Ref. §	Requirement text
1.3.2.	The role of infrastructure administrator is always the responsibility of the service provider. Depending on the method of sharing responsibilities between the service provider and the commissioning entity described in the service agreement, roles of security administrator, system administrator, network administrator, etc. may be under the responsibility of the service provider or that of the sponsor.
2.3.	This service provides runtime environments for the deployment and orchestration of containers. The commissioning entity does not have control of the underlying technical infrastructure (network, storage, servers, operating system), managed and controlled by the service provider. However, the sponsor has mastery of system tools, libraries, middleware, and application code.
3.3.2.	(…) The assessment of compliance with these additional requirements is not part of the criteria for the SecNumCloud qualification of the service provider's offer. It must be taken into account by the commissioning entity in a risk assessment process for its own IS before using the services of the service provider.
4.	(…) The use, by the sponsor, of a qualified SecNumCloud service for data hosting subject to legal or regulatory requirements (such as Restricted data, health data, etc.) requires the assessment of additional requirements to be carried out by the sponsor as part of an approval process (see chapter 3.3.2.) including in particular a risk assessment.
5.1.a	The provider must perform the state of the art service for the type of activity chosen: use stable software with monitoring of security patches and set up in order to obtain an optimal level of security.
5.1.b	The provider must apply the ANSSI [HYGIENE], reinforced level, computer hygiene guide to the service's information system
5.2.a	The provider must document and implement a service information security policy
5.2.b	The information security policy must identify the commitments of the provider regarding compliance with the national legislation and regulations in force according to the nature of the information that could be entrusted by the sponsor to the provider; however, it is ultimately up to the sponsor to ensure compliance with legal and regulatory constraints applicable to the data it actually entrusts to the provider.
5.2.c	The information security policy should cover, in particular, the topics covered in Chapters 6 to 19 of this repository
5.2.d	Provider management must formally approve the information security policy
5.2.e	The provider must review the information security policy annually and each major change that may have an impact on the service
5.3.a	The provider must document a risk assessment covering the entire scope of the service
5.3.b	The provider must carry out his risk assessment using a documented method guaranteeing the reproducibility and comparability of the approach
5.3.c	The provider must take into account in the risk assessment:
	- Managing Sponsor's information with different security needs;
	- risks affecting the rights and freedoms of data subjects in the event of unauthorised access, unwanted modification and disappearance of personal data;
	- the risk of failure of the partitioning mechanisms of the technical infrastructure resources (memory, compute, storage, network) shared between sponsors;
	- the risks associated with incomplete or insecure erasure of data stored on shared memory or storage spaces between sponsors, particularly when reallocating memory and storage spaces
	- the risks associated with exposure of administrative interfaces on a public network.
	- the risks of breach of the confidentiality of sponsor data by third parties involved in the provision of the service (suppliers, subcontractors, etc.).
5.3.d	The service provider must list, in a specific document, the residual risks associated with the existence of extraterritorial laws aimed at collecting data or metadata from commissioners without their prior consent.

5.3.e	The service provider must make available to the commissioning entity, at the latter's request, the elements for assessing the risks associated with submitting the commissioning party's data to the law of a non-member state of the European Union.
5.3.f	Where there are specific legal, regulatory or sectoral requirements related to the types of information entrusted by the sponsor to the provider, the provider must take them into account in its risk assessment by ensuring that all the requirements of this repository are met on the one hand and not to lower the level of security established by compliance with the requirements of this repository on the other hand.
5.3.g	The management of the provider must formally accept the residual risks identified in the risk assessment
5.3.h	The provider must review the risk assessment annually and each major change that may have an impact on the service
6.1.a	The provider must document and implement an internal security organization to ensure the definition, implementation and monitoring of the operational functioning of information security within his organization
6.1.b	The provider must designate an information system security officer and a physical security officer
6.1.c	The provider must define and assign information security responsibilities for the personnel involved in the provision of the service
6.1.d	The provider must ensure after any major changes that may have an impact on the service that the assignment of information security responsibilities is always relevant
6.1.e	The provider must define and assign responsibilities for the protection of personal data, consistent with its role in the processing of personal data (controller, processor or co-controller).
6.1.f	When processing a large number of data including particular categories of personal data as defined in [GDPR], the provider must appoint a Data Protection Officer
6.1.g	It is recommended that the provider, regardless of the volume of personal data it processes, appoint a Data Protection Officer.
6.1.h	The provider must carry out or contribute to the carrying out of an impact assessment relating to the protection of personal data when the processing is likely to create a high risk to the rights and freedoms of the data subjects (processing of particular categories of personal data as defined in [GDPR], large-scale data processing, etc.). This analysis should include a legal assessment of respect for fundamental principles and rights, as well as a more technical study of the technical measures implemented to protect individuals from risks to their privacy
6.2.a	The provider must identify risks associated with cumulative responsibilities or tasks, take them into account in risk assessment and implement measures to reduce these risks
6.3.a	It is recommended that the provider establish appropriate relations with the competent information security and personal data authorities and, where appropriate, with sectoral authorities depending on the nature of the information entrusted by the sponsor to the provider
6.4.a	It is recommended that the provider maintain appropriate contacts with groups of specialists or recognized sources, including to take into account new threats and appropriate security measures to counter them
6.5.a	The provider must document a risk estimate prior to any project that may have an impact on the service, regardless of the nature of the project
6.5.b	To the extent that a project affects or is likely to affect the level of security of the service, the provider must notify the Sponsor and inform the Sponsor in writing of the potential impacts, the measures put in place to reduce these impacts and of the residual risks affecting it
7.1.a	The Service Provider shall document and implement a procedure for verifying information concerning its personnel in accordance with the laws and regulations in force. These checks apply to anyone involved in the provision of the service and must be proportional to the sensitivity or specificity of the sponsor's information entrusted to the provider and to the risks identified
7.1.b	The service provider must reinforce these checks when it comes to staff with elevated administrative privileges on software and hardware components of the infrastructure of the service. It is understood by elevated administrative privileges, actions allowing the elevation of privileges or the possibility of carrying out actions without technical traces or deactivate, alter technical traces.
7.2.a	The service provider must have an ethical charter integrated into the internal rules, providing in particular that:

