Cloud IT service providers (SecNumCloud)

Requirements reference document – Essential level

Version 3.0 of 8 December 2016
### VERSION HISTORY

<table>
<thead>
<tr>
<th>DATE</th>
<th>VERSION</th>
<th>DOCUMENT CHANGES</th>
<th>EDITOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>30/07/2014</td>
<td>1.3</td>
<td>Published version for comments.</td>
<td>ANSSI</td>
</tr>
<tr>
<td>20/03/2015</td>
<td>2.0</td>
<td>Intermediate version used for the experimental procedure</td>
<td>ANSSI</td>
</tr>
</tbody>
</table>
| 08/12/2016 | 3.0     | **First applicable version.**  
Principal modifications:  
- creation of a reference document per level of approval;  
- clarifications made to certain requirements;  
- rewriting of chapters 9, 10, 13 and appendices;  
- more precise integration of the PASSI, PRIS and PDIS labels. | ANSSI  |

Comments on this document should be sent to:

**Agence nationale de la sécurité des systèmes d'information (The French Networks and Information Security Agency)**

SGDSN/ANSSI  
51 boulevard de La Tour-Maubourg  
75700 Paris 07 SP
1. INTRODUCTION
   1.1. General overview
   1.1.1. Context
   1.1.2. Purpose of the document
   1.1.3. Document structure
   1.2. Document identification
   1.3. Acronyms and definitions
      1.3.1. Acronyms
      1.3.2. Definitions
      1.3.3. Roles

2. ACTIVITIES COVERED BY THE REFERENCE DOCUMENTATION
   2.1. Supply of SaaS services
   2.2. Supply of PaaS services
   2.3. Supply of IaaS services

3. APPROVAL OF CLOUD IT SERVICE PROVIDERS
   3.1. Approval methods
   3.2. Scope of the approval
   3.3. Warnings
      3.3.1. Risks linked to the absence of approval
      3.3.2. Risks linked to the protection of information

4. APPROVAL LEVELS
   4.1. Essential Level
   4.2. Advanced Level

5. RISK MANAGEMENT AND INFORMATION SECURITY POLICIES
   5.1. Principles
   5.2. Information security policy
   5.3. Risk assessment

6. INFORMATION SECURITY ORGANISATION
   6.1. Functions and responsibilities linked to information security
   6.2. Segregation of tasks
   6.3. Relations with the authorities
   6.4. Relations with specialised work groups
   6.5. Information security in project management

7. HUMAN RESOURCES SECURITY
   7.1. Selection of candidates
   7.2. Conditions for hire
   7.3. Awareness, learning and training on information security
   7.4. Disciplinary process
   7.5. Rupture, term or modification in the labour contract

8. ASSET MANAGEMENT
   8.1. Inventory and property of assets
   8.2. Restitution of assets
   8.3. Identification of the information security needs
   8.4. Marking and manipulating information
   8.5. Management of removable media

9. ACCESS CONTROL AND IDENTITY MANAGEMENT
9.1. Policies and access control
9.2. Registering and deregistering users
9.3. Management of access rights
9.4. Review of user access rights
9.5. Management of user authentications
9.6. Access to administration interfaces
9.7. Restriction of access to information

10. CRYPTOLOGY
10.1. Encryption of the data stored
10.2. Flow encryption
10.3. Password hashing
10.4. Non-repudiation
10.5. Management of secrets

11. PHYSICAL AND ENVIRONMENTAL SECURITY
11.1. Physical security perimeters
11.1.1. Public areas
11.1.2. Private areas
11.1.3. Sensitive areas
11.2. Physical access control
11.2.1. Private areas
11.2.2. Sensitive areas
11.3. Protection against outside and environmental threats
11.4. Working in private and sensitive areas
11.5. Delivery and loading areas
11.6. Wiring security
11.7. Hardware maintenance
11.8. Disposal of assets
11.9. Secured recycling of hardware
11.10. Hardware on hold for use

