Responsibility Assignment Matrix

Table of contents

1. Introduction

The responsibility assignment matrix describes the responsibilities of the stakeholders in the framework of their contractual relations. The requirements are in line with ISO 27001, HDS and the SecNumCloud (SNC) labels.

ISO 27001 requirements apply to all Clients who have signed a contract with Outscale.

SNC requirements apply only to Clients who have signed an SNC Service Agreement for SNC Qualified Services.

HDS requirements apply only to Clients who have signed the HDS Specific Conditions for HDS Certified Services.

By default, everything that applies to the ISO 27001 standard applies to the SecNumCloud and HDS labels. The specific SecNumCloud and/or HDS label requirements are indicated in the column “Label,” by the terms “SNC” and “HDS” respectively. When one of the responsibilities indicated in the matrix does not stem from any of the standards, “ - ” will be indicated in the “Label” column.

Any changes made to the responsibility assignment matrix will be subject to the Client's acceptance.

In the event that terms beginning with a capital are used which are not defined in this Appendix or in the Agreement, it is agreed between the parties that said terms must have the same meaning as given in the associated label.

2. Tools

- Outscale’s responsibility

Description	Label
Outscale provides the Client with an application programming interface (API) or Graphical User Interface (GUI) with its Virtual Machines so that it can manage the virtualized infrastructure.	-
Outscale provides a service control API enabling the Client to automate the management and administration of the Services in accordance with the SLA.	-
In the framework of the Services, Outscale undertakes not to access Client Data: Outscale manages the physical storage of the Data, but undertakes not to access their logical storage.	-

- Client’s responsibility

Description	Label
It is up to the Client, assisted if necessary by an IT specialist, to ensure that its system can be administered via the interface supplied by Outscale, which implies that the Client must have asked Outscale any useful questions in this respect before accepting the Agreement.	-

The Client uses the API in accordance with its intended purpose and public documentation (including the automatic order subscription features).	-

3. Good use of the Service

- Outscale's responsibility

Description	Label
Outscale places the Services ordered at the disposal of the Client.	-
Outscale supplies the On Demand Resources subscribed on condition that they are available at the time of the order.	-
Outscale makes its Support Service available to the Client via the following channels: - Outscale support web interface - Email - Telephone	-
Outscale does not have access to the Client Data. As an exception, Outscale may access the Client Data following an express, written request by the latter for the purposes of carrying out actions that are indispensable for incident diagnosis and resolution. Outscale may refuse a request for intervention involving access to Client Data if it considers the action can be carried out by the Client. In any case, technical support is provided from within the European Union by authorized personnel who have met the recruitment criteria defined by Outscale in accordance with the SNC label.	SNC – 9.7 d)

- Client's responsibility

Description	Label
The Client undertakes not to do anything with the Services supplied that could endanger the Outscale services or the resources of other clients.	-
The Client undertakes to use the Services supplied reasonably and in good faith, in accordance with its business such as described in the tacit or express specification of its needs as well as in its corporate purpose. The Client therefore undertakes not to carry out any activity which would result in an abnormal use of the facilities or hardware necessary to supply the Services. This applies to any activity which would result in premature wear of the storage media (in particular hard disks) placed directly or indirectly at its disposal, in particular by carrying out activities such as calculation or cryptocurrency mining.	-
The Client alone is responsible for its System (including the Data, wherever they come from); it is also responsible for its domain names, SSL certificates, the management of its System logs in accordance with the law, etc.	-
The Client uses the Services in accordance with the public documentation.	-
The Client ensures that the System is not contrary to the different standards, laws, decrees, etc. both national and international (incitement to racial hatred, pedophilia, public order disturbance, defamation, press and audiovisual communication laws, economic public order, spam, cybercrime, etc.).	-
The Client must not commit or facilitate, either directly or indirectly, any acts of counterfeit, parasitism, or unfair competition via the Services.	-

If the Client intends to process critical or strategic data (for example invoicing data, payroll, R&D elements, etc.) on the Outscale Virtual Machines/Object Storage, it is up to the Client to take out specific cybersecurity insurance to cover IT risks.	-
When using the support services, the Client receives a ticket. The Client must use this ticket in all exchanges with the client support services and keep the same object in all email exchanges to enable efficient follow-up of any request and its resolution. The detailed procedure related to support is described in the Outscale Public Documentation: https://docs.outscale.com/	-

4. Regionalization

- Outscale's responsibility

Description	Label
Outscale provides its clients with the documentation associated with the Services and a support Service in French in accordance with the Agreement.	HDS – 4.5.5
Outscale undertakes to give a list of all countries within which Client Data are or may be hosted.	HDS – 4.4.7.1 P
Outscale informs the Client of the hosting centers in which the health data are stored.	HDS – 4.4.7.1 C
Outscale allows the Client to choose the hosting countries in which the health data will be stored, and implements measures to enable this choice to be respected.	HDS – 4.4.7.1 C
By default, Outscale shall provide the Client with a different set of Access Keys to the Service for each Region.	-
The Outscale infrastructure is designed so that the failure of an Availability Zone does not affect the other Zones within the Region.	-

- Client's responsibility

Description	Label
It is the Client's responsibility to launch its System in all the Region's Availability Zones provided by Outscale.	-
When the Client chooses to host personal health data, they shall, in accordance with the General Data Protection Regulation, conclude the specific HDS conditions with Outscale and choose among the available Regions, the hosting country in which the health data will be hosted.	HDS – 4.4.7.1 C

5. List of Client contact persons

- Outscale's responsibility

Label	Label
Outscale keeps the list of contact persons designated by the Client in order to transmit the contact details to the competent authorities upon request. This list is updated regularly.	HDS – 4.5.4

- Client's responsibility

Description	Label
The Client undertakes to appoint a Manager with the technical skills and legal capacity necessary to: - Use and manage the Services (in particular authorize and/or manage extensions to the scope of the Services), - Operate the Resources, - Manage the Account and in particular ensure that the payment information is valid at all times in order to avoid any payment delays. The Client undertakes towards Outscale to maintain a permanent contact Manager. This contact person must be able to refer Outscale to a health professional whenever necessary.	HDS – 4.5.4

6. Recovery and deletion of client data/Reversibility

- Outscale's responsibility

Description	Label
In the event of the termination of the Agreement, for any reason, the Client Data shall be deleted as indicated below, with the exception of the data that must be kept by law (in particular invoicing information and related identifications shall be kept to comply with legal obligations applicable to Outscale for a period of up to 10 (ten) years). Client accounts are deactivated manually by Outscale, but the deletion of Client Data by Outscale is automatic. Once an Account has been deactivated, the data is accessible for a period of 90 days before complete destruction. A certificate of data destruction may be transmitted to the Client if the latter requests one from Outscale. The Client is informed that the log which constitutes proof of destruction of the Client Data is supplied at the latter's request and is kept for a period of one (1) year. The Client therefore has one year in which to request this proof. However, the Client is informed and recognizes that Outscale is not able to destroy any Data that the Client has shared with a third party, namely by sharing OMI or disk images, as long as the latter is using the shared data. It is up to the Client to define the rules for the sharing of Resources and, if applicable, not to share confidential and/or Personal Data. The Client guarantees Outscale and holds it harmless against any possible conviction, on whatever grounds, following a violation of this provision by the Client.	-
Outscale has defined a policy governing the access and return of personal data to clients, as well as their destruction, and undertakes to make this policy available to clients upon request.	HDS – 4.4.5.3 P