	- the services are carried out with loyalty, discretion, impartiality and confidentiality of the processed information;
	- staff use only the methods, tools and techniques validated by the provider;
	- the staff undertake not to disclose any information to a third party, even anonymized and decontextualized, obtained or generated as part of the service unless the sponsor's formal and written permission;
	- the staff undertake to report to the provider any manifestly illegal content discovered during the service;
	- staff undertake to comply with existing national legislation and regulations and good practices related to their activities.
7.2.b	The provider must have the ethics charter signed by all persons involved in the provision of the service.
7.2.c	The service provider must introduce, in the employment contract of personnel with high administrative privileges on the components and equipment of the service infrastructure, a commitment of responsibility with a reference to the clauses of the labor code on the protection of confidentiality. business and intellectual property. It is understood by elevated administrative privileges, actions allowing elevation of privileges or the possibility of performing actions without technical traces or to deactivate, alter technical traces.
7.2.d	The provider must, at the request of a sponsor, make the rules of procedure and the charter of ethics accessible to him
7.3.a	The provider must raise awareness of information security and data protection risks to all persons involved in the provision of the service. They must provide them with updates to relevant policies and procedures for their missions.
7.3.b	The provider must document and implement an information security training plan adapted to the service and missions of staff.
7.3.c	The provider's information system security officer must formally validate the information security training plan
7.4.a	The provider must document and implement a disciplinary process applicable to all persons involved in the provision of the service who violated the security policy.
7.4.b	The provider must, at the request of a sponsor, make it accessible to him the penalties incurred in the event of a breach of the security policy
7.5.a	The provider shall define and assign roles and responsibilities relating to the termination, termination or modification of any contract with a person involved in the provision of the service
8.1.a	The provider must keep up to date the inventory of all equipment implementing the service. This inventory shall specify for each equipment:
	- equipment credentials (name, IP address, MAC address, etc.)
	- the function of the equipment;
	- the model of the equipment;
	- the location of the equipment;
	- the owner of the equipment;
	- the need for security of information (as defined in Chapter 8.3).
8.1.b	The provider must keep up to date the inventory of all software implementing the service. This inventory must identify for each software, its version and the equipment on which the software is installed.
8.1.c	The provider must ensure that software licenses are valid throughout the service
8.2.a	The claimant must document and implement a procedure for the return of assets to ensure that each person involved in the provision of the service returns all assets in his possession at the end of his period of employment or contract
8.3.a	The provider must identify the different security needs of the service information.
8.3.b	When the Sponsor entrusts the provider with data subject to specific legal, regulatory or sectoral constraints, the provider must identify the specific security needs associated with these constraints
8.4.a	It is recommended that the provider document and implement a procedure for marking and handling all information involved in the delivery of the service, in accordance with its security requirement as defined in Chapter 8.3
8.5.a	The provider shall document and implement a procedure for the management of removable media in accordance with the security need defined in Chapter 8.3.

8.5.b	When removable media are used on the technical infrastructure or for administrative tasks, these media must be dedicated to use.
9.1.a	The provider must document and implement an access control policy based on the result of his risk assessment and shared responsibility.
9.1.b	The provider must review the access control policy annually and each major change that may have an impact on the service
9.2.a	The provider must document and implement a user registration and unsubscribe procedure based on an account management interface and access rights. This procedure should indicate which data should be deleted from a user.
9.2.b	The provider must assign registered accounts when registering users under his responsibility.
9.2.c	The provider must implement means to ensure that the unsubscribing of a user leads to the deletion of all his/her access to the resources of the service's information system, as well as the deletion of his data in accordance with the registration and unsubscribe procedure (see requirement 9.2 .
9.3.a	The provider must document and implement a procedure to ensure the allocation, modification and removal of access rights to resources from the service's information system.
9.3.b	The provider must make available to the Sponsor the tools and means that allow a differentiation of the roles of the users of the service, for example according to their functional role.
9.3.c	The provider must keep up to date the inventory of users under his responsibility who have administrative rights over the resources of the service's information system.
9.3.d	The provider must be able to provide, for a given resource implementing the service, a list of all users who have access to it, whether under the responsibility of the provider or sponsor and the rights of access granted to them.
9.3.e	The provider must be able to provide, for a given user, whether under the responsibility of the provider or sponsor, a list of all his/her access rights to the various elements of the service information system.
9.3.f	The provider must define a list of access rights that are incompatible with each other. When assigning access rights to a user, the user must ensure that he does not have access rights that are incompatible with each other under the previously established list.
9.3.g	The provider must include in the access rights management procedure actions to revoke or suspend the rights of any user
9.4.a	The provider must review the user's access rights on its perimeter of responsibility annually.
9.4.b	The provider must make available to the Sponsor a tool to facilitate the review of the access rights of users under the responsibility of the sponsor.
9.4.c	The provider shall review quarterly the list of users within its scope of responsibility that may use the technical accounts referred to in requirement 9.2
9.5.a	The provider must formalize and implement procedures for managing user authentication. In accordance with the requirements of Chapter 10, these shall include:
	- management of authentication means (issuing and resetting password, updating CRLs and import root certificates when using certificates, etc.)
	- the establishment of means for multi-factor authentication in order to respond to the different use cases of the repository.
	- systems that generate passwords or verify their robustness, when password authentication is used. They should follow the recommendations of [NT_MDP].
9.5.b	Any authentication mechanism must provide for an account to be blocked after a limited number of unsuccessful attempts.
9.5.c	As part of a SaaS service, the provider must offer the Sponsor multi-factor authentication methods for end-user access.
9.5.d	Where technical, non-nominative accounts are required, the provider must put in place measures requiring users to authenticate with their registered account before they can access these technical accounts.
9.6.a	Administration accounts under the responsibility of the Provider must be managed using tools and directories separate from those used to manage user accounts under the responsibility of the Sponsor.
9.6.b	The administration interfaces made available to the Sponsor must be separate from the administration interfaces used by the provider.

