Information Security Policy

Repository: [*Repositório\General\Manual e Política\Políticas\Políticas*]	
Model: 012021	Approved by: Gustavo Comanduci
Issued on: 03/12/2021	Edited by: Cristiano Diniz

1. Purpose

1.1. This policy aims to establish the guidelines and standards for information security and protection of personal data of WBR Consultoria (SIGGA), supported by a strategic decision by the company's executive board and developed within the scope of a standardized Information Security Management System (ISMS). In particular, it seeks to:

a. ensure the adoption of rules and procedures that allow SIGGA employees and other interested parties to follow safe behavior standards, protective of the company's sensitive information and in compliance with the applicable legislation, as defined in item 2.4 below;

b. observe the three (3) pillars of information security (confidentiality, integrity, availability) to better meet the needs of SIGGA's customers and employees and to ensure that the company's image in the market is maintained and consolidated as an image of a high quality products and services supplier;

c. prevent security incidents such as unauthorized access, loss, destruction, disclosure and/or unauthorized modification of data, as well as protect information against a wide range of threats.

1.2. This policy applies to (i) all personal data that SIGGA eventually handles in relation to the identified or identifiable natural person; as well as (ii) all sensitive information of the company and its customers, as defined below.

2. Terms and Definitions

2.1. Personal Data. Personal data means all information related to an identified or identifiable natural person.

2.2. Sensitive Information. Sensitive information means any data that has any value for the operation of SIGGA, regardless of the format and storage mean.

2.3. Information. Sensitive Information and Personal Data means Information, when taken together and generically.

2.4. Applicable Law. Applicable legislation meansthe laws that regulate aspects of

intellectual property and deal with data protection, including LGPD (General Data Protection Law), GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act).

2.5. For the purposes of this Policy, the other terms and definitions contained in the Information Security Management System manual shall apply.

3. Applicability

3.1. This Policy is applicable to all SIGGA employees, associated companies and/or affiliates, joint ventures and/or any third parties that have or will have a relationship with the company.

3.1.1. The executive board of SIGGA, together with the managers responsible for information security, is committed to the effective management and the application of the policies defined in the ISMS, in order to excel in the security of the organization and the guidelines established herein.

3.1.2. It is the responsibility of all employees to know and respect the ISMS policy, being involved in issues related to safety and acting actively so that their skills are used for the continuous improvement of the ISMS.

3.1.3. The continuous improvement of the procedures and processes established in the ISMS is a joint responsibility of the SIGGA management, the representatives of the execute board and the information security team. The procedures and processes must be regularly revisited and improved, ensuring the effectiveness of the policy established in the ISMS.

3.1.4. Sigga shall observe this policy in any circumstances, including in external relationships with customers, suppliers and/or any other interested parties.

3.1.5. In the case of external relationships in which the other party does not have an information security policy, or where the respective policy does not guarantee the same levels of security as the present one, a representative of the management, together with the information security team, shall assess whether there is any risk to the safety of SIGGA.

4. Guidelines

4.1. Information assets. The assets associated with the Information and the information processing resources are duly identified and inventoried.

4.1.1. An owner is defined for each Information asset, who shall be responsible for ensuring that it is used in accordance with this Policy.

4.1.2. Only software approved and published by the IT area may be used in assets controlled by the ISMS.

4.1.3. The guidelines for the proper use of assets are informed during the process of hiring people. Specific assets have a professional responsible for handling manipulation, ensuring proper use.

4.1.4. The sharing of corporate data processed by Information assets is not allowed without the prior and specific authorization of the responsible manager.

4.2. Access Control. Access control is one of the mechanisms used to physically and logically protect the environment with SIGGA Information. Access to information assets shall only be allowed to authorized persons, under the terms of this Policy.

4.2.1. The right to use the assets is controlled and assigned at the time of hiring, during the employee's professional relationship with the company, terminated at the end of the relationship with SIGGA when the physical assets are collected.

4.2.2. If the contractor has the need to access a specific corporate system, it shall be provided by means of an authorization from the information manager involved.

4.3. Physical Access Control.

4.3.1. Collaborators Admission. Access to information, equipment, documents and secure areas is duly controlled so that only authorized persons have access to these resources.

a. The identification of employees to access SIGGA's facilities is controlled by a security device that guarantees access only to authorized personnel. Restricted environments are controlled by security devices and access is only allowed with the authorization of the person in charge.

b. Dismissed collaborators may only enter Sigga's premises if they are duly accompanied by a responsible collaborator.

4.3.2. Visitors Admission. The entry and attendance of visitors is only allowed during business hours, with the accompanied by a responsible employee. The visitor must go through the security procedures carried out by the condominium's concierge and, at the end of the visit, he/she must be accompanied until he/she leaves the company's facilities. During the entire period that the visitor is at the SIGGA facilities, he/she must be in the field of vision of any employee of the company, except in the case of private places, such as toilets.