Outscale has implemented a reversibility procedure describing the conditions for the return of data at the end of the agreement or in the event its accreditation is withdrawn.	HDS – 4.4.5.3 C
Outscale has identified the temporary personal health data and implemented the internal procedures necessary to ensure their destruction.	HDS – 4.4.3.1 P
Outscale guarantees that the virtual storage allocated to the Client does not enable any previously stored data to be accessible or visible.	HDS – 4.4.6.14

- Client's responsibility

Description	Label
The Client alone is responsible for its System and takes the steps necessary to facilitate reversibility operations where necessary, which involves, inter alia, providing documentation for this purpose and defining Reversibility plans.	-
Recovery of its Data by the Client if it has access to its Data; Upon termination of the Agreement, for any reason, the Client must imperatively retrieve all its Data hosted at Outscale before the effective termination date. From this effective termination date (at midnight Paris time): (i) the Client shall no longer have access to its Data, and (ii) the Data shall be destroyed by Outscale.	-
Recovery of its Data by the Client if it does not have access to its Data; When the Agreement is terminated, whatever the reason, and the Client no longer has access to the Services following a suspension of the Services as provided, it must imperatively request from a Data recovery Service prior to the effective termination date. The Client cannot order this Data recovery Service if it is not up-to-date with payment of its invoices to Outscale. The Client must therefore imperatively pay Outscale all outstanding amounts owed before the effective termination date. The Client may request a Data recovery Service by email addressed to Outscale customer service who shall issue an offer. If the Client accepts this offer, OUTSCALL shall retrieve and transmit to the Client its Data upon payment of the Data recovery Service. As of the date of effective termination (midnight, Paris time) the Client Data shall be destroyed.	-

7. Assessment of risks

- Outscale's responsibility

Description	Label
Outscale undertakes to document a risk assessment procedure covering the entire scope of the Service.	ISO – 6.1.2 + SNC – 5.3 a)
Outscale carries out its assessment of risks using a documented method that guarantees the reproducibility and comparability of the process.	ISO – 6.1.2 + SNC – 5.3 b)
As part of its risk assessment process, Outscale undertakes to take the following elements into account: - management of client information with different security needs; - risks with an impact on the rights and freedoms of the data subjects in the event of unauthorized access, unsolicited modification or loss of personal data; - risks of failure of the technical infrastructure's resource separating mechanisms (memory, calculation, storage, network) shared between clients; - risks related to incomplete or unsecured deletion of data stored on memory space or storage media shared between clients, in particular during reallocation of memory and storage space; - risks related to administration interface exposure on a public network; - risk of violation of client data confidentiality by third parties involved in the provision of the service (suppliers, subcontractors, etc.); - risks related to natural events and physical accidents; - risks related to separation of duties; - risks related to development environments.	SNC – 5.3 c)
In its assessment of risks, Outscale undertakes to take into account the specific legal, regulatory or sector-based requirements related to the type of information entrusted by the client, making sure that the SecNumCloud label requirements are met and that the level of security of the SecNumCloud label requirements is not lowered.	SNC – 5.3 f) SNC – 8.3 b)
Outscale has identified risks associated with plurality of responsibilities or tasks and has taken these into account in its risk assessment and implemented measures to limit these risks.	SNC – 6.2 a)
Outscale takes development environment risks into account in its risk assessment.	SNC – 14.4 b)
Outscale has defined the measures necessary for risk management purposes and declares that no necessary measure has been neglected.	ISO – 6.1.3
Outscale has formally accepted the residual risks identified in the context of its risk assessment process.	ISO – 6.1.f + SNC – 5.3 e)
Outscale undertakes to conduct information security risk assessments at planned intervals or when significant changes are planned or made.	ISO – 8.2
Outscale undertakes to review its risk assessment process annually, and upon each major change which could have an impact on the Service.	SNC – 5.3 f)
Outscale undertakes to analyze and manage risks related to the virtual infrastructures deployed by: (i) providing training for the persons authorized to operate the Outscale infrastructure, in particular on the specificities of the cloud, (ii) auditing backups, data integrity and equipment access to the Outscale Infrastructure at regular intervals, (iii) deploying state-of-the-art resources to limit access to established functional needs only, (iv) using encrypted and/or dedicated links where necessary for sensitive communications.	-
Outscale undertakes to document residual risks linked to the existence of laws from outside Europe whose objective is the collection of data or metadata from clients without their prior consent.	SNC 5.3 d)

Outscale communicates to the Client, upon request, the risk assessment elements linked to client data being subject to the laws of a non-European Member State.	SNC-5.3 e) SNC -19.1 e)

- Client's responsibility

Description	Label
For any data subjected to specific requirements, the Client shall provide Outscale with the necessary elements to assess whether the Services satisfy the expected regulatory conditions and standards. Based on these elements, Outscale collaborates with the Client on the measures to be taken to provide an adequate response.	SNC – 5.3 c) SNC – 8.3 b)
The Client is responsible for conducting risk analysis on the System.	-

8. Information security policy

- Outscale's responsibility

Description	Label
Outscale supplies its Services in state-of-the-art conditions. Outscale seeks to use stable software with security fix follow-up and set up in such a way as to obtain an appropriate level of security.	ISO + SNC – 5.1 a)
Outscale undertakes to implement an information security policy adapted to its business and Service.	ISO – 5.2 + SNC – 5.2 a)
Outscale undertakes to formally approve its information security policy.	ISO – 5.1.1 + SNC – 5.3 d)
Outscale undertakes to implement a set of information security policies that is shared and communicated to its staff and to the suppliers concerned.	ISO – A5.1.1
Outscale undertakes to apply a security policy covering: - Periodical risk assessment; - The security of human resources; - The management of equipment; - Access control and management of identities; - Data encryption; - Physical and environmental security; - Security related to operations; - Communications security; - Compliance monitoring; - Operation of the technical infrastructure; - Management of suppliers; - Management of incidents related to information security; - Business continuity; - Compliance relating to the supply of the Service and national legislation and regulation applicable based on the type of information transmitted.	SNC – 5.2 c)
Outscale has identified, in accordance with its information security policy, its commitments in terms of compliance with applicable regulations and the nature of Data entrusted by the Client when it is aware of this.	SNC – 5.2 b)

Outscale undertakes to revise its information security policies at scheduled intervals or in the event of major changes.	ISO – A5.1.2
Outscale undertakes to review its general policy and its risk assessment annually and whenever a major change may impact the Service.	SNC – 5.2 e)
Outscale incorporates the ANSSI's computing safety guidelines for information systems in its own information security policy.	SNC – 5.1 b)
Outscale defines and attributes responsibilities in terms of the protection of personal data in line with its role in the context of processing concerning the Service, such as described in the DPA appendix.	SNC - 6.1 e)
Outscale appoints a data protection officer and shall carry out and contribute to performing a privacy impact assessment in case data processing lead to a high risk to the rights and liberties of the data subjects in the conditions set forth in the DPA.	SNC - 6.1 g) - 6.1h)