9.6.c	The administration interfaces made available to the Sponsor shall not allow any connection to administrator accounts under the responsibility of the provider.
9.6.d	The administration interfaces used by the provider must not be accessible from a public network and thus shall not allow any user connection under the responsibility of the Sponsor.
9.6.e	If administrative interfaces are made available to the Sponsor with access via a public network, administration flows must be authenticated and encrypted with means consistent with the requirements of Chapter 10.2.
9.6.f	The provider must set up a dual factor authentication system for access:
	- the administrative interfaces used by the provider;
	- to sponsor administration interfaces.
9.6.g	As part of a SaaS service, the administration interfaces made available to sponsors must be differentiated from end-user access interfaces.
9.6.h	Once an administrative interface is accessible from a public network, the authentication process must take place before any interaction between the user and the interface in question.
9.6.i	When the provider uses an IaaS service as the basis of another type of service (CaaS, PaaS or SaaS), the resources allocated for the use of the provider shall in no case be accessible via the public interface made available to other IaaS sponsors.
9.6.j	When the service provider uses a CaaS type service as the basis for another type of service (PaaS or SaaS), the resources allocated to the use of the service provider must under no circumstances be accessible via the public interface made available to other service sponsors CaaS.
9.6.k	When the provider uses a PaaS service as the basis for another type of service (typically SaaS), the resources allocated for the use of the provider must in no way be accessible via the public interface made available to the other PaaS sponsors.
9.7.a	The provider must implement appropriate silos between its sponsors.
9.7.b	The provider must implement appropriate partitioning measures between the service's information system and its other information systems (office automation, management information technology, building technical management, physical access control, etc.).
9.7.c	The provider must design, develop, configure and deploy the service information system, ensuring at least a partitioning between the technical infrastructure and the equipment necessary for the administration of the services and resources it hosts
9.7.d	In the context of technical support, if the actions necessary to diagnose and resolve a problem encountered by a commissioning entity require access to the data of the commissioning entity, then the service provider must:
	- authorize access to the data of the sponsor only after the explicit consent of the sponsor;
	- verify that the person to whom access must be authorized has satisfied the verifications of requirement 7.1.a) relating to the sensitivity or specificity of the commissioning entity's data;
	- check that the person to whom access must be authorized is located within the European Union;
	- in the case of an intervention carried out remotely by a person who has not satisfied the verifications of requirement 7.1.a), implement a secure gateway (bounce station) through which the person must connect and allow supervision (authorization or prohibition of actions, requesting explanations, etc.) in real time, by a person who himself has satisfied the verifications of requirement 7.1.a);
	- consider the actions carried out, once access is authorized, as administrative actions and log them as such;
	- remove the data access authorization of the commissioning entity at the end of these actions.
10.1.a	The provider must define and implement an encryption mechanism that prevents the recovery of Sponsor data in the event of a resource reallocation or recovery of physical media.
	- For example, in the case of an IaaS service, this objective can be achieved:
	- by disk or filesystem encryption, where the file-mode access protocol ensures that only empty blocks can be allocated (e.g. NAS storage where a physical block is actually affected only at the time of writin
	- Volume encryption for block access (e.g. SAN storage or local storag, with at least one key per sponsor;
	- in the case of a PaaS or SaaS service, this objective can be achieved by using application encryption within the provider's perimeter, with at least one key per sponsor
10.1.b	The provider must use a data encryption method that complies with [CRYPTO_B1] rules.

10.1.c	It is recommended that you use a data encryption method that meets the recommendations of [CRYPTO_B1].
10.1.d	The provider shall implement encryption of the data on removable media and backup media required to leave the physical security perimeter of the service's information system (as defined in Chapter 11), depending on the need for data security (see Chapter 8.3).
10.2.a	When the provider implements a network stream encryption mechanism, it must comply with the rules of [CRYPTO_B1].
10.2.b	When the provider implements a network stream encryption mechanism, it is recommended that it adhere to the recommendations of [CRYPTO_B1].
10.2.c	If TLS is implemented, the provider must apply [NT_TLS] recommendations.
10.2.d	If IPsec is implemented, the provider must apply [NT_IPSEC] recommendations.
10.2.e	If SSH is implemented, the provider must apply [NT_SSH] recommendations
10.3.a	The provider must store only the fingerprint of user passwords and technical accounts.
10.3.b	The provider must implement a hash function that complies with [CRYPTO_B1] rules.
10.3.c	It is recommended that the provider implement a hash function that meets the recommendations of [CRYPTO_B1].
10.3.d	The provider must generate passwords fingerprints with a hash function associated with using a cryptographic salt that complies with the rules of [CRYPTO_B1].
10.4.a	When the provider implements an electronic signature mechanism, it must comply with the rules of [CRYPTO_B1].
10.4.b	When the provider implements an electronic signature mechanism, it is recommended that it adhere to the recommendations of [CRYPTO_B1].
10.5.a	The provider must implement cryptographic keys that comply with [CRYPTO_B2] rules.
10.5.b	It is recommended that the provider implement cryptographic keys that comply with the recommendations of [CRYPTO_B2].
10.5.c	The provider must protect access to cryptographic keys and other secrets used for data encryption by an appropriate means: security container (software or hardwar or disjointed media.
10.5.d	The provider must protect access to cryptographic keys and other secrets used for administration tasks by a suitable security container, software or hardware.
10.6.a	On the technical infrastructure, the service provider must only use key certificates public from a certification authority of a member state of the European Union (the master key generation ceremonies must take place in a member country of the European Union and in the presence of the service provider).
11.1.a	The provider must document and implement security perimeters, including the marking of zones and the various means of limitation and control of access.
11.1.b	The provider must distinguish between public, private and sensitive areas.
11.1.1.a	Public areas are accessible to all within the limits of the property of the provider. The provider shall not host any resources dedicated to the service or to access components thereof in public areas.
11.1.2.a	Private areas may host:
	- platforms and means of service development;
	- administrative, operational and supervisory positions;
	- the premises from which the provider operates.
11.1.3.a	Sensitive areas are reserved for hosting the service's production information system away from administrative, operational and supervisory posts
11.2.1.a	The provider must protect private areas from unauthorized access. To do so, it must implement a physical access control based on at least one personal factor: knowledge of a secret, the possession of an object or biometrics.
11.2.1.b	It is recommended that the provider adhere to [G_SANSCONTACT]'s recommendations to implement physical access control.
11.2.1.c	The provider must define and document derogatory physical access measures in the event of an emergency.
11.2.1.d	The provider must display at the entrance of private areas a warning regarding the limits and conditions of access to these zones.
11.2.1.e	The provider must define and document the time ranges and conditions of access to private areas according to the profiles of the stakeholders.