12. SECURITY LINKED TO OPERATIONS
12.1. Documented operating procedures
12.2. Managing change
12.3. Segregation of the development, test and operating environments
12.4. Measures against malicious code
12.5. Information backup
12.6. Logging of events
12.7. Protection for logged information
12.8. Clock synchronisation
12.9. Analysis and correlation of events
12.10. Installation of software on systems in operation
12.11. Technical vulnerability management
12.12. Administration

13. SECURITY OF COMMUNICATIONS
13.1. Map of the information system
13.2. Network partitioning
13.3. Network monitoring

14. ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS
14.1. Secure development policy
14.2. Procedures for controlling changes to the system ........................................33
14.3. Technical review of the applications after a change made to the operating platform ....33
14.4. Secure development environment ................................................................33
14.5. Outsourced development ...........................................................................33
14.6. System security and compliance test ..........................................................33
14.7. Protection of test data ................................................................................34
15. RELATIONS WITH THIRD PARTIES ........................................................... 35
15.1. Identification of third parties ........................................................................35
15.2. Security in the agreements made with third parties ......................................35
15.3. Monitoring and review of third party services ..............................................35
15.4. Managing changes made in the services of third parties ............................35
15.5. Confidentiality undertakings ......................................................................35
16. MANAGING INCIDENTS LINKED TO INFORMATION SECURITY ............ 36
16.1. Responsibilities and procedures ..................................................................36
16.2. Reporting linked to information security ....................................................36
16.3. Assessment of events linked to information security and decision making ....36
16.4. Response to incidents linked to information security ..................................36
16.5. Learning from incidents linked to information security .............................36
16.6. Collecting proof ..........................................................................................36
17. CONTINUITY OF ACTIVITY .................................................................... 37
17.1. Organisation of the continuity of activity ....................................................37
17.2. Implementing continuity of activity ...............................................................37
17.3. Check, review and evaluate the continuity of activity ..................................37
17.4. Availability of the means for information processing ..................................37
18. COMPLIANCE ......................................................................................... 38
18.1. Identification of the legislation and of the contractual requirements that apply ....38
18.2. Independent review of information security ................................................38
18.3. Compliance with security policies and standards .......................................38
18.4. Technical compliance examination .............................................................38
19. ADDITIONAL REQUIREMENTS .............................................................. 39
19.1. Service agreement .....................................................................................39
19.2. Location of data .........................................................................................40
19.3. Regionalisation ..........................................................................................40
19.4. End of contract ..........................................................................................40
APPENDIX 1 DOCUMENTARY REFERENCES .............................................. 41
I. Codes, laws and regulations ..........................................................................41
II. Standards and technical documents ...............................................................41
III. Other documentary references ....................................................................42
APPENDIX 2 RECOMMENDATIONS TO COMMISSIONING ENTITIES .......... 43
1. **Introduction**

1.1. **General overview**

1.1.1. **Context**

This reference document covers cloud computing and concerns the approval of service providers providing such services.

Cloud computing can be defined as an IT management model that allows access, via a network, to shared and configurable IT resources. These resources are allocated on demand and sometimes as self-service. Cloud IT service providers supply various services which are usually classified into three types of activity: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Details are provided on these activities in chapter 2.

The approach consisting in specifically contractualising security in each cloud rendering project has shown its limits: the offers are most often integrated, in such a way that a negotiation *a posteriori* by each client can hardly be considered; in addition, it is also unrealistic to encourage each client to conduct regular audits of the services offered.

A centralised approach, defining a reference document that favours the emergence of approved services, was retained: this makes it possible to process the security issue in a global and effective way, with the service providers having a stable framework in which to work in order to move towards approval and the users able to base their trust on this approval.

The current reference document is in particular based on international standard [ISO27001] of which it incidentally includes the structure of appendix A. However, this reference document comprises additional requirements that differentiate it from the existing standard and do not induce any equivalence between the two sets of rules.

1.1.2. **Purpose of the document**

This document is the requirements reference document applicable to a cloud IT service provider (SecNumCloud), hereinafter referred to as “the service provider”.

Its aim is to enable the approval of the family of service providers in accordance with the terms and conditions described in chapter 3.