- Client's responsibility

Description	Label
For any data subjected to specific requirements, the Client shall provide Outscale with the elements necessary to assess whether the Services satisfy the expected regulatory conditions and standards. Based on these elements, the Parties collaborate together on any reasonable joint action in order to provide an adequate response.	SNC – 5.2 b)
The Client thus recognizes that the Services satisfy the legal and regulatory requirements applicable to its Data.	SNC – 5.2 b)

9. Organization of information security

- Outscale's responsibility

Description	Label
Outscale undertakes to implement an internal security organization.	ISO – A6.1.1 + SNC 6.1 a)
As part of its security organization, Outscale has appointed an information systems manager, an information systems security manager, a physical security manager and a data protection officer (DPO).	SNC – 6.1 b) e) f) g)
Outscale applies the principle of separation of duties and responsibilities in its organization.	ISO – A6.1.2
Outscale has defined and attributed responsibilities in terms of information security for the staff involved in supplying the Service and revises these duties after any major change that could have an impact on the Service.	SNC – 6.1 c) d)
Outscale maintains appropriate relations with the competent authorities.	ISO – 6.1.3
Outscale maintains appropriate relations with interest groups or specialized forums.	ISO – 6.1.4
Outscale integrates information security in project management, whatever the type of project.	ISO – 6.1.5
Outscale documents an estimation of risks prior to any project which could have an impact on the Service, whatever the nature of the risk.	SNC – 6.5 a)
If a project affects or could affect the level of security of the Service, Outscale undertakes to inform the Client of potential impacts, measures implemented to limit these impacts as well as residual risks concerning the Client.	SNC – 6.5 b)
Outscale undertakes to carry out or contribute towards an impact analysis relating to the protection of personal data when processing could impact the rights and liberties of the data subjects.	SNC – 6.1 h)
Outscale has adopted a policy and security measures to manage the risks stemming from the use of mobile devices.	ISO – A6.2.1
Outscale has implemented a policy and security measures to protect the information consulted, processed, or stored at teleworking sites.	ISO – A6.2.2
Outscale has defined a policy and measures to manage mobility situations for the administrators under its responsibility. In this context, Outscale declares that the measures implemented guarantee a level of security that is at least equivalent to the level of security when mobility is not involved.	SNC – 12.12 c)
Outscale carries out periodic testing to ensure that the protection measures implemented satisfy the security requirements and policies set in place, and to define their results (type of testing, regularity).	-

- Client's responsibility

Description	Label
Outscale advises the Client to define an internal organization facilitating collaboration with Outscale regarding the application of information security.	-

10. Security of human resources

- Outscale's responsibility

Description	Label
Outscale implements employment verification when hiring staff, in accordance with applicable laws and regulations and in adequation with the requirements of the business, the sensitivity of the information entrusted and the risks identified.	ISO – A7.1.1 + SNC 7.1 a)
Outscale carries out stricter background checks for staff with high administrator privileges.	SNC 7.1 b)
Outscale establishes contractual agreements for staff and subcontractors which specify their respective responsibilities within the organization in terms of information security.	ISO – A7.1.2
Outscale imposes security rules on all staff and contractors as defined in the policies and procedures applicable in the organization.	ISO – A7.2.1
Outscale has established a code of ethics as part of the internal rules and regulations, which specifies that: - the services are carried out with loyalty, discretion and impartiality and the information is processed confidentially. - the persons involved in supplying the Service undertake to use methods, tools and techniques that have been validated internally, not to disclose confidential information to any third parties, in any form, unless they have been given formal, written authorization by the client, to report any illegal content, comply with applicable national legislation and regulations and good practices linked to their activities and to sign the code of ethics.	SNC – 7.2 a) b)
Outscale places at the Client's disposal, if it so requests, the Outscale code of ethics and internal rules and regulations.	SNC – 7.2 d)
Outscale conducts awareness campaigns and adapted training programs for all its staff on the subject of information security and the risks related to personal data protection.	ISO – A7.2.2 SNC – 7.3 a)
Outscale has defined a formal disciplinary process known to all in order to take measures against employees breaching information security rules.	ISO – A7.2.3 SNC – 7.4 a)
Outscale places at the Client's disposal, if it so requests, the type of sanctions that may be imposed on its staff in the event of a breach of the security policies.	SNC – 7.4 b)
Outscale has defined and attributed roles and responsibilities relating to the termination, expiration or modification of any contract with a person involved in supplying the Service.	ISO – A7.3 SNC – 7.5 a)

- Client's responsibility

Description	Label
The Client requests communication of the documents relating to the Security of human resources from Outscale via the different communications channels placed at its disposal (Support, Account Managers or Service Delivery Manager if applicable).	SNC - 7.4 b) – 7.2 d)

11. Equipment management

- Outscale's responsibility

Description	Label
Outscale identifies and keeps an updated inventory of all the equipment used to provide the Service.	ISO – 8.1.1 + SNC 8.1 a) b)
Outscale has defined an internal manager for each internal asset.	ISO – 8.1.2
Outscale checks the validity of the software licenses that it supplies in the framework of the Services.	SNC – 8.1 c)
Outscale applies an equipment return procedure to ensure that each person involved in supplying the Service returns all the equipment in their possession at the end of their employment period or contract.	ISO – 8.1.4 SNC – 8.2 a)
Outscale has identified the different information security needs relating to the Service.	SNC – 8.3 a)
Outscale has implemented an information classification policy and information processing procedures.	ISO – 8.2
Outscale implements procedures for marking and handling all information involved in supplying the Service.	SNC – 8.4
Outscale undertakes to destroy paper copies using appropriate means.	HDS – 4.4.6.7
Outscale has implemented procedures for the management of removable devices in accordance with its information classification policy.	ISO – A8.3 + SNC 8.5 a) b)
Outscale has designed procedures to protect portable storage devices containing personal data, if they leave the premises, to ensure that these data are not accessible to unauthorized persons.	HDS – 4.4.6.4
Outscale prohibits the use of portable storage devices that are incompatible with encryption solutions.	HDS – 4.4.6.5
Outscale implements a backup, recovery and recovery test procedures for data which are (i) under its responsibility, (ii) necessary to operate the platform and (iii) Snapshots of volumes taken by the Client.	ISO - A12.3 SNC - 12.5
Outscale provides the means to guarantee the level of protection of confidentiality and integrity of retired equipment, recycled hardware and equipment that has not yet been put into use.	SNC - 11.8 SNC - 11.9 SNC - 11.10