11.2.1.f	The provider must document and implement the means to ensure that visitors are systematically accompanied by the provider during their access and stay in private areas. The provider must keep a record of the identity of the visitors in accordance with the laws and regulations in force.
11.2.1.g	In the event of an intervention (diagnostic, maintenance or administration actions) in the area private by a third-party visitor, the service provider must supervise (monitor, authorize, prohibit, question) actions by personnel who have satisfied the verifications of requirement 7.1.a.
11.2.1.h	The provider must document and implement mechanisms for monitoring and detecting unauthorized access to private areas
11.2.2.a	The provider must protect sensitive areas from unauthorized access. To do so, it must implement a physical access control based on at least two personal factors: knowledge of a secret, the possession of an object or biometrics.
11.2.2.b	It is recommended that the provider adhere to [G_SANSCONTACT]'s recommendations for the implementation of physical access control.
11.2.2.c	The provider must define and document derogatory physical access measures in the event of an emergency.
11.2.2.d	The provider must display at the entrance of the sensitive areas a warning regarding the limits and conditions of access to these areas.
11.2.2.e	The provider must define and document the time ranges and conditions of access to sensitive areas according to the profiles of the stakeholders.
11.2.2.f	The provider must document and implement the means to ensure that visitors are systematically accompanied by the provider when accessing and stays in sensitive areas. The provider must keep a record of the identity of the visitors in accordance with the laws and regulations in force.
11.2.2.g	In the event of an intervention (diagnostic, maintenance or administration actions) in the area private by a third-party visitor, the service provider must supervise (monitor, authorize, prohibit, question) actions by personnel who have satisfied the verifications of requirement 7.1.a.
11.2.2.h	The provider must document and implement mechanisms for monitoring and detecting unauthorized access to sensitive areas.
11.2.2.i	The provider must set up a logging of physical access to sensitive areas. He must conduct a review of these newspapers at least monthly.
11.2.2.j	The provider must implement the means to ensure that no direct access exists between a public area and a sensitive area.
11.3.a	The provider must document and implement the means to minimize the risks inherent in physical (fire, water damage, etc.) and natural (climate hazards, floods, earthquakes, etc.).
11.3.b	The provider must document and implement measures to limit the risk of fire departure and spread as well as the risk of water damage.
11.3.c	The provider shall document and implement measures to prevent and limit the consequences of a power supply outage and allow a resumption of service in accordance with the service availability requirements set out in the service agreement.
11.3.d	The provider must document and implement the means to maintain temperature and humidity conditions adapted to the equipment. In addition, it must implement measures to prevent and limit the consequences of air conditioning failures.
11.3.e	The provider must document and implement regular checks and tests of detection and physical protection equipment.
11.4.a	The provider must incorporate the physical security elements into the security policy and risk assessment in accordance with the level of security required by the category of the zone.
11.4.b	The provider must document and implement procedures relating to work in private and sensitive areas. It must communicate these procedures to the relevant stakeholders.
11.5.a	Delivery and loading areas and other points through which unauthorized persons can enter the premises without being accompanied are considered public areas. The provider shall isolate access points from these areas to private and sensitive areas, in order to avoid unauthorized access, or, failing that, implement countervailing measures to ensure the same level of security.
11.6.a	The provider must document and implement measures to protect electrical and telecommunications wiring from physical damage and interception possibilities.
11.6.b	The claimant must establish and maintain a wiring plan.

11.6.c	It is recommended that the provider implement measures to identify cables (e.g. colour coding, label, etc.) in order to facilitate their operation and to limit handling errors.
11.7.a	The provider shall document and implement measures to ensure that the conditions for installation, maintenance and maintenance of the service information system equipment hosted in private and sensitive areas are compatible with the confidentiality and availability requirements of the service defined in the service.
11.7.b	The provider must subscribe to maintenance contracts to provide security updates for software installed on the equipment of the service's information system.
11.7.c	The Provider shall ensure that the media can only be returned to a third party if the Sponsor's data is stored in it encrypted in accordance with Chapter 10.1 or has been previously destroyed using a secure erasure mechanism by rewriting random patterns.
11.7.d	The provider must document and implement measures to ensure that the conditions for installation, maintenance and maintenance of ancillary technical equipment (power supply, air conditioning, fire, etc.) are compatible with the service availability requirements set out in the service agreement.
11.8.a	The Provider shall document and implement a procedure for offsite transfer of Sponsor's data, hardware and software. This procedure must require written authorization from the management of the provider. In all cases, the provider must implement the means to ensure that the level of confidentiality and integrity protection of assets during transport is equivalent to that on site.
11.9.a	The Provider shall document and implement means to erase securely by rewriting random patterns of any data medium made available to a sponsor. If the storage space is encrypted as part of requirement 10.1 (, the erasure can be achieved by a secure erasure of the encryption key
11.10.a	The Provider shall document and implement a procedure for the protection of pending equipment
12.1.a	The provider must document the operating procedures, keep them up to date and make them accessible to the personnel concerned
12.2.a	The provider must document and implement a procedure for managing changes to information processing systems and means.
12.2.b	The provider must document and implement a procedure allowing, in the event of operations carried out by the provider and which may have an impact on the security or availability of the service, to communicate the following information to all its sponsors as soon as possible:
	- the scheduled date and time of the start and end of operations;
	- the nature of the transactions;
	- the impacts on the security or availability of the service;
	- the contact within the provider
12.2.c	As part of a PaaS service, the provider must inform the Sponsor as soon as possible of any future changes to software elements under its responsibility as soon as full compatibility cannot be ensured.
12.2.d	The Provider must inform Sponsor as soon as possible of any future changes to the service elements if it is likely to result in a loss of functionality to the Sponsor
12.3.a	The provider must document and implement the measures of physical separation of the environments based on the service production from the other environment, of which the development environment
12.4.a	The provider must document and implement detection, prevention and recovery measures to protect themselves from malicious codes. The scope of application of this requirement on the service information system must necessarily contain the user stations under the responsibility of the provider and the incoming flows on the same information system.
12.4.b	Providers must document and implement employee awareness of the risks associated with malicious codes and best practices to reduce the impact of infection
12.5.a	The provider must document and implement a data backup and recovery policy under its responsibility as part of the service. This policy must provide for a daily backup of all data (information, software, configurations, etc.) under the responsibility of the service provider.
12.5.b	The provider must document and implement safeguard safeguards in accordance with the Access Control Policy (see Chapter 9). This policy should provide for a monthly review of access to backups.
12.5.c	The provider must document and implement a procedure to regularly test the recovery of backups.
12.5.d	The provider must locate the backups at a sufficient distance from the main equipment consistent with the results of the risk assessment and to deal with major claims. Backups are subject to the same location requirements as operational data. The backup site (s) are subject to the same security requirements as the primary site, in particular those listed in Chapters 8 and 11. Communications