4.3.3. Supplier Admission. The access of suppliers to SIGGA shall happen upon request of service to the supplier and with the due authorization of a responsible person of the company. The supplier shall carry identification capable of certifying that he/she is the person hired for the service, as well as being accompanied by a SIGGA employee.

4.3.4. Delivery and Loading Areas. SIGGA has access points for deliveries and shipments that are located on the building's docks and the anteroom of our facility. Orders shall be received and delivered at one of these two points, except when the volume, weight, or other factor makes the operation unfeasible. In this case, the person responsible for delivery/loading shall be identified and accompanied by a SIGGA employee during the entire time that he/she is in our facilities.

4.3.5. Clean Table. All employees must undertake not to leave any confidential information in sight, whether on paper and/or annotated in a visible or accessible place. Special attention shall also be provided when using collective printers, collecting the printed document immediately after printing.

4.4. Logical Access Control.

4.4.1. Accesses in the Hiring Process. During the hiring process, employees shall receive the appropriate release of logical access to the information assets necessary for their activities.

a. The employee shall receive access to the information assets, such as network and systems, and must be responsible for the confidentiality of the information received. No employee shall be allowed to provide his password to other employees.

b. Specific accesses not included in the contracting process shall be dealt with directly with the person responsible for the Information asset.

4.4.2. Cancellation of Access. The employee termination process removes access rights to the various Information assets.

4.4.3. Internet Access. SIGGA provides access to the Internet to employees and visitors, and access to visitors is made through a specific network and separate from our corporate network.

a. The Internet made available by SIGGA to its employees, regardless of their contractual relationship, can be used for personal purposes, as long as such use does not cause risks to the company's image, reputation and infrastructure.

b. Sigga reserves the right to restrict access to sites that may put the company at risk.

c. Disclosure of SIGGA's confidential information in any discussion groups, lists or chats is prohibited.

4.4.4. Access to E-mail. All e-mail users are able to send and receive external messages.

a. The default for creating institutional e-mail is name.surname@sigga.com. In exceptional cases, of duplicity or that cause embarrassment to users, the standard shall be revised.

b. The e-mail account is made available exclusively for institutional use, and is not admitted for personal use.

4.4.5. Access to Source Code. Access to the source code of programs and associated items (such as drawings, specifications, verification and validation plans) is restricted to professionals involved in the process of developing and deploying systems.

a. All products generated during the systems development lifecycle must be stored in repositories subject to access control mechanisms, ensuring that only authorized employees have access.

b. The source codes of SIGGA's proprietary Information systems must be properly maintained, including versioning control, and protection against access or undue changes.

4.4.6. Removal or Adjustment of Admissions. The release of access to systems, directories, access groups or administrative profiles offered to users needs to be reviewed, in order to ensure that the accesses are compatible with the position, the area of operation and the functions performed.

a. The following must be submitted to a periodic review process: (i) access granted to systems and applications; and (ii) accesses granted to IT infrastructure.

b. The review of access to systems must be made according to the classification of the information contained in each system, or another criterion established by the executive board.

c. The review process must be carried out each time the employee undergoes a change of position or function or in a critical analysis to be carried out annually by the information security team.

4.4.7. Privileged Access. Credentials for privileged access to systems or physical assets must be granted upon the approval of the manager based on the role and the need for the development of work activities.

a. Sharing the use of privileged access credentials shall be prohibited. However, if there is a need for sharing due to technical issues, these must be authorized by the manager with formalization of the reason why the password is being requested and changing the password as soon as the cause of the request is addressed.

b. All users with privileged access IDs must also have access IDs for non-privileged activities, so that the use of access occurs when it is strictly necessary.

4.4.8. Use of Privileged Utility Programs. The use of utility programs that may be able to override system and application controls are restricted to IT staff and shall be used only to assist in the administration of Sigga's data network environment.

4.4.9. Secure Access to Systems and Password Management. The logon procedure must disclose only the Information necessary for the activities of a given employee, avoiding providing an unauthorized user with improper Information.

a. Help messages in the logon process shall not contain hints that may allow an unauthorized user to access the system.

b. Every user must have a unique, personal and non-transferable identification.

c. The holder assumes responsibility for the confidentiality of his/her personal password, and is responsible for any action taken with his/her login/password

d. Sharing, disclosure to third parties, paper notes of personal identification, or the entry of a password in a visible place and/or that can be accessed by another person, is not allowed

e. We encourage the use of strong passwords, we suggest that the password has at least the following formation: (i) eight (8) or more characters; and (ii) inclusion of upper and lower case letters, numbers and special characters.

f. It is not allowed to use weak passwords, such as based on proper names, personal data such as name, date of birth, document numbers, among others.

g. The passwords of the company's systems must be changed whenever there is any indication of possible compromise of the system or the password itself. We encourage passwords not to be reused.

h. The collaborator, when receiving a password created by a third party, must change it on his first access to a secure password, as suggested above.

4.4.10. Remote Access. The remote acess to infrastructure is made available only for specific cases and performed through a secure connection and protected by password. The information accessed remotely must be protected by means of software that contributes to the security of stored data and traffic of

Information.

