SECURITY OF JOTELULU'S SERVICES

Last update: November 2024

This document describes the technical and organisational measures implemented by JOTELULU as part of its services, to ensure the security of its clients' data, in particular data hosted on the infrastructures made available to them. It also describes the technical and organisational measures which the client is responsible for as part of the use of the services provided by JOTELULU. This document forms an integral part of the service agreement (or "Contract") in force between JOTELULU and the Client.

1. Security Objectives

JOTELULU

The technical and organisational measures implemented by JOTELULU aim to ensure, within the framework of the provision of its services, the security of data processed on behalf of its clients, notably the data hosted within the infrastructures made available to them, and in particular to protect the said data against destruction, loss, unavailability, alteration and unauthorised access.

Summary of the security objectives is available here: https://jotelulu.com/infraestructura-seguridad/

Client

The client defines its own security objectives, in particular those linked to its use of JOTELULU services. In particular, it ensures that the said services fit to its security objectives and, where applicable, to the needs and security objectives of the final customer.

2. Information Security Management System

JOTELULU

In order to achieve its security objectives, JOTELULU has put in place and maintains an appropriate information security management system ('ISMS'), under which policies, procedures and an organisation are formalised and implemented, enabling it to systematically and continuously:

- Identify information security risks, and put in place a treatment plan and appropriate technical and organisational measures;
- Designate the interested parties, and ensure that they are aware of the risks inherent in their role, and have the necessary expertise and resources to deal with these issues;

- Provide its clients with information enabling them to ensure that the services meet their needs, and to use the services in an appropriate manner so as to ensure the security of their data and the continuity of their activities.

This ISMS meets the requirements of the ISO27001:2022 standard and covers all activities carried out by JOTELULU and its subcontractors as part of the provision of the services.

The technical and organisational measures implemented within this framework are periodically reviewed and, if necessary, adapted to changes in the context (technological, regulatory, organizational, environmental, etc.) in which the services are provided.

JOTELULU provides its clients, upon request and in accordance with the terms of the Contract, with any additional useful information concerning its ISMS, including the threats taken into account and the criteria implemented as part of its risk management system.

Client

The client implements its own information security management system, to secure its information system and, in particular, its use of JOTELULU services.

In this context, the client shall ensure in particular that the services it uses, including the technical and organisational measures put in place by JOTELULU, are suited to its needs and, where applicable, to the needs of the final customers, and shall implement any necessary additional measure.

3. Risk management

JOTELULU

JOTELULU carries out formalised risk analyses using a methodology based on the ISO27005 standard. These analyses cover all activities linked to the supply of services provided by JOTELULU to its customers.

The risk analysis results in the definition of a treatment plan implemented under the responsibility of the CISO and asset managers.

The risk analysis is reviewed periodically, at least once a year, and gives rise to an update of the processing plan, thereby encouraging continuous improvement.

JOTELULU provides its clients, upon request and in accordance with the conditions set out in the Contract, with any additional useful information concerning its risk management, in particular the threats taken into account and the criteria implemented as part of its risk management system.

Client

The client is responsible for his own risk management, notably in connexion with its use of services.

The Customer ensures that the characteristics and conditions of use of JOTELULU services, and in particular the technical and organisational measures put in place by JOTELULU, are adapted to its activities and, where applicable, to the activities of the final customers, with regard to the risks inherent in said activities.

JOTELULU's services may be audited by the client as provided for in the Contract.

4. Standards et certifications

JOTELULU

As part of its activities, JOTELULU implements industry-recognised standards, in particular the following certification standards.

a) ISO/IEC27001 certification

JOTELULU has implemented an Information Security Management System (ISMS) that complies with the ISO/IEC27001:2022 standard.

The compliance of JOTELULU's ISMS with the ISO27001:2022 standard has been audited by a recognized independent auditor for the following services:

- Servers
- Remote Desktop
- File storage
- Object storage

b) CISPE Code of conduct

JOTELULU is committed to ensuring that its services comply with the *Code of Conduct for Cloud Infrastructure Service Providers* published by CISPE (Cloud Infrastructure Services Providers in Europe) association and approved by the CNIL on 3 June 2021 (see Deliberation 2021-065 of 3 June 2021), which defines the best practices that can be implemented by cloud “Infrastructures as a Service” providers to comply with the General Data Protection Regulation (GDPR).

c) INCIBE – Cybersecurity Catalog

JOTELULU is registered in the catalog of cybersecurity companies and services of INCIBE (Spanish National Cybersecurity Institute).

d) Innovative SME Seal

A seal that certifies that, in recent years, the company has carried out activities in the fields of Research, Technological Development, or Technological Innovation.

JOTELULU's compliance with these certification standards is reassessed and audited every year, both internally and by independent and recognized external auditors.

Where non-conformity is identified, corrective and remedial measures are put in place.

Client

Considering the context in which the use of JOTELULU services takes place, notably its contractual commitments to third-parties and the regulations applicable to its activities, the client ensures that JOTELULU services benefit from all required certifications.