	between primary and backup sites must be encrypted in accordance with the requirements of Chapter 10
12.6.a	The provider must document and implement a logging policy including at least the following:
	- a list of sources of collection;
	- List of events to log by source
	- The object of the event logging
	- frequency of collection and time base used;
	- the duration of local and centralized retention;
	- measures to protect logs (including encryption and duplication);
	- the localization of the logs.
12.6.b	The provider must generate and collect the following events:
	- User activities related to information security;
	- the modification of access rights within the scope of its responsibility;
	- events arising from anti-malicious code mechanisms (see 12.4);
	- Exceptions;
	- failures;
	- any other information security events.
12.6.c	The provider must keep the events resulting from the logging for a minimum period of six months subject to compliance with legal and regulatory requirements.
12.6.d	The provider must provide, upon request of a sponsor, all events relating to him.
12.6.e	It is recommended that the logging system set up by the provider follow the recommendations of [NT_JOURNAL].
12.7.a	The service provider shall protect logging equipment and logged events against breaches of their availability, integrity or confidentiality, in accordance with Chapter 3.2 of
12.7.b	The provider must manage the sizing of the storage space of all equipment hosting one or more collection sources in order to allow the local retention of logged events provided for in the event logging policy. This design management must take account of developments in the information system.
12.7.c	The provider must transfer the logged events with confidentiality and integrity protection to one or more dedicated central servers and must store them on a physical machine separate from the one that generated them.
12.7.d	The provider must put in place a safeguard of collected events according to an appropriate policy.
12.7.e	The provider must execute logging and event collection processes with accounts with sufficient privileges and must limit access to logged events in accordance with the access control policy (see Chapter 8).
12.8.a	The provider must document and implement a synchronization of the clocks of all equipment on one or more internal time sources that are consistent with each other. These sources can themselves be synchronized to several external reliable sources, except for isolated networks.
12.8.b	The provider must set up the timestamp for each logged event
12.9.a	The provider shall document and implement an infrastructure for the analysis and correlation of events recorded by the logging system in order to detect events that may affect the security of the service's information system, either in real time or ex post facto for events dating back to up to six months.
12.9.b	It is recommended that the Security Incident Detection Provider Requirements Repository (PDIS) be used to implement and operate the event analysis and correlation infrastructure.
12.9.c	The provider must pay the alarms lifted by the event analysis and correlation infrastructure at least daily
12.10.a	The provider must document and implement a procedure for controlling the installation of software on the equipment of the service information system.
12.10.b	The Provider shall document and implement a procedure for managing the configuration of software environments made available to the Sponsor, in particular to maintain them in a secure condition
12.10.c	The service provider must provide a capacity for inspection and removal, if necessary, of inbound (checking the authenticity and harmlessness of updates, verifying the harmlessness of tools provided, etc.) relating to the scope of the technical infrastructure:
	- this inspection and removal capability must generate activity logs and must be able to undergo a code audit,

	- entrants must be treated on specific systems operated and maintained by the provider and hosted in an area separated from the rest of the infrastructure.
12.11.a	The provider must document and implement a monitoring process to manage technical vulnerabilities in software and systems used in the service information system.
12.11.b	The provider must assess their exposure to these vulnerabilities by including them in the risk assessment and apply appropriate risk treatment measures.
12.12.a	The Provider shall document and implement a procedure requiring administrators under his responsibility to use dedicated terminals for the exclusive performance of administrative tasks, in accordance with Chapter 4.1 entitled “Control of the Administrative Position” of [NT_ADMIN]. He must master them and keep them up to date.
12.12.b	The provider must implement measures to tighten the configuration of the endpoints used for administrative tasks, including those in Chapter 4.3 entitled “Administration Station Security Measures” of [NT_ADMIN].
12.12.c	Where the provider authorizes a mobility situation for directors under his or her responsibility, it must be guided by a documented policy. The solution implemented must ensure that the level of security of this mobility situation is at least equivalent to the level of security outside of mobility (see Chapters 9.6 and 9.7). This solution should include, among other things:
	- the use of a non-disconnecting and non-bypassing encrypted tunnel for all flows (see Chapter 10.2);
	- Full disk encryption (see Chapter 10.1).
12.13.a	In the context of remote diagnostics or remote maintenance of infrastructure components, considering the risks to the confidentiality of the data of the sponsors, then the service provider must:
	- verify that the person to whom access is to be authorized has satisfied the verifications of requirement 7.1.a with respect to the sensitivity or specificity of the commissioner's data;
	- check that the person to whom access must be authorized is located within the European Union;
	- in the case of an intervention carried out by a person who has not satisfied the verifications of requirement 7.1.a, implement a secure gateway (bounce station) through which the person must connect and allow supervision of the actions (authorization or prohibition of actions, request for explanations, etc.) in real time, by a person who himself has satisfied the verifications of requirement 7.1.a;
	- consider actions taken, once access is granted, as administrative actions and log them as such.
	- remove the access authorization at the end of the intervention.
12.14.a	The service provider must provide a capacity for inspection and removal of outgoing technical infrastructure relating to the scope of the service (billing information, any logs required for handling incidents, etc.):
	- departures must be able to be redacted from data that could undermine the confidentiality of the data of the sponsors;
	- this inspection and deletion capability must generate activity logs and must be able to be the subject of a code audit;
	- Outgoing employees are treated on specific devices operated and maintained by the service provider, and hosted in an area separated from the rest of the infrastructure.
13.1.a	The provider shall prepare and maintain a mapping of the service's information system in relation to the inventory of assets (see Chapter 8.1 , including at least the following:
	- a list of hardware or virtualized resources
	- the names and functions of the applications, supporting the service
	- the network architecture diagram at level 3 of the OSI model on which the hotspots are identified:
	- points of interconnection, in particular with third party and public networks,
	- networks, subnets, including administrative networks,
	- equipment providing security functions (filtering, authentication, encryption, etc.),
	- servers hosting data or performing sensitive functions;
	- the matrix of authorized network flows by specifying:
	- their technical description (services, protocols and ports);
	- business or technical infrastructure justification;
	- where appropriate, where deemed unsafe services, protocols or ports are used, the compensatory measures put in place, in the defence-in-depth logic.
13.1.b	The claimant must review the mapping at least annually