4.4.11. Clean Screen. Employees, when applicable, must block all equipment, workstations and servers in any temporary absence, avoiding the misuse of the equipment.

4.4.12. Use of Mobile Devices. We do not allow access from personal mobile devices to the corporate network, so that all our employees' mobile devices are allowed access only to the guest network.

a. Personal mobile assets are not registered as SIGGA information security assets.

b. Personal mobile devices used by SIGGA employees for work activities must be protected by password or visual identification.

c. It is not permitted for the working document to be stored on a personal mobile device unless it is within the proper repository of a tool licensed by SIGGA.

d. Users of Corporate Information on personal mobile devices undertake to delete all Information upon request. It is forbidden to share information without the authorization of the responsible manager at the board level.

e. SIGGA's mobile assets are registered as information assets and follow all the requirements of this Policy.

4.4.13. Communications Security.The use of Information Systems is prohibited in order to carry out actions that are against national and international legislation and standards that may cause damage to the network or other systems, impairing network traffic or access to resources.

4.5. Security with Suppliers. Agreements with third parties, partners and suppliers are established and documented so that there are no disagreements between the parties, regarding their obligation to the applicable security requirements.

4.6. Security with Clients. In the case of visiting customers where safety standards are set for access to secure areas, it is mandatory that the SIGGA employees participate in all available safety training and follow all the guidelines ensuring their physical integrity.

4.7. Legal Compliance. SIGGA is committed to observing all the Applicable Law.

4.7.1. Adequacy to Applicable Legislation. SIGGA undertakes to observe the Applicable Law, the guidelines to be issued by the National Data Protection Agency ("ANPD") and to adopt all possible and necessary technical and organizational security measures for the protection of the processed Personal Data, including, without among others:

a. adopt security, technical and administrative measures capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication or any form of improper or illicit treatment;

b. adopt the minimum technical standards determined by the national authority to make the provisions of the previous item applicable, considering the nature of the information processed, the specific characteristics of the treatment and the current state of technology, especially in the case of sensitive personal data;

c. control and restrict the processing of data to the professionals necessary for the respective activities, who must be instructed on the appropriate form of treatment;

d. observe all the principles for the processing of data provided in the applicable legislation, respecting the rights of data subjects.

4.7.2. Intellectual Property. The lawful use of software is also ensured, always with its official and authorized licenses so as not to infringe intellectual and copyright rights of manufacturers and their representatives.

4.8. Information Security Incident Management. The guidelines for the management of Information Security incidents are established in a specific document, ensuring a consistent and effective approach to incident management, ensuring that weaknesses and information security incidents are detected, recorded, investigated and, whenever possible, prevented.

4.9. Business Continuity Management. SIGGA has established procedures for the recovery of services and critical processes in order to ensure that its activities considered essential continue to be performed and that critical services are available

to the user, in situations of crisis or unscheduled outages.

5. Responsibilities

5.1. Collaborators The following are the obligations attributable to every employee of the company:

a. Know and fully comply with the terms of the General Information Security Policy, as well as the other applicable security rules and procedures;

b. Report incidents, suspicions of security incidents or any doubts or requests to the Information Security Management System Team - ISMS;

c. Respond for non-compliance with the Information Security Policy and other security rules and procedures, as defined in the sanctions provided in this policy;

d. Ensure the security of Information and that all activities involving the processing of Personal Data are carried out in a safe and appropriate manner, in compliance with company policies and Applicable Laws.

5.2. In addition to the general obligations set forth above, the following responsibilities are provided:

5.2.1. Managers:

a. Be a multiplying agent, informing, encouraging and making employees aware of complying with the Information Security Policy;

b. Identify, classify and label the information generated under the responsibility of your business area, making adjustments as necessary;

c. Ensure that, at the time of hiring, employees or service providers are familiar with and accept the Information Security Policy.

5.2.2. Information Security Management System Team:

a. Maintain and improve the Information Security system;

b. Review and update the documents that make up the Information Security Policy;

c. Promote awareness and guide employees in relation to the Information Security Policy;

d. Encourage Information Security activities to be carried out in accordance with this policy;

e. Assess Information Security incidents and communicate the result to managers, if necessary.

5.2.3. Human Resources Area: ensure, at the time of hiring, that the process related to Information Security is executed.

6. Sanctions.

6.1. Violations of the rules that make up this Policy, both by employees and third parties, as well as other safety rules and procedures, must be reported immediately to the immediate manager, human resources and the ISMS.

6.2. Violations are liable to administrative penalties, including with regard to communication to the competent public authorities, if applicable.

7. Omissions

7.1. Omissions shall be analyzed by the ISMS Team, who will deliberate on each specific case and take the appropriate measures.

7.2. The guidelines established in this Policy and in the other security rules of SIGGA, not limited to this content, expect that all parties involved, whenever possible, shall associate measures that guarantee Information Security in all company activities.

8. References

- ISMS Manual;
- NBR ISO/IEC 27001 - Information Security Management System
- NBR ISO/IEC 27002 - Code of practice for information security management