Technical and Organizational Measures

Summary

Context

On this annex you will find a description of the technical and organizational measures put in place by Scaleway in order in particular to protect its customers' data against any security breach which may result in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to their data.

These technical and organizational security measures are complementary to our Personal Data Processing Agreement (DPA) as well as our Privacy Policy.

The measures presented below relate only to the infrastructures and services offered by Scaleway. In accordance with our Terms of Service, the Customer remains solely responsible for the adequacy of the Services subscribed to with the activities it carries out thanks to said Services and with the regulations applicable to these activities, in particular concerning the choice of backup and encryption options, access management or any means that it considers necessary to protect itself from a possible deletion, alteration or modification of its data.

Gouvernance

Information security policy

Scaleway has an information security policy reviewed every year in the event of significant modifications or developments (e.g. major change in the legal and regulatory framework to which Scaleway is subject or as part of continuous improvement following an audit).

Roles and responsibilities

In accordance with the ISO/IEC 27001:2022 standard, Scaleway manages information security through risk management, and has an Information Security Management System (ISMS). The roles assigned to support this system are defined and documented (including: CIO, Head of Cyber Governance, Risk and Compliance and VP Trust & Security Operations).

Scaleway also has a DPO and a team dedicated to data protection.

Audits and certifications

Audits

In order to ensure an optimal level of security, external and internal audits are planned at least once a year (this frequency may vary depending on the perimeters concerned).

In accordance with regulations, audits can be carried out by clients under the conditions provided for in our Data Processing Agreement (DPA) and after validation of our Agreement relating to the performance of intrusion tests.

Certificates and certifications

Scaleway has certifications and is committed to compliance with various standards in order to guarantee the security of its infrastructure and information system. These standards are accessible on the Security & Resilience page and Scaleway can also provide certificates on request.

Personnel security

Confidentiality

Scaleway ensures that all of its staff process its customers' data securely and confidentially. As such, our staff is contractually subject to:

- a confidentiality and non-disclosure agreement
- an IT charter aimed at securely regulating the use of the tools made available to them

Awareness and training

All Scaleway staff are made aware of both information security and data protection via mandatory training courses during the recruitment process. This knowledge is then updated every two years using our internal training tools.

Asset management

Inventory and knowledge of assets

All assets, whether physical or virtual, hardware or software, are inventoried and updated in our asset management system. In addition, each asset is assigned to a manager, responsible for maintaining it in operational and security conditions as well as managing access and their deactivation.

Workplace security

Scaleway implements measures at each workstation to guarantee an adequate level of security, in particular:

- use governed by an IT charter (in particular conditions of use for personal use (BYOD), security of storage and transport, ban on removable storage media, etc.)
- enrolling in a mobile device management solution
- automatic session lock and automatic disconnection of applications
- antivirus protection - antispam

- automatic security updates
- limitation of user access
- backed up and secure storage space
- supervised and secure maintenance
- disk encryption

End of asset life

Assets are monitored and end-of-life applications that no longer require maintenance are removed or replaced.

Any asset at the end of its life is subject to secure data erasure in accordance with state-of-the-art standards and, if necessary, physical destruction.

Information protection

Classification and marking of information

Every Scaleway document benefits from a classification and marking indicating its level of confidentiality.

Transfer of information

Scaleway only uses secure tools that have been previously validated by the IT department in order to exchange confidential or internal information (ex : instant messaging, email, file sharing). Confidential information transmitted to external third parties necessary for the operation of the services or the life of the company is transmitted encrypted and via a non-disclosure agreement (NDA).

Retention period and deletion of information

Scaleway undertakes to delete or anonymize personal data which is no longer necessary for processing or whose processing has ended and which does not require additional archiving to guarantee compliance with a legal obligation or a legitimate interest of the company.

Data masking

Whenever possible, in order to improve the confidentiality of the data processed, Scaleway also uses pseudonymization in order to dissociate the link between the identity of the person concerned and other sensitive information concerning them.

Test data

Scaleway prohibits copying personal data from production environments to testing environments with a lower level of security.

Physical security

All offices, warehouses or data centers used by Scaleway benefit from reinforced protection, in particular via the following security measures:

- access control by badge with identification number;
- restriction of access rights to secure areas based on an authorization profile;
- access logging system;
- supervision of visitors and external people through support and supervision adapted to the accessible area;
- video surveillance device at building entrances and exits;
- fire-fighting device;
- protection against physical and environmental threats through establishments that comply with applicable regulations;
- regular inspections and tests of support services (electricity, telecommunications, water distribution, ventilation and air conditioning) necessary for the equipment and operation of data centers;
- supervision of maintenance through maintenance contracts

Systems and network security

Secure authentication

Scaleway has a secure authentication policy that applies to all of its staff:

- Implementation of an architecture based on the so-called “Zero Trust” model and not on implicit trust
- Complex passwords reset at regular intervals
- Strong authentication with a second factor (2FA) for privileged accounts

System security

Privileged rights are restricted and their uses traced.

