of the personnel orientation provided by the SGF Global Human Resources Department in the "Onboarding" chapter.

This training must be updated on a regular basis, and Human Resources is responsible for verifying that employees have received appropriate training and that updates have been made.

6.7 Information Security Compliance and Auditing.

The Information Security Committee (ISC), with the advice of the Information Security Officer (ISO), will identify all elements, controls and/or systems that will be subject to the audit process to evaluate:

- ✓ Compliance objectives established for each control.
- ✓ Compliance with regulations and standards for each control.
- ✓ The generation of evidence necessary to demonstrate the maturity of the controls.
- ✓ Evaluate the compliance measures previously established in the organization's various policies and procedures.
- ✓ Apply corrective actions and improvements generated during the implementation processes of the various controls within the organization.

They shall be planned and performed in accordance with the audit plans established by the organization.

6.8 Acceptable Use of Information Security Assets.

The organization shall establish policies for access and acceptable use of information assets. Users shall comply with these policies, such as:

- ❖ Explicit administrative approval
- ❖ Usage authentication
- ❖ List of available resources
- ❖ Tagging equipment with owner information
- ❖ List of corporate-approved devices
- ❖ Identify the location of network assets
- ❖ Automatic session termination for remote access technologies
- ❖ Remote access to suppliers only when strictly necessary.

All SGF Global system components (servers, PCs, notebooks, network devices) have configuration norms and standards. This ensures that all security vulnerabilities are addressed and that best practices in security and cybersecurity are followed.

6.9 Information Security Violations.

Any situation demonstrating a violation of the Information Security Policy by employees, suppliers and/or interested parties directly or indirectly involved in the management of the Organization's technological infrastructure and information systems may result in a process to be initiated by the immediate supervisor or third party responsible, based on the evidence gathered, which may include, but is not limited to, the following:

- Disciplinary actions taken by the area that the Organization has provided for this purpose, according to the guidelines established by the Organization's Regulations and Policies, the Organization's Code of Ethics, the special clauses established with employees and/or contractors in their employment contracts, and/or all that is defined according to the laws of the country regarding the protection of sensitive data, computer crimes and any other related to the security of information.
- Suspension or restriction of access to information processing areas.
- Termination of employment or business relations (according to local regulations).
- Civil or criminal proceedings resulting from disciplinary actions.

7. POLICY REVIEW

To ensure its validity and compliance, this policy will be reviewed at least every 12 months. It is also subject to change as the organizational structure for managing security changes, as long as it is reviewed by the Information Security Committee and/or approved by the Director.

8. CHANGE CONTROL

Version	Descriptions	Date	Prepared	Revised	Approbator
01	Creación del Documento	14/08/2023	Consema	J. Ramirez	M. Sion