- Client's responsibility

Description	Label
The Client shall inform Outscale if any hosted data is subjected to specific legal, regulatory or sector-based requirements.	SNC – 8.3 b)
For any specific requirements applicable to the data, the Client shall supply Outscale with the elements necessary to assess whether the Services satisfy the expected regulatory conditions and standards. Based on these elements, Outscale cooperates with the Client on the measures to be taken jointly to provide an adequate response.	SNC – 8.3 b)
The Client shall define a classification of its resources, to classify them and make sure that its employees are aware of the correct use of the resources made available by Outscale.	-
The Client shall respect the terms of the software licenses supplied as part of the Service, in particular when a license is necessary for the use of third-party software.	-

12. Access control and identity management

- Outscale's responsibility

Description	Label
Outscale implements, documents and revises the access control policy for users placed under its responsibility, on the basis of operational and information security requirements.	ISO – A9.1.1
Outscale ensures that its users only have access to the network and network services for which they are authorized.	ISO – A9.1.2
Outscale implements a registration and deregistration procedure for users and an accreditation process destined to enable the attribution of access rights.	ISO – A9.2.1 SNC – 9.2 a)
Outscale implements processes to manage user access control in the allocation and revocation of access rights for all users, for all systems and all information Services.	ISO – A9.2.2 SNC – 9.3 a) g)
Outscale implements processes to limit and control the attribution and use of access privileges.	ISO – A9.2.3
Outscale implements a process for the attribution of secret authentication information.	ISO – A9.2.4
Outscale conducts a regular review of user access rights.	ISO – A9.2.5
Outscale undertakes to revoke or adapt its users' access rights at the end of their period of employment or in the event of any modification of their responsibilities.	ISO – A9.2.6
Outscale sets in place rules to protect authentication information and demands that all users follow these rules.	ISO – A9.3.1
Outscale implements access restrictions to information and systems applications.	ISO – A9.4.1
Outscale implements a secure connection procedure for access to certain systems and applications.	ISO – A9.4.2
Outscale implements multiple device password management systems which guarantee the quality of passwords.	ISO – A9.4.3
Outscale limits and controls the use of privileged utility programs which make it possible to bypass security measures.	ISO – A9.4.4
Outscale limits access to program source codes.	ISO – A9.4.5
Outscale provides the Client with the means to manage the access rights and identities of users who are the Client's responsibility, and to review these rights.	SNC – 9.3 b) 9.4 b)
Outscale keeps an up-to-date register of users or user profiles with access to personal data or to the systems used for their processing.	HDS – 4.4.6.9
Outscale implements processes to be able to supply, for a given user, under its responsibility or the Client's responsibility, the list of all access rights to different elements of the Service's information system.	SNC – 9.3 e)
Outscale keeps an inventory of users and rights attributed and implements the procedures necessary for the allocation, reallocation and revocation of access rights (including revocation or suspension) and ensures when attributing rights that the users do not have access rights that are incompatible and conducts reviews of these rights.	SNC – 9.2 a) c) SNC - 9.3 a) c) d) g)
Outscale attributes nominal accounts when registering the users placed under its responsibility.	SNC – 9.2 b)
Outscale keeps a list of incompatible access rights and ensures when attributing access rights that the user does not have incompatible access rights.	SNC – 9.3 f)

Outscale carries out an annual review of the access rights of the users under its responsibility.	SNC – 9.4 a)
Outscale carries out a quarterly review of the list of users under its responsibility.	SNC – 9.4 c)
Outscale uses separate listings for the management of the accounts of users placed under its responsibility.	SNC – 9.6 a)
Outscale supplies separate back office interfaces for its clients.	SNC – 9.6 b) c)
Outscale ensures that the back office interfaces that it uses are not accessible from a public network and cannot be used by the Client's users.	SNC – 9.6 d)
Outscale implements appropriate separation measures: - between clients; - between the Service's information system and the other information systems; - between the technical infrastructure, the equipment necessary for the administration of the Services and the resources that it hosts.	SNC – 9.7 a) b) c)
Outscale implements procedures for the management of user authentication concerning: - The management of authentication mechanisms and their life cycle; - The implementation of multifactor authentication; - Verification of the robustness of authentication mechanisms.	SNC – 9.5 a)
Outscale implements measures obliging users to authenticate via their nominal account before being able to access non-nominal technical accounts if these are necessary.	SNC – 9.5 d)
Outscale implements traceability in order to monitor generic user ID actions.	HDS – 4.4.6.8 C
Outscale implements measures to ensure that access to personal data or systems used for their processing is made through nominal accounts.	HDS – 4.4.6.8 P
Outscale implements procedures to block an account after a limited number of failed connections via the authentication mechanisms deployed.	SNC – 9.5 b)

- Client's responsibility

Description	Label
Access control and management of the identity of users, in particular users of the Services, are the Client's responsibility. Consequently, it defines all the policies governing access to the Services and reviews the access rights of the users of the Services.	-
For all actions within its account, the Client must authenticate its requests with the secrets it has initiated.	-
Outscale advises the Client to use double factor authentication with the Service and to impose the use of a separate physical device in order to maintain the level of security guaranteed by the SecNumCloud label.	SNC
The Client is advised to implement a password management and renewal policy.	-
The Client must regenerate its Access keys to the Service (in particular: passwords, etc.) regularly and at the request of Outscale, in particular for security reasons. Outscale provides the Client with the tools to manage its AK/SK expiration policies. In addition, should Outscale request a renewal and the Client does not modify its AK/SK rapidly (i.e., within TWENTY-FOUR (24) HOURS following the request) Outscale cannot be held liability for the resulting damages in connection with this failure to proceed with the modification.	-
The Access Keys to the Service are kept in the exclusive care of the Client.	-

13. Cryptography

- Outscale's responsibility

Description	Labels
Outscale implements a policy on the use of cryptographic measures to protect information.	ISO – A10.1.1
Outscale implements a policy for the management of cryptographic keys.	ISO – 10.1.2
Outscale undertakes to follow ANSSI's rules and recommendations on the implementation of cryptographic keys.	SNC – 10.5 a) b)
Outscale protects access to the cryptographic keys and other secrets used for data encryption.	SNC – 10.5 c)
Outscale protects access to the cryptographic keys and other secrets used for administration tasks.	SNC – 10.5 d)
Outscale undertakes to implement an encryption mechanism preventing the recovery of client data in the event of reallocation of a resource or recovery of a physical device.	SNC – 10.1 a)
Outscale undertakes to follow ANSSI's rules and recommendations concerning the choice and extent of the cryptographic mechanisms during use of an electronic signature mechanism.	SNC – 10.1 b) c)
Outscale undertakes to implement data encryption on removable devices and backup devices which may be removed from the physical security perimeter of the information system of the Service in question.	SNC – 10.1 d)
Outscale undertakes to follow ANSSI's rules and recommendations in the implementation of network flow encryption mechanisms.	SNC – 10.2 a) b) c) d) e)
Outscale undertakes to protect, via encryption, communications between the main site and the backup site.	SNC – 12.5 d)
Outscale does not limit the autonomous implementation of disk encryption by the Client.	-
Outscale implements encryption for data flows and data assessed as "sensitive" in the framework of its risk analysis process.	-
Outscale undertakes only to store the hash of user passwords and technical accounts.	SNC – 10.3 a)
Outscale undertakes to follow ANSSI's rules and recommendations in the implementation of a password hashing function.	SNC – 10.3 b) c)
Outscale undertakes to follow ANSSI's rules and recommendations in the generation of hashes of passwords.	SNC – 10.3 d)
The API and Outscale interfaces are maintained in state-of-the-art conditions in terms of cryptography. Outscale uses the following protocols: IPSEC, TLS, SSH. Furthermore, Outscale undertakes to take into consideration the recommendations made in the guides published by l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).	-
Outscale undertakes to follow ANSSI's rules and recommendations in the implementation of electronic signature mechanisms.	SNC – 10.4 a) b)
Outscale implements encryption for data and flows (via VPN) and for data classified as "sensitive" in the context of its risk assessment process.	-
Outscale undertakes to use public key certificates issued by a European Union Member State certification authority.	SNC - 10.6.a

