SUMMARY

1. INTRODUCTION 2
2. SCOPE 2
3. DEFINITIONS 2
4. RESPONSIBILITIES 3
4.1. Supplier services contracting area 3
4.2. Partners 3
5. GUIDELINES 3
5.1. General 3
6. INFORMATION SECURITY REQUIREMENTS 4
6.1. CONDUCT OF PARTNERS IN THE WEG GROUP 4
6.1.1. Logical Access and Acceptable Use 4
6.1.2. Information Security Incident Notification 4
6.1.3. Equipment safety 5
6.1.4. Breach of Conduct 5
6.2. PARTNER SECURITY AND PRIVACY CONTROLS 6
6.2.1. Privacy 6
6.2.2. Access control 6
6.2.3. Monitoring of services and management of information security operation 7
6.2.4. Threat Management 7
6.2.5. Security in system development 8
6.2.6. Business continuity, data management, retention and storage. 8
6.2.7. Training and awareness 8
6.2.8. Services and certifications 9
7. PERIODIC EVALUATIONS 9
8. SANCTIONS 9

1. INTRODUCTION

The main objective of this Information Security Policy for Partners is to direct an effective program for the protection of information assets, with a view to ensuring the confidentiality, integrity and availability of information, being the basis for the establishment of Information Security standards and procedures in the WEG Group.

2. SCOPE

All Partners (any person who has a legal relationship with the WEG Group as a supplier of products, licenses or services) must comply with the Information Security requirements defined herein.

Compliance with the established guidelines is essential for the effective partnership relationship signed and the achievement of adequate levels of information protection.

The guidelines and requirements established herein apply to all Partners who have access to WEG Group data, information and systems. Partners will be responsible for themselves and their employees, suppliers and service providers.

3. DEFINITIONS

- **DPIA**: is the acronym for Data Protection Impact Assessment, which stands for Personal Data Protection Impact Report (RIPD) in the Brazilian General Data Protection Law (LGPD). This process identifies, evaluates, and mitigates privacy risks in data projects before they are implemented. It is a legal and mandatory responsibility when data processing may put the rights and freedoms of data subjects at risk.
- **Opt-in:** it is a term in English that means the authorization of a user to receive information from a company.
- **Opt-out:** it is a term that means "choosing to leave", it is a movement in which the individual has the autonomy to stop being part of something that is inserted.
- **Segregation of Duties (SOD):** SOD is the acronym for *Segregation of Duties*, it is an internal control principle that aims to avoid risks, such as fraud, errors, and cyber attacks, in organizations. Segregation of Duties is based on the delegation of tasks between different people or groups, in order to prevent the same person from having full control over systems, processes, or confidential activities.
- **Least privilege policy:** This is a cybersecurity concept that consists of giving users only the least privileges necessary to perform their duties.
- **Runbooks:** detailed guides that outline an organization's procedures and processes, with the goal of ensuring that activities are performed consistently, safely, and efficiently.
- **Hardening:** a process that aims to strengthen the security of systems, networks, software, hardware, firmware, and IT infrastructures, making them more resistant to cyberattacks.
- **Security patches:** corrective updates that aim to fix vulnerabilities, flaws, and bugs in software and platforms.
- **OWASP:** Open Worldwide Application Security Project (OWASP) is an international non-profit organization that works to improve the security of web and mobile applications. OWASP is one of the leading initiatives to combat cybercrime.
- **Privacy and Security by Design:** concepts that refer to data protection and system security proactively, from the conception of a project or service.

- **Phishing:** a type of cyberattack that aims to steal personal information or access online accounts. Scammers use fraudulent messages that appear legitimate to trick victims into revealing sensitive data.
- **Ethical hacking:** Ethical hacking or ethical hacking, is a digital security practice that consists of simulating a cyberattack to identify and correct vulnerabilities in systems, networks, or applications.
- **Penetration testing:** Penetration testing (or pentesting) is an authorized simulated attack that organizations make on their own computer systems or networks to assess their security. The goal is to discover vulnerabilities using the same tools, techniques, and processes that hackers use. By exposing cybersecurity weaknesses, pen tests help reduce the risks of malicious cyberattacks.

4. RESPONSIBILITIES

4.1. Supplier services contracting area

- During the process of hiring Partners (including employees, suppliers and service providers linked to the Partner) who need to access the internal network, systems, information or data of the WEG Group, the contracting area must ensure that all those involved are aware of this information security policy.
- The contracting area must ensure that contracts with Partners include specific clauses on information security and data protection, including with express reference to this Information Security Policy.

4.2. Partners

- It is the responsibility of the Partners to observe and follow the guidelines set forth in this Information Security Policy; and
- The activities performed must comply with the legislation in force and the standardization of regulatory bodies and entities in relation to Information Security applicable to the object of the contract.