It gives to the client assurance regarding the competencies of the service provider and its staff, the quality of its services, and the confidence that the commissioning entity can place in the service provider.

It can also be used, in the interest of adopting best practices, independently of any regulatory framework.

It does not exclude either the application of national laws and regulations, or the application of general rules imposed on service providers as professionals and in particular their duty to advise their commissioning entities.

This reference document is designed without any assumption of the technologies that can be used to implement the services. In particular, the expression cloud computing used within this reference document does not necessarily mean the use of virtualisation solutions.

1.1.3. **Document structure**

Chapter 1 is the introduction to this reference document.

Chapter 2 describes the activities to which this reference document relates.

Chapter 3 presents the approval methods, which attest to the compliance of the cloud IT service providers against applicable requirements.
Chapter 4 presents the approval levels that are covered by the approval of cloud IT service providers.

Chapters Erreur ! Source du renvoi introuvable. to 19 present the requirements applicable to service providers.

Appendix 1 presents references in terms of laws, regulations, standards and other documents cited in this reference document.

Appendix 2 presents the recommendations to the commissioning entities for the provision of cloud IT services.

1.2. Document identification

This reference document is referred to as "Cloud IT service providers (SecNumCloud) – requirements reference document– Essential level". It can be identified by its name, version number and date of update.

1.3. Acronyms and definitions

1.3.1. Acronyms

The acronyms used in this reference document are:

- **ANSSI**: Agence nationale de la sécurité des systèmes d’information (The French Networks and Information Security Agency)
- **French DPA; CNIL**: French data protection authority
- **EBIOS**: Expression des besoins et identification des objectifs de sécurité (Expression of needs and identification of security objectives)
- **IaaS**: Infrastructure as a service
- **PaaS**: Platform as a service
- **PASSI**: Audit service provider for information system security (Prestataire d’audit de la sécurité des systèmes d’information)
- **PDIS**: Prestataire de détection des incidents de sécurité (Security incident detection service provider)
- **PRIS**: Prestataire de Réponse aux Incidents de Sécurité (Security Incident Response Service Provider)
- **SaaS**: Software as a service

1.3.2. Definitions

- **Audit**: a systematic independent, documented process with a view to obtaining proofs of audit, and to carrying out an objective assessment to determine the extent to which audit criteria are satisfied.
- **Property**: any element that represents value for the service to be approved.
- **Client**: entity calling upon a cloud IT service provider.
- **Cloud computing**: model allowing for easy access, on demand and via a network, to all of the shared and configurable IT services.
- **State of the art**: the set of best practices, technologies, and reference documents relating to the security of information systems and that are publicly accessible, as well as information that flows from it in an obvious fashion. These documents may be made available on the Internet by the information systems security community, distributed by reference or regulatory entities.
Information security incident – a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations of the organisation or of threatening information security.

Technical infrastructure – all of the hardware and software components required for the making available of resources allocated to the demand (virtualised or not). This basis allows for the accomplishing of the service within the framework of an IaaS service, or is used as a basis for building the service in the other cases.

Administration interface – software interface that allows an entity that has the required privileges (an administrator, a service account, etc.) to perform administrative and configuration actions for an information system.

Threat – potential cause of an undesirable incident that can harm a system or organisation.

Security measure - measure that modifies the likelihood or the severity of a risk. It includes the policy, procedures, guidelines, and the organisational practices or structures, and can be of an administrative, technical, managerial or legal nature.

Policy – intentions and orientations of an organisation such as formalised by its management.

Service provider – organisation proposing a cloud IT service and aiming for approval.

Information System Security Audit Service Provider – Audit service provider for information system security. It is said to be approved if an approval entity has certified its compliance with the Requirements reference document for information system security audit service providers.

Virtualised resources – abstraction of the hardware resources of a system (CPU, RAM, etc.) which are made available by the technical infrastructure.

Risk – effect of an uncertainty as to achieving these objectives. This is expressed in terms of a combination of consequences of an event and of its likelihood.

