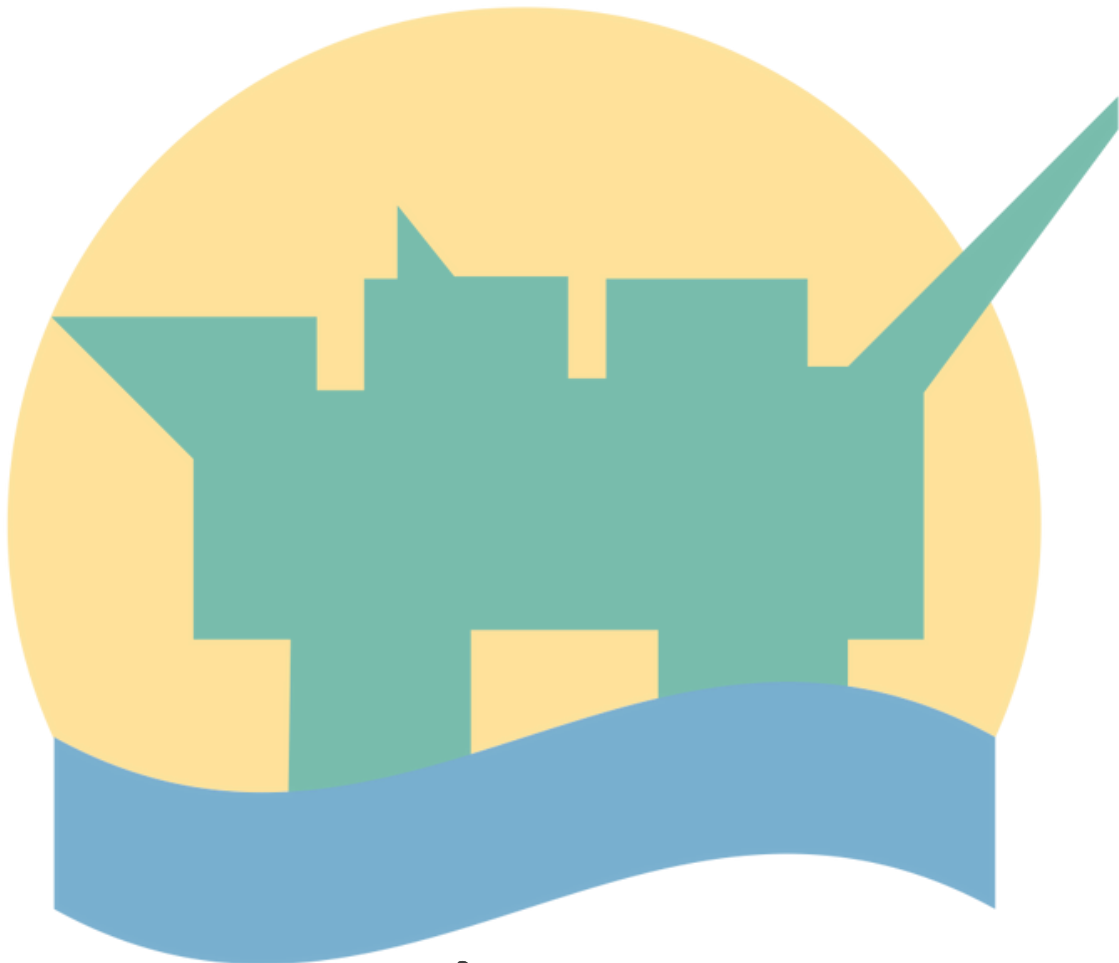
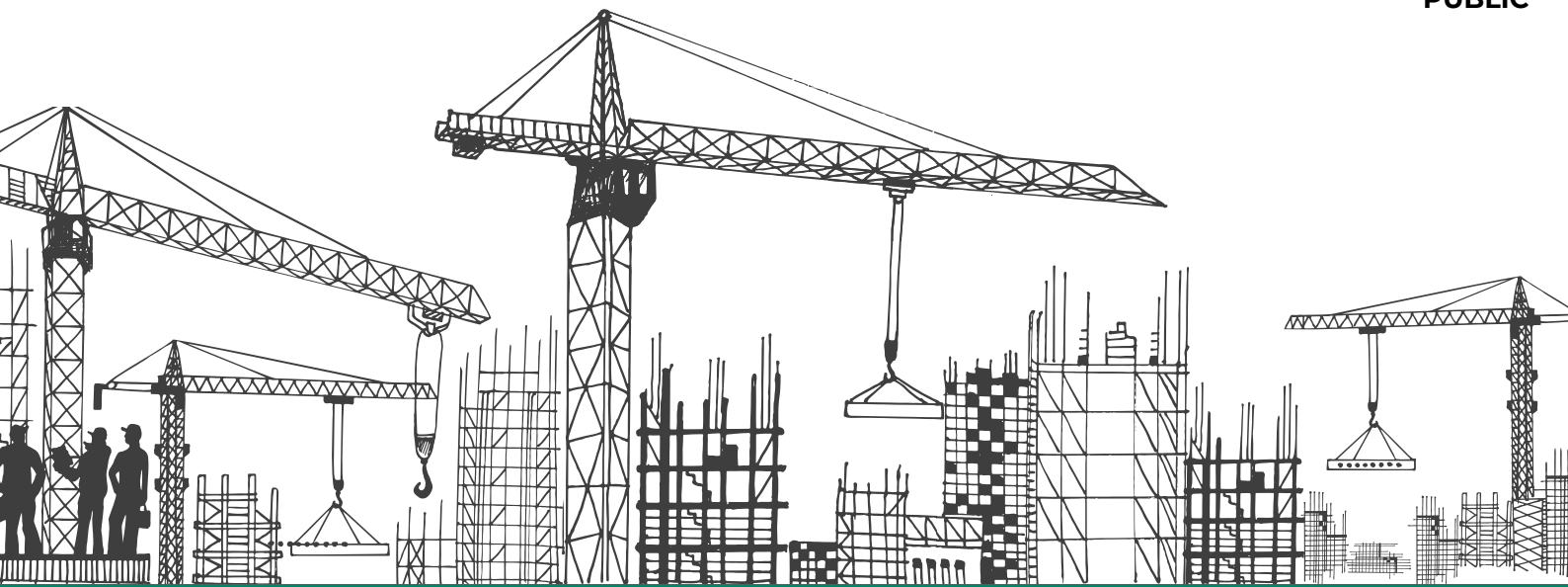