The client takes into account in particular the type of data hosted on the infrastructures made available by JOTELULU, the processing carried out on said data, as well as, where applicable, the nature of the activities of the final customers.

5. Physical and environmental security

JOTELULU

JOTELULU services are hosted in top-of-the-range European data centres, selected according to strict criteria of security, availability and connectivity.

a) Physical access control

- Physical access subject to prior authorisation and systematic identity check
- Access control using individual and nominative badges or Biometric access management system
- Implementation of five (5) layers physical security protection (perimeter access, building, technical premises, rack cabinets).
- 24/7 presence of professional security guards
- 24/7 continuous video surveillance system including exterior and interior cameras (access doors, SAS, corridors) and video recording to investigate in case of incident
- Logging and periodic review of accesses.

b) Fire protection system

All environments have fire-fighting systems designed to extinguish any fire in a matter of seconds and without residue, including:

- - Smoke detectors
- - Automatic start-up of extinguishing systems
- - Manual emergency stop buttons in all rooms
- - Optical and ionic detectors with VESDA system
- - 24/7 monitored alarms.

c) Environment Controls

The data centres are located in areas with no known flood or seismic risks.

The services infrastructures are installed in permanently controlled environments under the following conditions:

- Continuous cooling (24/24)
- Redundant air-conditioning equipments
- Temperature of 21 °C
- 50% relative humidity
- Automatic incident detection and monitoring system.

d) Certifications

The data centres in which JOTELULU's services are hosted are certified in accordance with the following standards:

- ISO 14001 - Environmental management systems
- ISO 22301 - Security and resilience
- ISO 27001 - Information security management
- ISO 9001 - Quality management
- ISO 50001 - Energy management systems
- SOC1/SOC2 – Service Organisation Controls
- PCI-DSS - Payment Card Industry Data Security Standard
- HDS - French Health Data Host certification framework (Paris DataCenters)
- ENS - Spanish National Security Scheme (Madrid DataCenters)

e) Monitoring

JOTELULU ensures, by means of periodic assessments, that the third-party providers in charge of making available and maintaining in operational conditions the data centres used in the context of the services, implement appropriate technical and operational measures as described above.

Client

The client is solely responsible for the physical and environmental security of all infrastructures that it uses and that are not provided by JOTELULU.

6. Services continuity

JOTELULU

JOTELULU has put in place a service continuity plan constituted of the various measures described below.

This plan is reviewed periodically and, if necessary, adapted to the changes that may occur in the context in which services are provided.

The measures implemented to ensure the continuity of critical assets are tested periodically.

a) Infrastructures redundancy

JOTELULU has deployed a redundant architecture so that the failure of a component does not impact the normal operation of services, in particular:

- The data centres are equipped with redundant connections to the electricity network and kinetic diesel generators sized to meet the energy needs of the entire building and the infrastructure
- Each server has two power supplies, each connected to a different electrical segment of the data centre.
- The data centres in which the services are hosted are neutral and offer a wide range of connectivity, enabling JOTELULU to have several network circuits from different suppliers to protect itself against a loss of connectivity due to the failure of one supplier.
- The infrastructures' equipment has at least two high-availability network connections (LAG), and each network connection has its own switch, so that a failure of one switch does not result in any interruption of service.
- JOTELULU has set up a multi-chassis link aggregation in which each router and each switch (aggregation and access) is redundant, which ensures the availability and scalability of the network.
- Administration Portal infrastructure is HA in 2 different DataCenters
- N x 1.25 redundancy on hypervisors, providing enough capacity to withstand the failure of up to 25% of them. In case of a hypervisor failure, the servers hosted on it are automatically started on other hypervisors.
- Storage high availability, combining storage-based clustering with synchronous mirroring to provide seamless recovery from failures.

b) Anti-DDoS system

The infrastructures are equipped with an anti-DDoS system that prevents and filters out Denial of Service attacks to ensure the services availability.

This system is structured around several filtering and detection lines that enable small attacks (a few hundred Mb/s) to be screened and differentiated from larger attacks of thousands of Gb/s.

c) Capacity planning

JOTELULU ensures through monitoring and periodic reviews that the capacity and sizing of the infrastructures used to provide the services are adapted to the service level agreements.

With regard to resources shared by several clients, JOTELULU makes best effort to meet its clients' capacity needs, but cannot guarantee any volume of available resources.

d) Change management

JOTELULU implements a change management policy designed to ensure continuity of services in the event of changes or modifications.

As part of the development, updating and evolution of the information system, the following principles are applied in particular:

- Requirements and Risks evaluation at the planning stage
- Development in a dev environment
- Testing and Quality Assurance acceptance, including security
- Testing un beta environments
- Put in production after approval following change process planning.

Clients are informed of changes that may have an impact on the conditions of use of services (in particular performance levels, interoperability conditions, security levels, continuity of services, functionalities changes, etc.).

Client

The client is responsible for the continuity of its activities, in particular the availability of the information system that it hosts on the infrastructures made available to it by JOTELULU.