Network security

Scaleway implements strict network segmentation to separate access.

The principle of separation of powers is strictly respected and only authorized employees can administer network equipment.

Security of exchanges

The security of exchanges is ensured by the following security measures:

- Secure email authentications with anti-phishing and spoofing protection

- End-to-end encryption of sensitive file shares (with non-disclosure agreement if necessary).

Change management

Change management is framed by a change management procedure. Changes are documented and analyzed. When customer impacts are identified, they are published on a dedicated page.

Supervision of audit tests

Internal intrusion tests on the system in production are planned in accordance with the constraints and needs of the staff in charge of the technical infrastructure. For each test, the technical scope is clearly defined and shared with the parties concerned and the information provided to the testers is limited to what is strictly necessary to carry out the audit. These tests have no operational impact on the data or services used by our customers.

Data protection by design and by default

Secure Development Lifecycle

Scaleway attaches great importance to the integration of security in the different stages of development operations:

- Planning phase: Carrying out a risk and compliance analysis by design and by default
- Design phase: compliance with secure coding rules
- Deployment phase: deployment into a staging environment and verification through security acceptance testing
- Operation phase: monitoring application logs to detect suspicious activity

Secure coding

- Appropriate protections against the most critical vulnerabilities of web applications are implemented in accordance with the ASVS (Application Security Verification Standard) developed as part of the OWASP (Open Web Application Security Project).
- A SAST (Static Application Security Testing) type analysis is systematically carried out on all suitable source codes.

Impact analyzes

Scaleway carries out data protection impact assessments (DPIAs) if the processing is likely to result in a high risk to the rights and freedoms of the data subjects.

Identity and access management for Scaleway staff

Scaleway implements a strict identity and access management policy concerning the access and rights assigned to its staff, in particular via the following systems:

- Respect the principles of least privilege and need to know
- Regular review of rights and access throughout the life cycle of entrusted user accounts (arrival, mobility, departure)
- Ban on shared user account unless necessary
- Centralization of identities
- Access logging

When an employee leaves, all of their access and rights are revoked.

Customer identity and access management

Scaleway provides its customers, in particular via the IAM (Identity and Access Management) product, with the following security devices in order to secure access to their resources:

- Password with minimum complexity level required
- Secure password storage in accordance with state-of-the-art standards
- Ability to enable multi-factor authentication (MFA)
- Possibility of fine-tuning permissions granted on organizational resources to human users or applications
- Logging of access and use of privileged rights

Monitoring of services and infrastructures

Scaleway has the following tools in particular to monitor its services and infrastructures:

- A security information and event management system (SIEM) allowing, among other things, the detection of security incidents
- A critical asset monitoring system and an incident reporting system
- An anti-fraud detection device

In accordance with our general conditions of service, we remind you that Scaleway does not have access to the data hosted by its customers who are responsible for monitoring and implementing appropriate detection systems within the scope not dependent on services and infrastructures. by Scaleway.

Threat and vulnerability management

Scaleway collects and processes threat and vulnerability intelligence using:

- an internal CSIRT team dedicated to incident response;
- its relationships with external groups or systems (including other CSIRT/CERTs).

Vulnerabilities affecting company assets are constantly identified using various complementary detection tools, including regular technical vulnerability scanners and monitoring processes.

Business continuity

The continuity of activity of Scaleway's infrastructures and services is ensured by the following systems:

- Business Continuity Plan (BCP)
- Critical operations identified and associated with a restoration procedure
- Information meeting availability criteria regularly backed up
- Redundancies in information processing resources
- Asset sizing monitoring

Scaleway reminds that the Customer is responsible for the continuity of its information system (example: the choice of backup and restoration measures or the adequate sizing to ensure the proper functioning of its information system).

Security of relations with sub-processors

Scaleway ensures that all of its sub-processors benefit from an equivalent level of security through the following measures:

- Control of the level of security and compliance relating to data protection before the conclusion of the contract
- Check at least at each contract renewal or every two years for critical sub-processors
- Use of Standard Contractual Clauses or adequacy system in the event of use of a sub-processor located in an unsuitable country
- Inventory of sub-processors and contract documentation
- Monitoring, review and regular management of contracts with sub-processors.

Management of events related to information security

Scaleway implements the following systems to ensure the management of security-related events:

- Internal and external reporting processes and tools for events and incidents, including an external security incident reporting system via the address csirt@scaleway.com.
- Human and automated means of log analysis and incident detection (SOC)
- A team entirely dedicated to security incident response (CSIRT)
- A continuous improvement process relating to the response to security incidents with the objective of constant learning.