13.2.a	The provider must document and implement, for the service information system, silos measures (logical, physical or encryption) to separate network flows according to:
	- sensitivity of the information transmitted;
	- the nature of the flows (production, administration, supervision, etc.)
	- the area of ownership of the flows (sponsors — with distinction per sponsor or group of sponsors, the provider, third parties, etc.); - the technical field (processing, storage, etc.).
13.2.b	The provider must partitioning, physically or by encryption, all data flows internal to the service's information system vis-à-vis any other information system. When this partitioning is carried out by encryption, it shall be carried out in accordance with the requirements of Chapter 10.2.
13.2.c	In the event that the technical infrastructure administration network is not physically partitioned, the administration flows shall pass through an encrypted tunnel, in accordance with the requirements of Chapter 10.2.
13.2.d	Provider must set up and configure an application firewall to protect the administration interfaces intended for its sponsors and exposed on a public network.
13.2.e	The service provider shall implement a filtering mechanism on all administrative and supervisory interfaces of the service's technical infrastructure that allows only legitimate connections identified in the authorized flow matrix.
13.3.a	The provider must have one or more security incident detection probes on the service's information system. These probes shall, in particular, allow for the supervision of each of the interconnections of the service's information system with third party information systems and public networks. These probes shall be sources of collection for the event analysis and correlation infrastructure (see Chapter 12.9).
14.1.a	The provider must document and implement rules for the secure development of software and systems, and apply them to internal developments.
14.1.b	The provider must document and implement appropriate training in secure development to the employees concerned.
14.2.a	The provider must document and implement a procedure for monitoring changes to the service's information system.
14.2.b	The provider must document and implement a procedure for validating changes to the service information system on a pre-production environment before they are put into production.
14.2.c	The provider must maintain a history of the software and systems versions (internal or external developments, commercial products) implemented to enable a complete environment to be reconstituted, if necessary in a test environment, as implemented on a given date. The retention period of this history must be consistent with that of the backups (see Chapter 12.5).
14.3.a	The provider must document and implement a procedure to test all applications before they are put into production in order to verify that there are no adverse effects on the activity or security of the service.
14.4.a	The provider must implement a secure development environment to manage the entire development cycle of the service information system.
14.4.b	The provider must take into account the development environments in the assessment of risks and ensure their protection in accordance with this repository.
14.5.a	The provider shall document and implement a procedure for supervising and controlling outsourced software and system development activity. This procedure shall ensure that the outsourced development activity complies with the provider's secure development policy and enables a level of external development security equivalent to that of internal development (see requirement 14.1 .
14.6.a	The Provider shall undergo compliance and security functionality testing of new or updated information systems during development. It must document and implement a test procedure that identifies:
	- the tasks to be carried out;
	- input data
	- the expected output results
14.7.a	The provider must document and implement a procedure to ensure the integrity of test data used in pre-production.
14.7.b	If the provider wishes to use sponsor data from production to perform tests, the provider must first obtain the consent of the Sponsor and anonymize them. The provider must ensure the confidentiality of the data when it is anonymized

15.1.a	The provider must keep up to date an ehaustive list of all third parties involved in the implementation of the service (hosting provider, developer, integrator, archiver, subcontractor operating on site or remotely, air conditioning providers, etc.). This list must be exhaustive, specify the contribution of the third party to the service and processing of personal data. The list must take into account cases of subcontracting at several levels.
15.1.b	The Provider must keep available to the Sponsor a list of all third parties who can access the data and inform the Sponsor of any changes in subcontractors within the meaning of Article 28 of the [GDPR] so that the Sponsor may object to this.
15.2.a	The provider must require third parties involved in the implementation of the service, in their contribution to the service, a level of security at least equivalent to that which it undertakes to maintain in its own security policy. It must do so through requirements, adapted to each third party and their contribution to the service, in the specifications or in the security clauses of the partnership agreements. The provider must include these requirements in contracts with third parties.
15.2.b	The provider must contract, with each of the third parties involved in the implementation of the service, audit clauses enabling a qualifying body to verify that those third parties comply with the requirements of this repository.
15.2.c	The provider must define and assign the roles and responsibilities relating to the modification or termination of the contract binding him to a third party involved in the implementation of the service
15.3.a	The provider shall document and implement a procedure to regularly monitor the measures put in place by third parties involved in the implementation of the service to comply with the requirements of this repository, in accordance with Chapter 18.3
15.4.a	The provider must document and implement a procedure for monitoring changes made by third parties involved in the implementation of the service that may affect the security level of the service's information system.
15.4.b	To the extent that a change of third parties involved in the implementation of the service affects the security level of the service, the provider shall notify all sponsors without delay in accordance with Chapter 12.2 and implement measures to restore the previous level of security
15.5.a	The Provider shall document and implement a procedure to review at least annually the requirements for confidentiality commitments or non-disclosure to third parties involved in the implementation of the service.
16.1.a	The provider must document and implement a procedure to provide prompt and effective responses to security incidents. These procedures must define the means and timelines for communicating security incidents to all sponsors concerned and the level of confidentiality required for such communication.
16.1.b	The provider must inform its employees and all third parties involved in the implementation of the service of this procedure.
16.1.c	The provider must document any breach of personal data and inform his customer thereof. The violation must be notified to the CNIL if it poses a risk to the rights and freedoms of the persons concerned. It must be the subject of information to the individuals concerned when the risk to their privacy is high
16.2.a	The Provider shall document and implement a procedure requiring its employees and third parties involved in the implementation of the service to report to the Service Provider for any security incidents, whether proven or suspected, as well as any security vulnerability.
16.2.b	The Provider shall document and implement a procedure that allows all sponsors to report any security incidents, whether proven or suspected, and any security vulnerability.
16.2.c	Provider must communicate to sponsors without delay security incidents and associated recommendations to limit their impacts. It must allow the sponsor to choose the severity levels of the incidents for which they wish to be informed.
16.2.d	The provider must communicate security incidents to the competent authorities in accordance with applicable legal and regulatory requirements
16.3.a	The provider must assess information security events and decide whether to qualify them as security incidents. For the assessment, it must be based on one or more scales (estimation, evaluation, etc.) shared with the sponsor.
16.3.b	The Provider shall use a classification that clearly identifies security incidents involving sponsor data in accordance with the results of the risk assessment. This classification should include violations of personal data.

