SECURITY INFORMATION GUIDELINES FOR SUPPLIERS

SUMMARY

1. Objectives

The guideline of this Information Security Policy is to define the rules and principles to be adopted by COOXUPÉ'S suppliers to guarantee the protection of the information made available by COOXUPÉ, including personal data and sensitive personal data.

It takes into account the security of suppliers' information systems and their infrastructures that are related to the services provided to COOXUPÉ and, if necessary, a questionnaire will be sent about the supplier's information environment and security.

2. Definitions

The classification of this document is considered "public" and should be shared with COOXUPÉ'S suppliers and service providers.

Related Documents
SECURITY AND PRIVACY PROCEDURE FOR PRODUCT AND SERVICE SUPPLIERS

3. Compliance

This guideline is subject to updating every six months or every year, depending on the need for internal adjustments at COOXUPÉ. It is up to the supplier to access the website www.cooxupe.com.br (*Governance and Transparency Menu*) to check for updates and revisions.

4. Human Resources Management

a) DATA PROTECTION AND INFORMATION SECURITY AWARENESS It is extremely important that COOXUPÉ suppliers' employees access security and/or data protection awareness programs and receive periodic updates on awareness. Security education must be an ongoing process in order to mitigate and reduce risks.

b) TERMINATION OR REPLACEMENT OF SUPPLIER'S EMPLOYEE(S): in the event of termination or replacement of the supplier's employee(s) assigned to provide services to COOXUPÉ, the supplier shall immediately notify COOXUPÉ in writing of the termination and/or replacement of the employee(s), so that the access rights of the former employee(s) may be duly removed and/or updated. If necessary, the supplier will be responsible for returning to COOXUPÉ any intellectual property documents, workstations, cell phones and/or any asset that COOXUPÉ has shared with the supplier".

5. Asset Managment

a) If supplier is going to store, process, share, disclose, integrate assets, information and data belonging to COOXUPÉ, he will receive a questionnaire with technical questions on information security, data protection and cyber security, for the evaluation of the supplier's assets, which may result in questioning by COOXUPÉ, if there is any doubt or divergence from the information filled out in the COOXUPÉ Information Security and Privacy Risk Assessment Form.

b) All suppliers' assets that need to connect internally to COOXUPÉ'S data network (except via VPN) must be inspected and the antivirus and advanced protection software used by COOXUPÉ, installed

c) COOXUPÉ assets that are shared with the supplier may not be shared with third parties, unless COOXUPÉ and/or the area responsible for the process is aware of this, through a formalized sharing agreement.

d) Suppliers must keep the assets of its environments that contain COOXUPÉ´S data/information, protected. Following information security procedures, standards and practices.

e) It is supplier's responsibility to adopt procedures to report anomalies or incidents in the assets where COOXUPÉ data and information, including personal data and sensitive personal data, are being stored, shared, disclosed, processed or viewed.

f) At the end of the services provided to COOXUPÉ, intellectual property assets, including personal data and sensitive personal data that have been shared may be subject to disposal, with formalization processes evidencing their deletion.

6. Access control

a) The supplier must maintain an acceptable level of access control in its environments containing COOXUPÉ data/information.

b) Access to COOXUPÉ'S assets must be carried out using authentication methods, which will be tracked by Cooxupé's access logs; in cases where data is processed, access to COOXUPÉ'S assets must follow specific security items that will be pre-agreed upon.

c) All access to the supplier's assets that hold COOXUPÉ data and information must be monitored by the supplier.

d) Suppliers must maintain access controls on their assets and processes for their employees, third parties and/or organizations that provide services to it, regarding the provision of services to COOXUPÉ.

e) Individually identify all employees or organizations that are under the responsibility of the supplier that provide services to COOXUPÉ.

f) Use authentication methods satisfactory to COOXUPÉ employees who access the supplier's assets.

g) All service accounts that will be used in the supplier's systems and/or platforms must be passed on and their access rights defined in conjunction with COOXUPÉ'S IT department.

h) Exclusion of standard accounts from systems, processes and assets after project implementation.

i) Keeping your assets up to date and maintaining controls and resources to mitigate access and improper attempts.

j) Control employee access to the supplier's assets by profile, i.e. access only to the data and information needed to carry out their work.

k) Safeguard the access credentials provided by COOXUPÉ, not allowing them to be shared, with exceptions agreed with both parties.

l) Suppliers must keep access logs, whether for integrations between systems, access by COOXUPÉ employees to its platform, as well as logs of storage, processing and sharing of assets belonging to COOXUPÉ, for later analysis and investigation, if necessary.

m) Access to the COOXUPÉ environment by employees, third parties or organizations that are the responsibility of suppliers will occur by VPN and named user.

7. Physical Security

a) The supplier must maintain appropriate physical security measures to protect computing systems, using software and hardware with an appropriate level of security to protect contracted assets, as well as maintaining protection measures against environmental disasters, power outages and other adverse events, in accordance with the risks relevant to the processes that impact COOXUPÉ'S business.

b) Suppliers must undertake not to leave papers, removable media, access credentials and/or other media containing COOXUPÉ assets on display**.**

c) Protect by appropriate access controls the datacenter(s) containing COOXUPÉ assets, in order to ensure that only authorized personnel are able to access it.

8. Operations Management

a) For any asset transfer containing COOXUPÉ data and information, it is not recommended to use public/non-corporate platforms in order to avoid data exposure.

b) It is recommended that supplier validates the configurations of assets that contain COOXUPÉ data and/or information, in order to avoid leaks and undue exposure of data and/or information.

c) When there is a need for the supplier to share, store, process, integrate processes and systems that contain COOXUPÉ assets, the information security team together with the supplier will evaluate the security requirements and if necessary, adjustments to the process may occur.

d) Suppliers must maintain protection against data exposure, attacks and intrusion attempts on platforms containing COOXUPÉ data.

e) Suppliers must use intrusion protection mechanisms for web attacks (Application Firewall) and software that automatically generates alerts for the cyber incident response team.

f) Use an updated antivirus solution on the devices of the supplier's employees who will provide services to COOXUPÉ to prevent data loss and intrusion attempts.

9. Business Continuity and Disaster Recovery

a) Suppliers must maintain a business continuity and disaster recovery plan that addresses the availability and integrity of the contracted system and/or service.

b) Implement redundancy to the support assets of the system supplier contracted by COOXUPÉ to maintain the agreed availability.

c) Suppliers must adopt a backup process and policies for the assets that store COOXUPÉ information.

d) The supplier will inform the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) via a questionnaire, with a view to the recovery and availability of assets containing COOXUPÉ data and/or information, as contracted.

10. Incident Response and Breach Notification

a) Suppliers must maintain a tested incident response program, which will be functional to respond to incidents involving COOXUPÉ data. Inform COOXUPÉ in the event of the discovery of any failure or vulnerability in the assets of its employees, third parties or organizations that contain COOXUPÉ data, as well as assets that provide access to COOXUPÉ data.

b) Unless the notification is delayed by the actions or demands of a legal authority, the supplier will inform COOXUPÉ immediately of any illegal access or unauthorized acquisition, use or disclosure of its data that has occurred in the contracted system and/or service.

c) Supplier shall take steps to mitigate the cause of any COOXUPÉ data breach, and shall take corrective measures to prevent future data breaches.

d) If the incident affects employees, cooperative members and others who have involvement with COOXUPÉ, the supplier shall, whenever it is possible, be responsible for providing such information on the nature and consequences of the data breach as is reasonably required to enable COOXUPÉ to notify affected individuals, government agencies and/or credit agencies.