- Client's responsibility

Description	Label
Outscale recommends that the Client encrypts its Data and does not give it the encryption key. The encryption key remains under the Client's responsibility.	-

14. Physical and environmental security

- Outscale's responsibility

Description	Label
Outscale has defined security perimeters to protect the areas containing sensitive or critical information and the means of processing this information.	ISO – 11.1.1 HDS SNC – 11.1
Outscale has implemented all the means and procedures necessary to guarantee the physical and environmental safety of the different zones defined (public, private and sensitive) within the perimeter of the Service.	SNC – 11.1
Outscale has implemented access limitation and access control in these different zones to protect them against unauthorized access, external and environmental threats.	ISO – 11.1.3 SNC -11.1 a
Outscale guarantees that no resource dedicated to the Service or making it possible to access components of the Service will be hosted in zones defined as public.	SNC – 11.1.1
Outscale undertakes to ensure that only authorized personnel can access these zones.	ISO – A11.1.2
Outscale ensures that the zones defined as private are protected against unauthorized access and that this physical access control is based on at least one personal factor such as knowledge of a secret, possession of an object, or biometrics.	SNC – 11.2.1 a)
Outscale undertakes to ensure that physical protection measures against natural disasters, malicious attacks or accidents are applied.	ISO – A11.1.4
Outscale has defined and documented exceptional physical access conditions in the event of an emergency.	SNC – 11.2.1 c)
Outscale has implemented procedures to define working conditions in the secure zones.	ISO – A11.1.5
Outscale has defined and documented the time slots and conditions of access to zones defined as private based on the worker profiles.	SNC – 11.2.1 e)
Outscale undertakes to control and limit access from delivery zones, loading areas or any public zone to information processing zones, in order to avoid any unauthorized access.	ISO – A11.1.6
Outscale has taken steps to isolate access points from delivery or loading zones to zones classified as private and sensitive.	SNC – 11.5
Outscale undertakes to take the steps necessary to secure the electric or telecommunications cables transporting data or required for the information services against any interception or damages.	ISO – A11.2.3 SNC 11.6 a)
Outscale ensures that all equipment is properly maintained to ensure its availability and integrity.	ISO – A11.2.4
Outscale takes steps to ensure that the installation, maintenance and repair conditions for the Service's information system equipment are compatible with confidentiality and availability requirements.	SNC 11.7 a)

Outscale undertakes to take the steps necessary to protect the hardware in order to reduce the risks related to threats, environmental dangers and unauthorized access.	ISO – A11.2.1
Outscale undertakes to take the steps necessary to protect the hardware against power cuts and other disturbances due to breakdowns in general services.	ISO – A11.2.2
Outscale undertakes to implement procedures to manage retired equipment.	ISO – A11.2.5
Outscale undertakes to take steps to guarantee the level of confidentiality and integrity protection for outgoing equipment, recycled hardware and equipment that has not yet been put into use.	SNC 18.1 a)
Outscale undertakes to implement security measures for equipment used outside the premises.	ISO – A11.2.6
Outscale undertakes to implement procedures for the scrapping of hardware containing storage media.	ISO – A11.2.7
Outscale undertakes to implement appropriate protection procedures for unsupervised user hardware.	ISO – A11.2.8
Outscale applies a clear office and locked workstation policy.	ISO – A11.2.9

- Client's responsibility

Description	Label
The Client shall define the physical and environmental measures necessary and applicable, in its organization, for all personnel and equipment, in the use of the Service in order to guarantee the security of the information against unauthorized access, external and environmental threats.	-

15. Security linked to operations

- Outscale's responsibility

Description	Label
Outscale undertakes to document operating procedures, keep them up-to-date and make them accessible to the Outscale staff concerned.	ISO – A12.1.1 SNC – 12.1 a)
Outscale undertakes to monitor changes to the organization, business processes, systems and information processing means with an impact on information security.	ISO – A12.1.2
Outscale undertakes to supervise and adjust the use of resources and make projections as to the extent of resources necessary to guarantee the performance required from the system.	ISO – A12.1.3
Outscale undertakes to separate development, test, and operating environments to reduce the risks of unauthorized access or changes in the operating environments.	ISO – A12.1.4
Outscale undertakes to implement a procedure for the management of changes and to inform the client of all operations that have a negative impact on the security or availability of the Service.	SNC – 12.2 a) b)
Outscale undertakes to implement measures making it possible to physically separate development, test, and production environments.	SNC – 12.3 a)
Outscale undertakes to implement protective measures and awareness campaigns against malicious codes including covering detection, prevention, and recovery measures together with adapted awareness actions.	ISO – 12.2.1 SNC 12.4 a) b)

Outscale undertakes to implement a policy to backup and restore data under its responsibility in order to guarantee the SLAs on the durability of snapshots and object storage, and a procedure to test the recovery of backups.	ISO – 12.3.1 SNC – 12.5 a) c)
Outscale undertakes to implement protective measures for backups, to locate them a sufficient distance away from the main equipment and to apply the same security requirements as for the main site.	SNC – 12.5 b) d)
Outscale has implemented a procedure governing the recovery of data, and to ensure that data recovery operations are logged in a journal.	HDS – 4.4.6.3
Outscale implements an event logging policy.	ISO – 12.4.1 SNC – 12.6 a)
Outscale protects the information logs.	ISO – 12.4.2
Outscale undertakes to ensure the integrity of the logs.	ISO – 12.4.2 HDS – 4.4.6.10P
Outscale undertakes to protect the logs against unlawful access.	ISO – 12.4.2 HDS – 4.4.6.10P
Outscale keeps track of events reported in the logs.	HDS – 4.4.6.10P
Outscale undertakes to keep a trace of events reported in the logs for a minimum period of 6 (six) months.	SNC – 12.6 c)
Outscale undertakes to provide the Client, at the latter's request, with a list of the events concerning it within the limit of the legal conservation period for these data applicable to Outscale.	HDS – 4.4.6.10C SNC – 12.6 d)
Outscale undertakes to keep a log of systems administrator and technical operator activities.	ISO – A12.4.3 SNC – 12.6 b)
Outscale undertakes to generate and collect any event linked to information security.	SNC – 12.6 b)
Outscale transfers events logs to dedicated servers that are separate from the servers that generated them.	SNC – 12.7 c)
Outscale must limit access to the event logs.	SNC – 12.7 d)
Outscale implements time synchronization on a single temporal reference source.	ISO – A12.4.4 SNC – 12.8 a)
Outscale implements time-stamping of each logged event.	SNC – 12.8 b)
Outscale undertakes to protect the logging facilities and logged events against obstruction of their availability, or breach of their integrity or confidentiality.	SNC – 12.7 a)
Outscale undertakes to manage the size of storage space for all equipment, taking account of information systems evolutions.	SNC – 12.7 b)
Outscale undertakes to implement an infrastructure enabling the analysis and correlation of events recorded by the logging system to detect events likely to affect the security of the Service's Information System with daily analysis alarms.	SNC – 12.9 a)
Outscale undertakes to process the alarms triggered by the analysis and correlation of events infrastructure on a daily basis.	SNC – 12.9 c)
Outscale implements a procedure to control the installation of software on the Service's Information System equipment.	SNC – 12.10 a)
Outscale implements a procedure for the management of the configuration of software environments available for the client.	SNC – 12.10 b)
Outscale implements a procedure for the management of technical vulnerabilities.	SNC – 12.11 a) ISO – A12.6.1