16.4.a	The Provider must deal with security incidents until they are resolved and must inform Sponsors in accordance with the procedures.
16.4.b	The provider must archive documents detailing the security incidents.
16.4.c	It is recommended that the Provider use a qualified Security Incident Response Provider (PAS) to deal with security incidents requiring additional expertise
16.5.a	The Provider shall document and implement a continuous improvement process to reduce the occurrence and impact of types of security incidents that have already been dealt with
16.6.a	The provider shall document and implement a procedure for recording information relating to security incidents and which can be used as evidence
17.1.a	The provider must document and implement a business continuity plan that takes into account information security.
17.1.b	The service provider must review the business continuity plan of the service annually and each major change that may impact the service
17.2.a	The Provider shall document and implement procedures to maintain or restore the operation of the service and ensure the availability of information at the level and within the time frame for which the Provider has committed to the Sponsor in the Service Agreement
17.3.a	The Provider shall document and implement a procedure to test the Business Continuity Plan to ensure that it is relevant and effective in crisis situations
17.4.a	The provider shall document and implement measures to meet the need for availability of the service defined in the service agreement (see Chapter 19.1).
17.5.a	The service provider must document and implement an offline backup procedure for the configuration of the technical infrastructure.
17.6.a	The service provider must document and make available to the commissioning entity a backup of its data.
18.1.a	The provider must identify the applicable legal, regulatory and contractual requirements applicable to the service. In France, the provider must consider at least the following themes:
	- personal data [LOI_IL] [GDPR] ;
	- professional secrecy [CP_ART_226-13], where appropriate, without prejudice to the application of article 40 (2) of the Code of Criminal Procedure concerning reporting to a judicial authority;
	- abuse of trust [CP_ART_314-1]
	- the secrecy of private correspondence [CP_ART_226-15];
	- breach of privacy [CP_ART_226-1]
	- fraudulent access to or maintenance of an information system [CP_ART_323-1].
18.1.b	Depending on its role in the processing of personal data (data controller, processor or co-controller), the provider must justify and document the choices of technical and organisational measures made to meet the personal data protection requirements of this repository (see Part 19.5).
18.1.c	The provider must document and implement procedures to comply with the applicable legal, regulatory and contractual requirements applicable to the service, as well as specific security requirements (see Requirement 8.3 ().
18.1.d	The claimant must, at the request of a sponsor, make all of these procedures available to the claimant.
18.1.e	The provider must document and implement a process of active monitoring of the applicable legal, regulatory and contractual requirements applicable to the service
18.2.1.a	The provider must document and implement a three-year audit program that defines the scope and frequency of audits in accordance with change management, policies, and risk assessment results.
	The provider must include in the audit program a qualified audit per year by a qualified information system security audit provider [PASSI]. The entire audit program must include:
	- audit of the configuration of the technical infrastructure of the service. This audit is carried out by sampling and must include all types of equipment and servers present in the service information system;
	- intrusion testing of administration interfaces exposed on a public network;
	- the user interface penetration test for SaaS services;
	- if the service benefits from internal developments, the source code audit relating to the security functionalities implemented (the continuous approach should be preferred).
18.2.1.b	It is recommended that the service provider implement automated mechanisms for auditing the configuration adapted to the technical infrastructure of the service.

18.2.2.a	Prior to the assessment for qualification of the service, the service provider must have a initial independent review of information security by an audit service provider information systems security [PASSI] qualified. This initial review should in particular cover:
	- for services other than IaaS (CaaS, PaaS, SaaS, etc.), an audit of the configuration of virtual or physical resources, operating systems and basic software (OS, middleware, databases, ...) within the scope of the service;
	- an intrusion test on the service administration interfaces made available sponsors;
	- for a SaaS type service, an intrusion test on the interface made available end-users as well as an audit of the source code covering the functionalities of implemented security (authentication, session management, management of partitioning multi-tenant mode case). While SaaS provides an information security service, a dedicated product certification is required.
18.2.3.a	a) In the event of a major change that could affect the service, the service provider must have a independent change review by a systems security audit service provider qualified [PASSI] information. This independent change review should cover in particular the following audit activities:
	- architectural audit;
	- organizational and physical audit;
	- audit of the configuration of the technical infrastructure of the service;
	- an intrusion test on the service administration interfaces made available;
	- sponsors;
	- for a SaaS type service, an intrusion test on the interface made available end-users as well as an audit of the source code covering the functionalities of implemented security (authentication, session management, management of partitioning multi-tenant mode case). While SaaS provides an information security service, a dedicated product certification is required.
18.3.a	The provider through the Information Security Officer must regularly ensure that all security procedures under his responsibility are carried out correctly in order to ensure their compliance with security policies and standards
18.4.a	The Provider shall document and implement a policy to verify the technical compliance of the service with the requirements of this repository. This policy should define objectives, methods, frequencies, expected results and corrective measures.
19.1.a	The provider must establish a service agreement with each of the sponsors of the service. Any change to the service agreement must be subject to acceptance by Sponsor.
19.1.b	The provider must identify in the service agreement:
	- the obligations, rights and responsibilities of each party: provider and third parties involved in the provision of the service, sponsors, etc.;
	- elements explicitly excluded from the responsibilities of the provider within the limits of the legal and regulatory requirements in force, in particular Article 28 of the [GDPR];
	- the location of the service. The location of the media must be specified when it is carried out from a state outside the European Union, as required by requirement 19.2.e
19.1.c	The provider must propose a service agreement applying the law of a Member State of the European Union. The applicable law must be identified in the service agreement.
19.1.d	The service agreement must state that the collection, handling and storage of data made in the context of pre-sales, implementation, maintenance and shutdown of service comply with the requirements of French and European legislation in force and that these same data are not subject to other legal regimes.
19.1.e	The provider must describe in the service agreement the technical and organisational means it implements in order to ensure compliance with the applicable law.
19.1.f	The provider must include in the service agreement a clause revising the agreement providing for termination without penalty for the sponsor in the event of loss of the qualification granted to the service.
19.1.g	The Provider must include in the Service Agreement a reversibility clause allowing the Sponsor to retrieve all of its data (provided directly by the Sponsor or produced as part of the Service from the Sponsor's data or actions).
19.1.h	The provider must ensure this reversibility through one of the following technical arrangements:
	- the provision of files in one or more documented and usable formats outside the service provided by the provider;