Security of an information system – all of the technical and non-technical controls that make it possible for an information system to manage the availability, integrity or confidentiality of the data that is processed or transmitted and the related services that these systems provide or make available.

Supervision – surveillance of the proper operation of an information system or of a service. This concerns data collection (measurements, alarms, etc.) but it does not make it possible to act on the element that is monitored (which is done through administrative tasks).

Information system – organised set of resources (hardware, software, staff, data, and procedures) that allow information to be processed and circulated.

Vulnerability – weakness of property or control that can be exploited by one or more threats.

1.3.3. Roles

Administrator – user that has privileged rights that allow him to perform the tasks that have been allocated to him.

Security administrator – administrator in charge of the configuration of security, in particular the management of access rights for administrators.

Infrastructure administrator – administrator in charge of the management and maintaining in operational condition and condition of security of the technical infrastructure of the service. He is always under the responsibility of the service provider.

System administrator – administrator of the logical resources handled by the technical infrastructure of the service. According to the type of architecture of the service, the system administration can concern abstract resources (virtual machines, virtual networks, etc.), operating systems, middleware, business software, etc. (see the diagram in chapter 2).
**Business administrator** – administrator in charge of the functional administration at the applications level.

**User** – Any person who has an account within the perimeter of the service. This generic term encompasses the end users and the administrators.

**Final user** – person benefiting *in fine* from the service implemented. This can be the personnel of the client in the case of an internal service, or its own clients in the case of a service proposed outside.

The administrator roles can be allocated, either to the service provider, to the client, or be shared, this is according to the service and the respective responsibilities described in the service agreement.

*For example:* for an IaaS service for hosting servers, the roles can be distributed as follows:

- the service provider has infrastructure administrators (for the technical base that makes it possible to make the resources available to the client) and security administrators who allocate the access rights to them;

- the client has security administrators, system administrators who manage the servers that are hosted within the framework of the service, business administrators on the services that the client sets up himself and end users of these same services.
2. **Activities covered by the reference documentation**

This chapter presents the various activities covered in the reference documentation.

2.1. **Supply of SaaS services**

This service concerns the making available by the service provider of applications hosted on a cloud IT platform. The client does not have control of the underlying cloud platform. The service provider transparently manages for the client all of the technical aspects that require computer skills. The client retains the possibility of carrying out a few business configurations in the application.

Examples: "CRM", collaborative tools, email system, Business Intelligence, "ERP", etc.

2.2. **Supply of PaaS services**

This service concerns the making available by the service provider of platforms for hosting applications. The client does not have control of the underlying technical infrastructure, managed and controlled by the service provider (network, servers, OS, storage, etc.). The client however have control of the applications deployed on this platform. The client can also have control of certain services that comprise this platform or of certain configuration elements according to the distribution of the roles defined in the service.

Example: application containers managed by an orchestration tool.

2.3. **Supply of IaaS services**

This service concerns the making available of abstract IT resources (CPU power, memory, storage etc.). The IaaS model allows the client to have virtualised outsourced resources. The latter retains the control over the operating system (OS), the storage and applications deployed as well as over certain network components (firewall, for example).
<table>
<thead>
<tr>
<th></th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>End user</td>
<td>Business use</td>
<td>Business use</td>
<td>Business use</td>
</tr>
<tr>
<td>Business Administrator</td>
<td>Business configuration</td>
<td>Business configuration</td>
<td>Business configuration</td>
</tr>
<tr>
<td>System Administrator</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td>Middleware and other basic software</td>
<td>Middleware and other basic software</td>
<td>Middleware and other basic software</td>
</tr>
<tr>
<td></td>
<td>Operating systems</td>
<td>Operating systems</td>
<td>Operating systems</td>
</tr>
<tr>
<td></td>
<td>Virtualised resources</td>
<td>Virtualised resources</td>
<td>Virtualised resources</td>
</tr>
<tr>
<td>Technical Infrastructure Administrator</td>
<td>Virtualisation layer</td>
<td>Virtualisation layer</td>
<td>Virtualisation layer</td>
</tr>
<tr>
<td></td>
<td>Physical machines</td>
<td>Physical machines</td>
<td>Physical machines</td>
</tr>
<tr>
<td></td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td></td>
<td>Client</td>
<td>Service provider subject of the approval</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1- Distribution of the responsibilities by type of service**
3. Approval of cloud IT service providers

3.1. Approval methods

The reference document contains the requirements and recommendations for cloud IT service providers.