5. GUIDELINES

5.1. General

Partners, whether they are suppliers of products, licenses, or services, must commit to fully comply with the following:

- Protect the information from unauthorized access, modification, destruction or disclosure while maintaining its confidentiality.
- Ensure that the resources made available to them are used only for the purposes approved by the WEG Group.
- Ensure that the systems and information under its responsibility are adequately protected in accordance with the WEG Group's standards.
- Ensure continuity of processing of critical business information.
- Comply with the laws and standards that regulate intellectual property aspects.
- Implement and maintain information security controls, in accordance with the best market practices and applicable regulations.
- Immediately report to the WEG Group any non-compliance with the Information Security Policy for Partners, by themselves or by other people, whether or not they are linked to the Partner.

- Comply with the WEG Group's General Conditions for the Purchase of Goods, Materials and/or Services ("GCC") – available at: https://www.weg.net/ -> This is WEG -> GENERAL PURCHASING CONDITIONS FOR SUPPLIERS – and the WEG Group's Code of Ethics for Suppliers ("Code of Ethics") – available at: https://www.weg.net/ -> This is WEG -> CODE OF ETHICS FOR SUPPLIERS. The Partner must strictly comply with the parameters applicable to it on data protection and privacy established in any applicable legislation, as well as follow the best market practices on the subject.
- Partners who carry out critical activities on behalf of the WEG Group must undergo an Information Security ("IS") assessment process. In the IS evaluation process, an IS Self Assessment will be carried out during the supplier qualification and contract negotiation phases. Depending on the result of the Self Assessment, the WEG Group may request additional procedures to verify the Partner's adequacy to the IS parameters established in this Information Security Policy for Partners.

6. INFORMATION SECURITY REQUIREMENTS

6.1. CONDUCT OF PARTNERS IN THE WEG GROUP ENVIRONMENT

6.1.1. Logical Access and Acceptable Use

- For Partners who need to access the WEG Group environment remotely, the WEG manager responsible for the contract must provide access through a single and individual user, in which they can only have access to the work resources and environments necessary for the performance of their functions.
- Partners' computers cannot be connected to the WEG Group's internal network without the prior approval of the area responsible for information security, the software of the Partners' equipment must be duly licensed.
- It is forbidden to access, download or distribute any content that violates copyright or property of the WEG Group. Likewise, access to or distribution of illegal, pornographic content of any nature or that violates the Statute of the Child and Adolescent is not allowed.
- The access credentials made available to the partner are for exclusive use only and may not be disclosed or shared with others.
- The partner must keep its access credentials secure, and it is its sole and exclusive responsibility for any use made with its access credentials, including any misuse.
- It is the Partner's responsibility to communicate any dismissal of its employees, suppliers or service providers.

6.1.2. Information Security Incident Notification

Partner shall, when it discovers an incident or reasonably suspects that an incident is occurring or has occurred:

- Immediately initiate incident handling to investigate, promptly contain, and protect any IT systems and company data at risk, minimize and mitigate the impact of the incident on IT systems.
- Immediately notify the WEG Group by e-mail soc@weg.net.

Partner must notify the incident including the following information:

- The nature and suspected scope of the incident.
- The suspicious date on which the incident began.
- The date and time of discovery of the incident.

- Actions taken by Partner to ensure continued provision of scope and to protect and recover company data, where relevant; and
- Contact details of a Partner representative to respond to WEG Group's requests for such information.

The Partner must provide the WEG Group with the following information as soon as possible:

- the suspected cause(s) of the incident and the actor(s) involved.
- The estimated impact of the incident.
- Proposed corrective actions and estimated time for full recovery from the impact of the incident; and
- Proposed corrective actions, including to ensure continued provision of scope and to protect and retrieve company data where relevant.

The Partner shall provide the WEG Group with regular updates of the information provided pursuant to the preceding paragraphs, together with any other information that the WEG Group may reasonably request in connection with the incident (including records of all access to the relevant IT systems in connection with the incident and evidence to demonstrate the effective protection and recovery of the company's data).

The Partner shall immediately provide the WEG Group with all assistance that the WEG Group may need to enable it to investigate, respond to, mitigate the impact and correct incidents (including the protection and recovery of company data) and to communicate and respond to individuals or public authorities, including the relevant regulatory authorities.

The Partner shall provide the WEG Group with a final report of the incident, including a root cause analysis, as soon as it is available.

Notwithstanding anything to the contrary in the contract, an incident shall not be considered a force majeure event to the extent that it has been contributed by any breach of this annex or negligence of a member of the Partner.

6.1.3. Equipment safety

- Each Partner is responsible for the protection of the physical devices containing WEG Group information that are in its custody; and
- Partners are aware that access to any WEG Group environment or the use of any IT resource in the WEG Group environment, even in situations where the partner uses personally owned equipment, are subject to monitoring and inspection, except in situations where the applicable local law expressly prohibits such conduct.