	- the establishment of technical interfaces allowing access to data according to a documented and usable scheme (API, pivot format, etc.).
19.1.i	The service provider must indicate in the service agreement the level of availability of the service.
19.1.j	The provider must indicate in the service agreement that it cannot have the data transmitted and generated by the Sponsor, the provision of which is reserved to the Sponsor.
19.1.k	The Service Provider must indicate in the Service Agreement that it does not disclose any information relating to the performance to third parties unless the Sponsor expressly authorised in writing.
19.1.l	The service provider must indicate in the service agreement whether the commissioner's data is automatically saved or not. If not, the service provider must make the commissioning entity aware of the risks involved and clearly indicate the operations to be carried out by the commissioning entity in order for its data to be saved.
19.1.m	The service provider must indicate in the service agreement whether it allows remote access for administrative or support actions to the service information system.
19.1.n	The provider must specify in the service agreement that—the service is qualified and include the certificate of qualification;
	- Sponsor may file a Qualified Service Claim with ANSSI;
	- the Sponsor authorizes ANSSI and the Qualifying Body to evaluate the service and its service information system to verify that they comply with the requirements of this repository
19.1.o	The Provider shall specify in the service agreement that the Sponsor authorizes, in accordance with this Repository (see Requirement 18.2, a qualified information system security audit provider (ISS authorized by the provider to audit the service and its information system as part of the control plan.
19.1.p	The service provider must specify in the service agreement that it undertakes to make available all the information necessary for carrying out audits of compliance with the provisions of Article 28 of the [GDPR], conducted by the sponsor or a mandated third party.
19.1.q	It is recommended that the third party mandated for audits be a qualified information system security audit provider [PASSI].
19.2.a	The provider must document and communicate to the sponsor the location of the storage and processing of the latter's data.
19.2.b	The provider must store and process the sponsor's data within the European Union.
19.2.c	The administration and supervision of the service must be carried out from the European Union.
19.2.d	The service provider must store and process technical data (identities of beneficiaries and administrators of the technical infrastructure, data handled by the Software Defined Network, technical infrastructure logs, directory, certificates, access configuration, etc.) within the European Union.
19.2.e	The provider can carry out support operations to sponsors from a state outside the European Union. It must document the list of operations that can be carried out by the sponsor support from a state outside the European Union, and the mechanisms for ensuring access control and supervision from the European Union.
19.3.a	The provider must ensure that the interfaces of the service available to the sponsor are at least available in French.
19.3.b	The provider must provide first-level support in French
19.4.a	a) At the end of the contract between the service provider and the commissioning entity, that the contract has expired or for any other reason, the service provider must ensure secure erasure of all sponsor data. This erasure This erasure must be the subject of a formal notice to the commissioning entity from the service provider respecting a period of twenty-one calendar days. The erasure can be carried out using one of the following methods, and within a specified timeframe in the service agreement.
	- Complete rewrite erasure of any media that hosted this data
	- clearing the keys used for encrypting Sponsor's storage spaces described in Chapter 10.1;
	- secure recycling, under the conditions set out in Chapter 11.9
19.4.b	At the end of the contract, the provider must delete the technical data relating to the sponsor (directory, certificates, access configuration, etc.).
19.5.a	The provider must justify compliance with the data protection principles for the processing of personal data carried out on his own behalf. It must at least justify the following points:
	- the purposes of the specific, explicit and legitimate processing;

	- the traceability of processing activities on its behalf and that of its sponsor;
	- the lawful basis for the treatment;
	- the prohibition of the diversion of the purpose of processing;
	- the data used comply with the principle of minimum necessary and sufficient for treatment; thus adequate, relevant and limited;
	- the quality of the data used for the processing maintained: accurate and up-to-date data;
	- defined and limited shelf times.
19.5.b	The provider must justify, for the processing of personal data carried out on his own behalf, that the rights of the data subjects are respected. It must at least justify the following points:
	- information to users via fair and transparent processing;
	- collecting consent from users: express, demonstrable and withdrawn;
	- the possibility for users to exercise the rights of access, rectification and erasure;
	- the possibility for users to exercise the rights of limitation of processing, portability and opposition
19.5.c	When acting as a subcontractor (data processor) within the meaning of Article 28 of [GDPR], the provider must provide assistance and advice to the sponsor by informing them if an instruction from the latter constitutes a breach of data protection rules
19.6.a	The registered office, central administration or main establishment of the service provider must be established within a member state of the European Union.
19.6.b	The share capital and voting rights in the service provider's company must not be, directly or indirectly: - individually held at more than 24%; - and collectively owned more than 39%; by third-party entities with their registered office, central or main administration establishment in a non-member state of the European Union. These aforementioned third-party entities cannot individually: - by virtue of a contract or statutory clauses, have a right of veto; - by virtue of a contract or statutory clauses, appoint the majority of the members of the administrative, management or supervisory bodies of the service provider.
19.6.c	In the event of recourse by the service provider, within the framework of the services provided to the commissioning entity, to services of a third party company - including a subcontractor - with its registered office, central administration or main establishment in a non-member state of the Union European or owned or controlled by a third party company domiciled outside the European Union, this aforementioned third-party company should neither have the practical competence to obtain the data processed through the service. These data referred to are those entrusted to the service provider by the sponsors as well as all technical data (identities of beneficiaries and administrators of the technical infrastructure, data handled by the Software Defined Network, technical infrastructure logs, directory, certificates, access configuration, etc.) including information on the sponsors. For the purposes of this article, the notion of control is understood as being that mentioned in II of Article L233-3 of the Commercial Code.
19.6.d	Within the framework of paragraph 3, any third party company that the service provider uses to provide all or part of the service provided to the commissioning entity must guarantee the service provider autonomy of continuous operation in the provision of the cloud computing services it operates or must be SecNumCloud qualified. For the purposes of this article, the notion of operating autonomy is understood as being the ability to maintain the provision of the cloud computing service by calling the service provider's own skills or by using services available from at least two third-party companies.
19.6.e	The service provided by the provider must comply with the legislation in force in terms of rights fundamental values and the Union's values relating to respect for human dignity, freedom, equality, democracy and the rule of law. It can be taken into consideration for the assessment of the aforementioned compliance, the fact that the service provider maintains links with a foreign government or public body.