A service provider is approved in accordance with the process for approving a trusted service provider [PROCESS_QUALIF], and enables an attestation of the fact that the service provider complies with the requirements of the reference documentation.

Service providers must comply with the requirements in order to obtain the approval.

The recommendations are provided as a matter of best practice and are not subject to verification to obtain the approval.

3.2. Scope of the approval

In order to be approved, service providers must meet all the requirements of this reference document over the scope chosen. The scope is defined by all or a portion of the activities described in chapter 2.

Approved service providers retain the ability to provide services outside the scope for which they are approved, but cannot, in this case, use this approval status for the purpose of providing these services.

An approved cloud IT service provision can be combined with other complementary services (development, integration of security products, etc.) without losing the benefit of the approval.

3.3. Warnings

3.3.1. Risks linked to the absence of approval

An unapproved cloud IT service provision can, potentially, expose the commissioning entity to certain risks, especially leaks of confidential information, compromising, the loss or unavailability of its information system.

Accordingly, in the case of a non-approved service, it is recommended that the commissioning entity request from its service provider a document listing all the requirements of this reference document that are not covered as part of its service, in order for the commissioning entity to understand the risks to which it is exposed.

3.3.2. Risks linked to the protection of information

Compliance with the SecNumCloud reference document does not take the place of the legal or regulatory requirements that apply to certain specific types of data such as the data at the Restricted Distribution level or health data. The hosting of specific data in an approved SecNumCloud service requires compliance with the additional requirements described in the documents [EX_DONNEES].

The clauses of this reference document that refer to approved products apply when these products exist.

Moreover, this reference document is based on an objective of protecting the client's data, but does not provide any strong technical guarantees against an access of the service provider to the data processed on the information system of the service, only contractual commitments. Clients who want to provide protection, from a technical standpoint, for their data against access by the service provider, must consequently implement additional means of encryption, under their control, of their data.

Finally, note that the virtualisation that is generally used in cloud IT services must not be considered as a partitioning mechanism that is equivalent to a physical separation.
4. **Approval levels**

Two approval levels are distinguished for cloud IT services.

4.1. **Essential Level**

This corresponds to a level of security allowing for the storage and the processing of data for which a security incident would have limited consequences for the client. It ensures in particular compliance with security best practices for IT hygiene, such as described in the guide [HYGIENE] by ANSSI.

The requirements for the Essential level are defined in this reference document.

The compliance of a cloud IT service at the Essential level does not certify its compliance with the State Information Systems Security Policy [PSSIE].

4.2. **Advanced Level**

This corresponds to a level of security allowing for the storage and the processing of data for which a security incident would have substantial consequences for the client, and even jeopardise its long-term survival.

The requirements for the Advanced level are defined in [SNC_AVANCE].
5. **Risk management and information security policies**

5.1. **Principles**
   a) The service provider must perform the service in the state of the art for the type of activity retained: use stable software that benefits from follow-ups for security patches and parameters in such a way as to obtain an optimal level of security.
   
   b) The service provider must apply ANSSI’s IT hygiene guide, [HYGIENE] to the service’s information system.

5.2. **Information security policy**
   a) The service provider must document and implement an information security policy relative to the service.
   
   b) The information security policy must identify the commitments of the service provider as to compliance with the national legislation and regulations in effect according to the nature of the information that could be entrusted by the client to the service provider; it is, however, ultimately up to the client to ensure compliance with the legal and regulatory constraints that apply to the data that it actually entrusts to the service provider.
   
   c) The information security policy must in particular cover the themes addressed in chapters 6 to 19 of this reference document.
   
   d) The management of the service provider must formally approve the information security policy.
   
   e) The service provider must revise the information security policy annually and at each major change that can affect the service.