6.1.4. Breach of Conduct

The following situations are considered violations of this Information Security Policy for Partners, not limited to:

- Any actions, omissions or other situations that may expose the WEG Group to financial or image loss, directly or indirectly, potential or actual, compromising its information assets.
- Misuse or disclosure of any information without the express permission of the WEG Group, such as: corporate data, trade secrets or other information.
- The commissive or omissive non-compliance with any guideline, rule, parameter or obligation established in this Information Security Policy for Partners.

- Use of data, information, equipment, software, systems or other technological resources, for illicit purposes, which may include the violation of laws, internal and external regulations, ethics or requirements of regulatory bodies in the area of operation of the WEG Group; and
- Failure to immediately communicate to the WEG Group any Information Security incidents or non-compliance with this Information Security Policy for Partners.

6.2. SECURITY AND PRIVACY CONTROLS IN THE PARTNER ENVIRONMENT

Upon being requested by the WEG Group's business area, the Partner in question will be registered by the Information Security Governance team in a tool to verify its cyber-health. This platform provides scoring scores. The Partner's overall score must reach at least 80% or the average score of its market segment provided by the tool itself, whichever is higher.

Partners who do not reach the desired score will receive an adequacy and compliance report from the WEG Group so that the Partner can take measures to achieve the desired score within 180 days.

In addition to the registration procedure described above, the Partner must follow the following information security guidelines, also provided for in the Self Assessment document sent and maintained by the Information Security area.

6.2.1. Privacy

- Present through documentation the flow of WEG data in the Partner's environment, containing its entire life cycle (collection, processing, storage, sharing and deletion).
- Inform the WEG Group what information is collected, for what purpose, what is the legal basis for processing the data, where it is stored and for how long, always seeking to minimize the storage period and the amount of information collected.
- Have an impact assessment related to a holder's personal data (DPIA), as well as have a process that grants WEG Group unrestricted access to their processed and stored information, provided for in the scope of the contract.
- Have an *opt-in* and *opt-out process* for prior and free expression of the WEG Group and the holders of personal data about the sharing through a partnership. It is also noteworthy that the default should be non-sharing. Only after the interested party's *opt-in* will the Partner be able to share data with partners.

6.2.2. Access control

- Have a properly documented Access Management process.
- To give the WEG Group unrestricted access to the data and information stored or to be processed, according to the specific services defined, valuing the confidentiality, integrity, availability and recoverability of this data and information.
- To give visibility to the WEG Group of the procedures and controls used to comply with the contract, as described in the item above, in particular, for the identification and segregation of WEG Group's customer data, through physical or logical controls.
- Not allowing the use of shared accounts or generic users for critical systems, as well as maintaining controls related to login, such as (but not limited to): forcing changes on first access, blocking the user

after a number of certain invalid attempts, requiring complex password patterns and other information security practices in accordance with the best market standards.

- Have a formalized and documented process for granting, changing and revoking access, especially those with privileged shares.
- Have a process for controlling the absence of segregation of function (SOD).
- Adopt a policy of least privilege.
- Have methods for physical and logical access control of visitors; and
- Have remote access controls for employees/service providers during *teleworking* periods.

6.2.3. Monitoring of services and management of information security operation

- Ensure that it has the highest level of capacity in providing information and adequate management resources to monitor the services to be provided, as well as ensuring compliance with the legislation and regulations in force.
- Inform and give access to the WEG Group, when requested, on the appropriate management resources for monitoring the contracted services.
- Have resources and tools for monitoring the capacity and availability of your assets, correlating alerts and generating incident tickets in an automated way.
- Have a structured Incident Response process, including the categorization of incidents and *runbooks* for handling and resolving known incidents.
- Prevent, detect and reduce incidents related to the cyber environment, evidencing procedures and controls that cover, at least, authentication, encryption, intrusion prevention and detection, data leakage prevention, periodic tests and scans to detect vulnerabilities, application of security *patches*, application of *hardening* on its servers and workstations, protection against malicious software and blocking of non-approved software, the establishment of traceability and segmentation mechanisms for the computer network, the maintenance of data and information security copies.
- WEG reserves the right to immediately and unilaterally revoke any access in the event of a security incident or abnormal/inappropriate behavior in the WEG environment involving the Partner, whether confirmed, under suspicion or under investigation.
- Provide, when requested, information related to the number of incidents that occurred in the last 24 months, classifying them by their relevance. All data on incidents of "medium", "high" or "very high" severity must be stored by the Partner for at least 5 years; and
- Keep the WEG Group permanently informed of any limitations that may affect the provision of services or compliance with the legislation and regulations in force.