In this respect, the client:

- ensures the proper management of the elements and processes within its scope of responsibility as set out in the service contract
- ensures that the characteristics and conditions of the services (in particular the sizing and performance level of the services) are such as to enable it to achieve its availability and continuity objectives;
- is responsible for activating and configuring any functions and options made available to it to ensure the continuity of its activities (in particular back-up and versioning functions);
- implements any additional measures (such as remote back-ups, redundant resources, etc.) which may be necessary to guarantee that these objectives are met;
- takes account of incidents as well as changes and developments to the services communicated to it by JOTELULU, and adapts, if necessary, its organisation and the conditions under which it uses the services.

7. Logical access management

JOTELULU

a) JOTELULU access to information system

JOTELULU implements the following measures to secure access to the various components of the information system used in the context of the services:

- Documented and centralised identity and access management;
- Formalised process for assigning and removing access rights;
- Implementation of the least privilege and minimisation principles;
- Allocation of access rights on the basis of predefined roles or operational groups membership;
- Periodical review of access rights;
- Supervision of the employee entry/exit process, in particular to ensure that access rights are allocated and revoked appropriately, especially when an employee leaves the organization or changes his/her mission.
- Use of individual and nominative user accounts if possible;
- Implementation of a *state-of-the-art* password management policy;
- Implementation of a mandatory multi-factor authentication system for roles with privileges, in particular administrators;
- Logging of connections and secure storage of logs.

b) Client's access to the services

JOTELULU provides the client with a platform enabling it to designate the persons authorised, on the client's behalf, to use JOTELULU services.

In particular, this platform allows users to be created and deleted, and different user profiles to be created with specific access rights.

The platform also enables client to use two-factor authentication.

Access and events logs are recorded and kept for 12 (twelve) months, and are available to the client within the platform or upon request to Client Support.

Client

The client is solely responsible for managing the access of members of its staff to the services and to the services management Platform made available to it by JOTELULU. In particular, the client is responsible for:

- The creation and deletion of user accounts for members of its staff, and the allocation of the rights necessary for them to carry out their duties;
- Activating the two-factor authentication (2FA) functionality;
- Controlling and periodically reviewing the access rights of its staff;

- The implementation of technical and operational measures to ensure the confidentiality of the authentication methods of the users who are members of its staff.

In addition, the client is solely responsible for managing authorisations and logical access to systems and applications not provided by JOTELULU (including those deployed as part of the services).

8. Assets management

JOTELULU

All the assets required to provide the services (in particular physical and virtual machines, network equipment, , storage space, etc.) are inventoried.

The inventory of assets is updated periodically.

Each asset is the responsibility of an identified team in charge of ensuring the proper management of the asset in compliance with the policies implemented by JOTELULU (analysis and treatment of associated risks, vulnerability management, access management, maintenance in operational condition, etc.).

At the end of its life or in the event of a change of use for an asset that may contain data, an erasure process that complies with industry standards is implemented beforehand.

Similarly, equipment reaching the end of its life is destroyed in accordance with industry standards.

Client

The client is responsible for managing and securing the assets that it uses as part of the services (instances, storage spaces, systems and applications installed on the infrastructures made available to it, etc.).

Before the effective date of termination or expiry of the services they use, customers must ensure that the data hosted on them is deleted.

9. Vulnerability management

JOTELULU

The information system used to provide the services has appropriate protection against the risks of intrusion (partitioning, firewalls, IP filtering and intrusion detection systems, bastion access).

Employees' workstations are equipped with up-to-date antivirus software and a malicious code detection system.

In addition, JOTELULU maintains a technology watch enabling it to detect and remedy vulnerabilities in the assets used to provide its services.

Vulnerabilities are detected in particular via :

- Information from the manufacturers and publishers of the components used;
- User communities;
- Open-source communities, where applicable;
- Incidents detected by JOTELULU and/or its customers;
- Service monitoring;
- Code and configuration reviews, particularly in the case of new developments;
- Internal audits and penetration tests carried out periodically.

When a vulnerability is detected, an impact study is carried out, mitigation and remediation actions are implemented, and exposed customers are informed.

Client

The client is responsible for the management of vulnerabilities of elements which are outside the scope of responsibility of JOTELULU, in particular systems and applications deployed on the infrastructures made available by JOTELULU.

The client implements all useful measures to minimise the impact of and remedy vulnerabilities of which it is aware, in particular those which are reported to it by JOTELULU.

10. Human resources

JOTELULU

JOTELULU implements appropriate measures to ensure that the staff it employs have the necessary skills and knowledge to contribute to information security, in particular :

- Employees entry and exit is governed by processes that control the assignment and return of assets and the allocation of logical access to the information system;
- All employees are made aware of information security and the protection of personal data on their arrival and then periodically (at least once a year);
- All contracts (for work or services) include a confidentiality undertaking;
- Formalised policies and procedures relating to the management and use of the various components of the information system are made available to employees which are committed to comply with such policies and procedures;
- Communications and test campaigns are carried out with employees on a regular basis.

Client

The client remains responsible for the members of its staff, in particular those responsible for using the services.

The client shall ensure that its staff members have the necessary knowledge and skills to use the services and communicate to them the conditions of use of the services (including in the event of modification), and more generally all useful instructions and information.