Outscale assesses its exposure to these vulnerabilities as part of its risk assessment process and applies adapted risk response measures.	SNC – 12.11 b)
Outscale implements a procedure obliging Outscale administrators to use workstations dedicated exclusively to administration tasks.	SNC – 12.12 b)
Outscale implements stronger measures for workstations used for administration tasks.	SNC – 12.12 b)
Outscale implements a policy to cover the mobility of administrators under its responsibility, including disk encryption and the use of an encrypted tunnel for all administration flows.	SNC – 12.12 c)
Outscale maintains and monitor a capacity plan that takes into account human, technical, financial and information resources.	HDS – 4.3.3.2
Outscale monitors the resource capacity of all its cloud regions.	HDS – 4.3.3.2
Outscale ensures that installations or software updates are deployed and qualified in test environments before commissioning.	HDS – 4.3.2.1
Outscale uses its best endeavors to ensure that changes made to the Outscale Infrastructure are tested and qualified to ensure there is no negative impact on the functioning, performance, and security of the Outscale Infrastructure.	HDS – 4.3.2.1
Outscale implements procedures to control the installation of software on operating systems.	ISO – A12.5
Outscale sets in place rules governing the installation of software by users.	ISO – A12.6.2
Outscale fixes requirements for the audit of information systems.	ISO – A12.7.1

- Client's responsibility

Description	Label
The Client defines the organizational and technical measures necessary to guarantee state-of-the-art deployment and administration of the System, whether acting on its own account or on behalf of a third party.	-
The Client shall familiarize itself with the documentation associated with the Services and the recommendations issued by Outscale in order to guarantee an appropriate, correct and secure use of the Service.	-
The Client shall analyze and manage risks to the System by: - Providing training to those authorized to operate the Services, in particular on cloud computing specificities; - Regularly auditing backups, data integrity and equipment access to the System.	-
The Client shall ensure, if necessary, the capacity of its System to operate nominally from a functional and security standpoint, even in the event of Service degradation, including by adopting the following good practices: - Automate Infrastructure deployment and updating tasks. - Deploy its application redundancy by sharing the load over different Virtual Machines, or Virtual Machines at independent sites. - Ensure backups incrementally by using different storage types or suppliers. - Separate access rights between development, integration, and production environments. - Protect its environments and its application with systems such as Antivirus, WAF, Protection DDoS, etc. - Ensure that direct or indirect software components are subject to a security review and are not exposed to known security flaws.	-

16. Communications security

- Outscale's responsibility

Description	Label
Outscale undertakes to implement a policy for the management and protection of networks.	ISO – A13.1.1
Outscale implements appropriate separation measures: (i) between clients, (ii) between the Service's information systems and the other information systems, (iii) between the technical infrastructure, the equipment necessary for the administration of the Services and the Resources that it hosts.	-
Outscale has defined management requirements applicable to the internal or outsourced Services.	ISO – A13.1.2
Outscale implements network separation.	ISO – A13.1.3
Outscale implements and revises, at least once a year, mapping of the Service's information system.	SNC – 13.1 a) b)
Outscale implements separation measures (logical, physical or via encryption) to isolate the different network flows and filtering, thus only authorizing legitimate connections.	SNC – 13.2 c) d) e)
Outscale implements network surveillance as part of the security incident detection process.	SNC – 13.3 a)
Outscale implements policies and procedures to protect the transfer of information.	ISO – A13.2.1
Outscale ensures that personal data are encrypted before transmission on public networks.	HDS – 4.4.6.6
Outscale has defined agreements on the transfer of information in activities with suppliers.	ISO – A13.2.2
Outscale undertakes to protect information in transit via e-mail.	ISO – A13.2.3
Outscale undertakes to limit the use of paper copies.	HDS – 4.4.6.2
Outscale has defined confidentiality and nondisclosure commitments to maintain the security of information transferred within its organization and towards external entities.	ISO – A13.2.4
Outscale has included a confidentiality clause in its employees' work contracts, and if it uses subcontractors, this requirement also applies to service providers.	HDS – 4.4.6.1

- Client's responsibility

Description	Label
The Client analyzes and manages the risks on virtualized infrastructures installed in the region(s) by: - Deploying state-of-the-art resources to limit access to functional requirements alone; - Using encrypted and/or dedicated links if necessary for communications considered sensitive.	SNC 3.2 b)

17. Security of developments

- Outscale's responsibility

Description	Label
Outscale defines the information security requirements applicable to information systems.	ISO – A14.1.1
Outscale defines and applies rules for software and systems development.	ISO – A14.1.2
Outscale implements, documents, applies secure development rules for software and systems, and trains the staff concerned.	HDS – 4.3.2.1 SNC – 14.1 a) b)
Outscale implements procedures to monitor changes.	ISO – A14.1.2 SNC – 14.2 a)
Outscale implements a procedure to validate changes.	SNC – 14.2 a)
Outscale undertakes to keep a version history of software and systems.	SNC – 14.2 c)
Outscale inspects and tests changes made to Outscale Infrastructures.	ISO – A14.2.3
Outscale implements and documents a procedure to monitor and validate changes before commissioning, and keeps a version history of software and systems and tests them before commissioning.	HDS - 4.3.2.1 SNC – 14.3 a)
Outscale never uses its clients' production data when carrying out tests. Outscale undertakes to request prior authorization from the Client to use its production data to carry out tests and guarantees that the data remain anonymous and confidential.	SNC – 14.7 b)
Outscale ensures that the requirements of the Services are identified prior to the projects and reviewed during the different stages of the project.	HDS – 4.3.1
Outscale ensures that potential financial, organizational, and technical impacts are taken into account when providing new or modified Services. The Client is informed of any modification to the Service and of the actions to be taken if necessary.	HDS – 4.3.1
Outscale shall use its best endeavors to warn clients as early as possible regarding any future modification to elements of the Service if this is likely to result in any loss of functionality for the Client.	SNC - 12.2 d
Outscale ensures that strong authentication and encryption measures are implemented in order to protect and secure information transmitted via application services on public networks.	ISO – A14.1.3ISO
Outscale implements a software package updating policy.	ISO – A12.2.4
Outscale has established systems security engineering principles for the implementation of information systems.	ISO – A14.2.5
Outscale sets up secure development environments.	ISO – A14.2.6 SNC – 14.4 a)
Outscale protects development environments.	SNC – 14.4 b)
Outscale supervises and controls outsourced development activities.	ISO – A14.2.7 SNC – 14.5 a)
Outscale undertakes to carry out security functionality tests during development.	ISO – A14.2.8 SNC – 14.6 a)
Outscale implements test procedures including tasks to be carried out, input data, and expected results, to ensure the integrity of the pre-production test data.	SNC – 14.6 a)
Outscale implements system compliance tests for new information systems, upgrades, and new versions.	ISO – A14.2.9