6.2.4. Threat Management

Partner shall ensure that vulnerabilities in IT systems are patched or updated in a timely manner. In any event, the Partner shall:

a) Within 24 hours of the discovery of any critical vulnerability (CVSS or CVE 9.0 or higher) in the relevant IT systems of the contracting group that is not provided by a third party:

- Begin the process of developing and deploying an update or patch to fix the vulnerability.

- Notify the WEG Group in soc@weg.net and provide details about the vulnerability and related threat, and what measures the Partner has implemented to mitigate the threat or vulnerability.
- Ensure that all relevant Partner IT systems have the latest third-party provided patches installed and deployed; and
- Install and deploy updates or patches for vulnerabilities included in the U.S. Cyber & Infrastructure Security Agency's catalog of known exploited vulnerabilities within 24 hours of the release of the update or patch. If any update or patch cannot be applied for any reason within 24 hours, the Partner must immediately notify the WEG Group within soc@weg.net.

b) The Partner shall:

- Ensure that relevant IT systems are continuously monitored to ensure their security, authenticity, confidentiality, integrity, and availability; and
- Continuously generate the relevant IT system logs necessary to: (A) enable incident response; (B) identify the source of an incident; and (C) recreate the sequence of events leading up to an incident. Partner must securely maintain these records for at least 180 days from the date of generation so that these records can only be accessed by authorized users.

6.2.5. Security in system development

- Adopt *Privacy and Security by Design* practices in your software development processes.
- Describe the security features and data accessed by the applications, which must be evaluated by the Information Security area during the approval phase (Ex: Technical Specification and/or Functional Diagram).
- Use integrity validation routines to prevent errors, whether involuntary or intentional, using fictitious data or anonymizations in a non-productive environment.
- Adopt security analysis practices in the source code.
- Adopt security analysis practices in their applications (Ethical Hacking Tests and penetration tests).
- Provide for security validations in the code quality and verification process. At a minimum, those that appear in the OWASP TOP 10 should be considered.

6.2.6. Business continuity, data management, retention and storage.

- Define a business continuity program to ensure that possible incidents do not affect the services provided to the WEG Group, especially contemplating the disaster recovery plan, regularly testing the assurance controls in order to verify how prepared the company is for real cases.
- Inform and give access to the WEG Group, when requested, about the security measures for the transmission and storage of data and information, as well as its disposal, using secure exclusion procedures (digital and/or physical).
- Have a backup execution process that is carried out periodically on the assets that store WEG Group information, in order to avoid or minimize data loss in the event of incidents.

6.2.7. Training and awareness

- Ensure the existence of a training and awareness program in Information Security and Data Privacy, with a minimum annual periodicity, for all its employees, suppliers and service providers, and the training must

be contemplated with the mandatory application of the Partner Code of Conduct for newly hired employees, suppliers and service providers.

- Include in its Information Security and Data Privacy training and awareness program campaigns to prevent *phishing* and guidance on social engineering, as well as lectures, the issuance of IS and Data Privacy newsletters, etc.
- Partners' employees, suppliers or service providers who have access to or process personal data and/or sensitive information must be aware of this Policy and of what it concerns information security training from.

6.2.8. Services and certifications

The Partner shall:

- Notify, in advance and formally, the subcontracting of services relevant to the object of the contract with the WEG Group.
- Have information security or business continuity recognitions, proven by independent external audit reports.
- Inform and give access to the WEG Group, when requested, about the certifications necessary for the provision of services, as well as the reports related to the controls used in the provision of the contracted services, prepared by a specialized independent auditing firm; and
- Have mechanisms to communicate anomalies or security incidents to the WEG Group, the Individuals involved and the National Data Protection Authority.

7. PERIODIC EVALUATIONS

The WEG Group may carry out, whenever it deems necessary, evaluations to attest to the effectiveness of the implementation of the controls presented in this document, and for this purpose, it must notify the partner 30 days in advance. Evaluations may also occur in the event of a security incident or change in the market conditions applicable to the Partner's or WEG Group's segment.

8. SANCTIONS

Violation of a control or non-adherence to the Information Security Policy for Partners and its definitions are considered serious faults or violations, and applicable penalties or sanctions may be applied in accordance with the WEG Group's internal policies and/or provided for in the contract.

In case of violation of any obligation or provision of this Policy by the Partner, its employees, suppliers, service providers and/or any persons related to the Partner, the Partner undertakes to indemnify, hold harmless, defend and hold harmless the WEG Group from any and all losses or damages, without prejudice to other penalties, sanctions and/or penalties provided for in the contract or by law.

The Partner acknowledges and agrees that mere indemnification may not be the appropriate way to remedy any violations of this Policy, and the WEG Group may use any form and/or means of specific execution of obligations that may be applicable in the event of a threat or effective violation of this Partnership.