March 3rd, 2022
Notice

Frequency Asked Questions

"Overkiz Data Protection and Security Policy"

Does Overkiz have a security policy? (Information System Security Policy or Information Security Policy)

Yes. Overkiz believes that information security governance is a critical component of its business and supports actions to improve its security level while maintaining efficient business processes.

The Overkiz security policy helps to:
- ensure the continuity of computer-based business operations
- prevent breaches of sensitive data
- strengthen the trust of employees and partners in information systems.

Does Overkiz have security rules (security-based policies, technical procedures, etc.)?

Yes. Overkiz has security rules in several areas of the company, including a Quality team with a CISO and an ISMS Manager, and a technical team, ensuring end-to-end encryption for the solution.

Has Overkiz appointed someone to manage your information system security (CISO)?

Yes, the Information Security Management System (ISMS) Manager is responsible for enforcing compliance with procedures implemented within Overkiz and for ensuring that all staff members are aware of the security impacts of the Overkiz solution.

The Chief Information Security Officer (CISO) is responsible for implementing the information system and for maintaining its availability, security, and integrity.

Has Overkiz implemented an information security management system (ISO 27001)?

Yes, Overkiz is ISO 27001-certified for the development and supply of SaaS-based Home Management System business-to-business (BtoB) service infrastructures for residential homes and vertical housing.

Has Overkiz defined a business continuity plan (BCP)?

Overkiz has established measures to guarantee service availability in the event of an incident.

2. Personal data

Does Overkiz have a data protection and confidentiality policy?

Yes. Please refer to our website: https://www.overkiz.com/en/privacy-policy.html

Has Overkiz conducted a risk analysis regarding your customers' personal data?

Yes. To carry out these risk analyses, Overkiz uses the tool provided by the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL).

Has Overkiz appointed a Data Protection Officer (DPO)?

Yes, the DPO ensures the compliance of organizational and technical measures employed within Overkiz.

Has Overkiz established a program to train and raise awareness among employees regarding customer personal data protection?

Yes, Overkiz is raising awareness among all of its employees and new hires.

Has Overkiz developed a policy for encrypting your customers' data?

Yes, this policy is based on our cryptography procedure.

Is there a documented procedure within Overkiz for managing incidents (identification, analysis, action plan, database collection, etc.)?

Yes, the information security management system encompasses incident management.

3. Audit and oversight

Does Overkiz have internal oversight to address information security and data protection?

Yes, this is handled by our quality teams.

Does Overkiz undergo periodic data security audits?

Yes, regular audits are conducted on our information systems both on a preventive basis by Overkiz and at the request of customers.

4. Physical security

Is there a physical security policy implemented by the company with different rules based on site criticality?

Yes, the development sites are subject to different access controls (badge and access code).

Does Overkiz verify physical access rights at your premises?

Access control verifications are performed at the Metz-Tessy location (sign-in sheet).