- Client's responsibility

Description	Label
The Client implements a procedure to manage changes made to its Systems in order to control the impact on data security (availability, integrity, confidentiality, traceability).	SNC- 14.2 a)

18. Relations with suppliers

- Outscale's responsibility

Description	Label
Outscale undertakes to keep an up-to-date list of suppliers involved in the implementation of the Service (host, developer, integrator, archiver, subcontractor, etc.) and indicate their contribution to the Service.	SNC - 15.1 b)
Outscale undertakes to implement a management policy for the Services provided by suppliers.	ISO – A15.1.1
Outscale undertakes to implement, and agree with suppliers, the pertinent information security requirements based on the type of services provided.	ISO – A15.1.2 SNC – 15.2 a)
Outscale undertakes to implement processes and procedures to guarantee the security of information in the framework of the supply chain of products and/or Services with suppliers.	ISO – A15.1.13
Outscale undertakes to contractualize audit clauses with each of the suppliers involved in the supply of the Service allowing a certification body to check that these suppliers comply with SNC label requirements.	SNC – 15.2 b)
Outscale defines and attributes roles and responsibilities relating to the modification or end of contract with suppliers.	SNC – 15.2 c)
Outscale monitors and reviews the Services provided by suppliers.	ISO – A15.2.1 HDS – 4.4.6.12 SNC – 15.3 a)
Outscale implements management of changes made to supplier services.	ISO – A15.2.2 SNC – 15.3 a)
Outscale ensures that changes made to the services provided by suppliers do not result in a decreasing level of security.	HDS - 4.4.6.12 HDS - 4.4.6.13
Outscale undertakes to list subsequent data processors and to inform the Client beforehand in the event of a modification of this list.	HDS - 4.4.4.1 P
Outscale undertakes to fix contractually with the subsequent data processors the technical and organizational measures necessary to meet the personal data protection and security objectives.	HDS – 4.4.6.12
Outscale establishes a list of suppliers involved in the implementation of the Service, and demands from them: - a level of security that is equivalent to the Outscale security policy; - audit clauses allowing a certification body to check the application of the "Cloud computing services providers (SecNumCloud) label requirements," and assess the measures implemented on a regular basis; - a review, at least once a year, of the requirements in terms of confidentiality and nondisclosure commitments.	SNC – 15.1 a)

Outscale undertakes to implement monitoring of changes made by suppliers, and if the changes are likely to affect the level of security of the Service's information system, to inform all clients immediately and take the measures necessary to restore the same level of security as before.	SNC – 15.4 b)
Outscale implements a procedure to revise, at least once a year, the requirements in terms of confidentiality and nondisclosure with respect to suppliers.	SNC – 15.5 a)

- Client's responsibility

Description	Label
The Client must inform Outscale if it does not accept the changes of suppliers which were notified to it.	-

19. Management of incidents

- Outscale's responsibility

Description	Label
Outscale documents and implements an incident management policy defining the responsibilities and procedures in the event of an incident related to information security.	ISO – A16.1.1
Outscale has defined the technical and organizational means necessary to provide a rapid and efficient response to security incidents, and in particular: - Define response times and means of communication for all the clients concerned, - Inform its personnel and the third parties involved in the implementation of the Service regarding the incident reporting and management procedure.	SNC – 16.1 a) b)
Outscale must report events related to information security as rapidly as possible.	ISO – A16.1.2
Outscale must report any confirmed or suspected security breach in the systems or Services.	ISO – A16.1.3
Outscale implements a procedure requiring staff and suppliers involved in the implementation of the Service to report to it any security incident confirmed or suspected as well as any flaw in security.	SNC – 16.2 a)
Outscale implements a procedure to enable any client to report all confirmed or suspected security incidents and security flaws.	SNC – 16.2 b)
Outscale must immediately report: - security incidents and the associated recommendations to limit their impact to clients, giving them the possibility of being notified depending on the severity of the incident, - security incidents to the competent authorities.	SNC – 16.2 c) d)
Outscale must document the assessment of the events and their qualification as security incidents.	ISO – A16.1.4 SNC – 16.3 a)
Outscale documents the assessment of events and their classification as security incidents and shares this information with the Client, at its request or if it is impacted.	SNC – 16.3 a)
Outscale implements a classification of security events including personal data breaches.	SNC – 16.3 b)
Outscale implements response procedures for incidents related to information security.	ISO – A16.1.5
Outscale must notify the client of any personal data breach as soon as it has been brought to its attention.	HDS – 4.4.5.1P
Outscale must notify the French data protection authority, CNIL, concerning any personal data breach if it represents a risk for the rights and liberties of the data subjects.	SNC – 16.1 c)
Outscale undertakes to deal with security incidents until they are solved and inform the clients concerned, and to keep elements of proof relating to security incidents for the legal conservation period.	SNC – 16.4 a) b)
Outscale implements a continuous improvement process and draws lessons from incidents linked to information security.	ISO – A16.1.6 SNC – 16.5 a)
Outscale implements processes for the collection and protection of proof.	ISO – A16.1.7 SNC – 16.6 a)
Outscale undertakes to implement communication channels to report flaws and vulnerabilities. (https://en.outscale.com/reporting-vulnerabilities/)	-

- Client's responsibility

Description	Label
The Client informs Outscale of any confirmed or suspected security incident as well as any security flaw it is aware of within 24 hours by filling out the vulnerability report available on the website: https://en.outscale.com/reporting-vulnerabilities/	SNC 16.2 b)
The Client must ensure supervision of hosted components, in particular applications and data, to detect any loss of data availability, integrity and confidentiality, and must process alerts and incidents according to predefined procedures. These procedures must include informing the service provider in the event of alerts or incidents which could endanger the hosting Services or infrastructure.	SNC 16.2 b