Guidance on **Information Security and Privacy and Data Protection**





Dear Supplier,

This Guidance aims to present the Information Security and Privacy and Data Protection guidelines that govern the relationship between Estaleiros do Brasil LTDA. (EBR) and its suppliers, fostering healthy, sustainable, and transparent partnerships.

Our organization maintains a corporate policy in compliance with applicable national and international laws, regulations, and standards. This document must be acknowledged and adhered to by all our suppliers in every location where the organization operates.

By accepting this guidance, our suppliers must ensure the protection of personal data and the security of information handled in the commercial relationship. They acknowledge that all agreements, contracts, and business relationships with EBR will be subject to the provisions of this document and the application of disciplinary measures.

EBR suppliers must comply with the following principles:

01

Compliance with Legislation

Suppliers must fully comply with the current personal data protection legislation, including the General Data Protection Law (Law No. 13.709/2018 – “Lei Geral de Proteção de Dados”) and any applicable international regulations. They must also adhere to EBR's contractual clauses, especially regarding the response to cyber incidents.

02

Best Practices in Information Security

Suppliers must ensure that their products, services, and processes comply with the best information security practices, particularly ISO 27001 and other relevant standards. They must maintain proactive measures to prevent, identify, and mitigate potential technological risks that could negatively impact EBR and its security. Additionally, they must guarantee the confidentiality, integrity, and availability (CIA) of the information handled in the fulfillment of their contract.

03

Risk and Incident Management

It is the responsibility of suppliers to control and mitigate technological and cybersecurity risks associated with the services provided to EBR, whether the activity is remote, on-premises, cloud-based, or in person, adopting preventive measures to protect EBR from technological impacts.

In the event of security incidents and privacy and data protection breaches, suppliers must immediately inform EBR and take all necessary corrective actions in accordance with the established incident response protocols of the company and the General Data Protection Law.

04

Transparency and Information Classification

Suppliers must ensure that all classified information (confidential, protected, public, etc.) is handled appropriately, preventing any unauthorized disclosure and/or leakage.

05

Privacy and Personal Data Protection

Suppliers commit to adopting robust practices to ensure the privacy and protection of personal data processed on EBR. When acting as processors or co-controllers, they must strictly follow the instructions of EBR, the data protection officer, and implement appropriate technical and organizational measures to protect this data from unauthorized access, leaks, etc. They must also be prepared to assist EBR in the relationship with data subjects, such as the right to access, correction, deletion, etc.

06

Evidence and Compliance

EBR may request evidence that suppliers are implementing the necessary security measures through audits or requests for compliance reports. Suppliers must be prepared to demonstrate their compliance with information security and privacy requirements, including the implementation of appropriate technical, administrative, and physical controls. They should also conduct periodic internal audits to ensure that security controls are being followed and provide audit reports when requested.

07

Third-Party and Subcontractor Management

Suppliers are responsible for ensuring that any third parties or subcontractors handling EBR's information on their behalf also comply with information security, privacy, and data protection standards. Suppliers must monitor their subcontractors, ensuring that all of them follow the guidelines established by EBR.

08

Personal Data and Information Retention Period

Suppliers must ensure that personal data is retained only for the period necessary to fulfill the purposes agreed with EBR, in accordance with the instructions provided by the data protection officer. They must comply with legal data retention periods and follow best practices for secure disposal.

09

Disciplinary Measures and Contract Termination

EBR reserves the right to monitor its suppliers and conduct audits to ensure and verify the effectiveness and accuracy of the processes and controls outlined in this Guidance. EBR may also request corrective actions when necessary.

Non-compliance with the provisions established in this Guidance will result in the adoption of disciplinary measures, ranging from the termination of existing contracts to the blocking and de-registration of the supplier for future business transactions.

Adherence to this Guidance is essential to qualify as a supplier for EBR.



www.ebrbrasil.com