5.3. **Risk assessment**
   1. The service provider must document a risk assessment that covers the entire perimeter of the service.
   
   2. The service provider must carry out its risk assessment by using a documented method that guarantees reproducibility and comparability of the approach.
   
   3. The service provider must take into account in the risk assessment:
      - the management of client information that has different security needs;
      - the risks of failure of the mechanisms of partitioning technical infrastructure resources (memory, calculation, storage, network) that are shared between clients;
      - the risks linked to the incomplete or non-secure erasing of data stored in the memory areas or of storage shared between clients, in particular during reallocations of memory and storage areas;
      - the risks linked to the exposure of administrative interfaces over a public network.
   
   4. When there are specific legal, regulatory or sector requirements linked to the type of information entrusted by the client to the service provider, the latter must take them into account in its risk assessment by ensuring compliance with all of the requirements of this reference document on the one hand and not lower the level of security established through the compliance with the requirements of this reference document on the other hand.
   
   5. The management of the service provider must formally accept the residual risks identified in the risk assessment.
6. The service provider must revise the risk assessment annually and at each major change that can affect the service.
6. **Information security organisation**

6.1. **Functions and responsibilities linked to information security**

   a) The service provider must document and implement an internal organisation of security in order to ensure the definition, setting up and monitoring of the operational functioning of the information security within its organisation.

   b) The service provider must designate a manager for information systems security and a manager for physical security.

   c) The service provider must define and allocate the responsibilities in terms of information security for the personnel involved in supplying the service.

   d) The service provider must ensure after any major change that can affect the service that the allocation of the responsibilities in terms of information security is still pertinent.

6.2. **Segregation of tasks**

   a) The service provider must identify the risks associated with the accumulation of responsibilities or tasks, take them into account in assessing the risks and implementing measures for reducing these risks.

6.3. **Relations with the authorities**

   a) It is recommended that the service provider set up suitable relations with the competent authorities in terms of information security and of data of a personal nature and, where applicable, with the sector authorities according to the nature of the information entrusted by the client to the service provider.

6.4. **Relations with specialised work groups**

   a) It is recommended that the service provider maintain suitable contacts with groups of specialists or recognised sources, in particular in order to take new threats into account and the appropriate security measures to counter them.

6.5. **Information security in project management**

   a) The service provider must document an estimate of the risks prior to any project that can affect the service, and this regardless of the nature of the project.

   b) Where a project affects or is likely to affect the level of security of the service, the service provider must inform the client and inform him in writing of the potential impacts and the measures taken to reduce these impacts as well as the residual risks concerning him.
7. **Human resources security**

7.1. **Selection of candidates**
   a) The service provider must document and implement a procedure for verifying information concerning its personnel that is compliant with the laws and regulations in effect.

   These verifications apply to any person involved in the supply of services and must be proportional to the sensitivity of the client information entrusted to the service provider as well as to the risks identified.

7.2. **Conditions for hire**
   a) The service provider must have a code of ethics incorporated into its internal regulations, stipulating, in particular, that:
      - services are performed with loyalty, discretion and impartiality;
      - employees use only those methods, tools and techniques that have been approved by the service provider;
      - employees undertake to not disclose information to a third party, even if anonymised and decontextualised, which has been obtained or generated as part of the service, unless the client has given formal written authorisation;
      - employees undertake to alert the service provider to all clearly illegal content discovered during the provision of the service;
      - employees undertake to comply with the national legislation and regulations in force and with best practices related to their activities.

   b) The service provider must have the code of ethics signed by all of the employees involved in supplying the service.

   c) The service provider must, when requested by a client, provide it with the internal regulations and the code of ethics.

7.3. **Awareness, learning and training on information security**
   a) The service provider must increase the awareness on information security for all of the employees involved in supplying the service. It must provide them with pertinent procedure and policy updates in the framework of their assignments.

   b) The service provider must document and implement a training plan concerning information security that is suited to the service and to the assignments of the employees.

   c) The service provider's information systems security manager must formally validate the training plan concerning information security.