20. Management of business continuity

- Outscale's responsibility

Description	Label
Outscale has determined its information security requirements for the management of business continuity and the management of data recovery after incidents.	ISO – A17.1.1
Outscale implements and maintains processes, procedures, and measures to guarantee the required level of information security continuity.	ISO – 17.1.2 SNC – 17.4
Outscale undertakes to check the information security continuity measures at regular intervals.	ISO – A17.1.3
Outscale has defined the technical and organizational means necessary to ensure business continuity, and in particular: - document and implement technical and organizational means and procedures to guarantee compliance with Service standards, - ensure they remain operational, - restore them, - test them.	HDS – 4.3.3.1 SNC – 17.2 a) 17.3 b)
Outscale places at the client's disposal documented information on its technical infrastructure backup facilities and the means made available to the client to make its own backups in the context of its own continuity as well as how they function.	SNC - 17.5 SNC - 17.6
Outscale undertakes to define internal fail-safe procedures when the hosting Service cannot be provided in normal operation conditions (this does not concern the Client's fail-safe procedures).	-
Outscale undertakes to guarantee the availability of the information processing means.	ISO – A17.2.1
Outscale has defined a retention period for its security policies and operational procedures.	HDS – 4.4.5.2P
Outscale implements a business continuity plan.	HDS – 4.3.3.1 SNC – 17.1 a)
Outscale undertakes to revise its business continuity plan annually, and every time there is a major change that may impact the Service.	SNC – 17.1 b)
To maintain the Cloud infrastructure up-to-date and guarantee the good quality of the Services, hardware maintenance on hypervisors is planned regularly by Outscale in the different Regions. Two weeks before the maintenance operation, an email is automatically sent to the Clients concerned with the list of their Virtual Machines impacted. If the Client has not stopped these Virtual Machines at the time of the maintenance operations, they will be forcibly shut down, which may damage the Client's applications.	-

Outscale may also have to conduct urgent maintenance work, in which case it will use its best endeavors to inform the Client as soon as possible.	

- Client's responsibility

Description	Label
The Client shall implement a business continuity plan for the hosted systems/applications to cater for situations in which the hosting Service is unavailable for a period of time that is incompatible with the needs of its own users. The recovery plan must include: - its own technical resources (premises, facilities) and procedures to restart the systems/applications in the event of extended unavailability; - fail-safe modes allowing users to continue their activities in the event of unavailability then resume them when the hosted systems start up again.	SNC 17.1 a)
The Client acknowledges being informed that Outscale does not make automatic client Data backups and that the Client is the sole responsible for using the facilities placed at its disposal to backup Data and/or the configuration of the System.	SNC - 17.5 - 17. 6 et 19.1 m)

21. Compliance

- Outscale's responsibility

Description	Label
Outscale must identify the legal, regulatory, and contractual requirements that are applicable to the Services provided.	ISO – A18.1.1 SNC – 18.1 a)
Outscale must, depending on its role in processing personal data, justify and document its choice of technical and organizational measures implemented to satisfy personal data protection requirements.	SNC – 18.1 b)
Outscale undertakes to implement an active monitoring of legal, regulatory, and contractual requirements applicable to the Service.	SNC – 18.1 e)
Outscale undertakes to implement appropriate procedures to guarantee compliance with legal, regulatory, and contractual requirements in terms of intellectual property rights and the use of proprietary software.	ISO – A18.1.2
Outscale undertakes to implement appropriate procedures to protect the organization's recordings in order to satisfy legal, regulatory or contractual requirements and support the organization's essential activities.	ISO – A18.1.3
Outscale undertakes to implement appropriate procedures to guarantee the protection of privacy and the protection of personal data in accordance with applicable legislation and regulations, as applicable.	ISO – A18.1.4
Outscale undertakes to provide the procedures and the means to allow its clients to satisfy requests by the data subjects to exercise their rights. The rights covered are those defined by articles 15 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016.	HDS – 4.4.1
Outscale must, depending on its role in processing personal data, justify and document its choice of technical and organizational measures implemented to satisfy personal data protection requirements.	SNC – 18.1 c)

Outscale undertakes to process personal data only upon documented instruction by the client and in accordance with the agreement.	HDS – 4.4.2P
Outscale undertakes not to use the health data that it hosts for any purpose other than the execution of the Services and undertakes not to use them for marketing, advertising, commercial or statistics purposes.	HDS – 4.4.2C
Outscale undertakes to implement a client notification process in the event of a court-ordered seizure unless this notification is prohibited.	HDS – 4.4.2P
Outscale undertakes to keep an up-to-date log of requests for information as well as requests to exercise rights in order to keep track of these requests and their execution.	HDS – 4.4.3P
Outscale undertakes to implement cryptographic measures in accordance with applicable agreements, laws, and regulations.	ISO – A18.1.5
Outscale undertakes to make the procedures applicable to the Services available to the Client upon request.	SNC – 18.1 d)
Outscale undertakes to review the security requirements defined in the policies, standards, and regulations applicable on a regular basis.	ISO – 18.2.2
Outscale undertakes to conduct regular reviews of the information systems to ensure compliance with the organization's information security policies and standards.	ISO – 18.2.3
Outscale undertakes to have regular and independent reviews of information security carried out.	ISO – 18.2.1
Outscale undertakes to implement an audit program in line with change management, the policies implemented, and the results of risk assessment.	SNC – 18.2 a)
Outscale undertakes to cover in its audit program: the audit of the configuration of the servers and network facilities; intrusion testing, external and internal access testing; code audit.	SNC – 18.2 a) b)
Outscale undertakes to have an annual audit performed by a certified PASSI (audit of information system security) service provider.	SNC – 18.2 b)
Outscale undertakes to communicate the certification audit reports for the scope of health data hosting to any clients who request them.	HDS – 4.5.3
Outscale undertakes to provide certification audit reports to the certification body, in the event of a transfer or equivalence request.	HDS – 4.5.3
Outscale ensures the correct execution of all the security procedures and their compliance with security policies and standards.	SNC – 18.5 a)
Outscale implements and documents a technical compliance policy.	SNC – 18.5 b)

- Client's responsibility

Description	Label
The Client must inform Outscale if data subjected to specific legal, regulatory, or sector-based requirements are entrusted to it (in particular relating to vital organisms, banking data, health data, information systems of vital importance (SIIV), etc.).	-
The Client must implement adequate procedures, in the framework of the use of the Services, to enable legal, regulatory, and contractual requirements to be met.	-
Data transfers carried out by the Client are under its responsibility alone.	-
The Client is informed that it must implement a health information system that complies with the General Security Policy for Health Information Systems (PGSSI-S) drawn up by the health information systems strategy delegation (DSSIS) of the French Ministry for social	HDS – 4.5.2

affairs and healthcare and the Shared Healthcare Information Systems Agency (ASIP Santé) and its binding Labels such as defined in the laws and regulations.	
The Client undertakes to comply with the General Security Policy for Health Information Systems (PGSSI-S) and the related labels.	HDS – 4.5.2
The Client must ensure that laws applicable to the Services are respected, in strict compliance with the provisions effectively applicable to the Client.	-
The Client must ensure that all current regulations applicable to its Data (and in particular personal data, health data, banking data, obligations applicable to Organisms of Vital Importance (OIV) etc.) are complied with.	-
If the Client operates a website open to the public, the Client must ensure that it complies with the legal obligations in this respect.	-