7.4. **Disciplinary process**
   a) The service provider must document and implement a disciplinary process that applies to all of the employees involved in supplying the service who have breached the security policy.

   b) The service provider must, when requested by the client, provide the client with the sanctions incurred in case of a breach of the security policy.

7.5. **Rupture, term or modification in the labour contract**
   a) The service provider must define and allocate the roles and the responsibilities concerning the rupture, the term or the modification of any contract with an employee involved in the supply of the service.
8. Asset management

8.1. Inventory and property of assets

a) The service provider must maintain an up-to-date inventory of all of the equipment that implements the service. This inventory must specify for each piece of equipment:
   - the information for identifying the equipment (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 needs in terms of information security (in the meaning of chapter 8.3).

b) The service provider must maintain an up-to-date inventory of all of the software that implements the service. This inventory must identify for each software, its version and the equipment on which the software is installed.

c) The service provider must ensure the validity of the software licences all throughout the provision of service.

8.2. Restitution of assets

a) The service provider must document and implement a procedure for remitting assets that makes it possible to ensure that each employee involved in the supply of the service returns all of the assets in their possession at the end of the period of use or of their contract.

8.3. Identification of the information security needs

a) The service provider must identify the various information security needs related to the service.

b) When the client entrusts the service provider with data subjected to specific legal, regulatory or sector constraints, the service provider must identify the specific security needs associated with these constraints.

8.4. Marking and manipulating information

a) It is recommended that the service provider document and implement a procedure for marking and manipulating all of the information that participates in the delivery of the service, in accordance with its security needs defined in chapter 8.3.

8.5. Management of removable media

a) The service provider must document and implement a procedure for the management of removable media, in accordance with the security need defined in chapter 8.3.

b) When removable media is used in the technical infrastructure or for administrative tasks, this media has to be dedicated to one use.
9. Access control and identity management

Unless explicitly mentioned, this chapter concerns access control and the management of the identities of the users:

- placed under the responsibility of the service provider (its employees and possibly third parties that participate in the supply of the service);
- placed under the responsibility of the client, but for which the service provider implements the means for controlling access (by supplying the client in particular with an interface for managing accounts and access rights).

The users for which the client implements the means for access control and for the management of identities are outside of the scope of this reference document.

9.1. Policies and access control

a) The service provider must document and implement an access control policy based on the results of its risk assessment and on the sharing of responsibilities.

b) The service provider must revise the access control policy annually and at each major change that can affect the service.

9.2. Registering and deregistering users

a) The service provider must document and implement a procedure for registering and for deregistering users using an access rights and account management interface. This procedure must indicate which data is to be deleted when a user departs.

b) The service provider must allocate nominative accounts when registering users who are placed under its responsibility.

c) The service provider must implement means that make it possible to ensure that the deregistering of a user results in the deletion of all of his accesses to the resources of the information system of the service, as well as the deletion of his data in accordance with the registration and deregistration procedure. (see requirement 9.2 a)).

9.3. Management of access rights

a) The service provider must document and implement a procedure that makes it possible to ensure the allocation, modification and removal of access rights to the resources of the information system of the service.

b) The service provider must provide its clients with the tools and the means that allow for a differentiation of the roles of the users of the service, for example according to their functional role.

c) The service provider must maintain an up-to-date inventory of the users under its responsibility who have administration rights to the resources of the information system of the service.

d) The service provider must be able to provide, for a given resource that implements the service, the list of all of the users who have access to it, whether they fall under the responsibility of the service provider or of the client as well as the access rights that have been granted to them.

e) The service provider must be able to provide, for a given user, whether they fall under the responsibility of the service provider or of the client, the list of all of their access rights to the various elements of the information system of the service.

f) The service provider must define a list of access rights that are incompatible with each other. It must ensure, during the allocation of the access rights to a user that he does not have access rights that are incompatible with each other in terms of the list established beforehand.

| Cloud IT service providers (SecNumCloud) – requirements reference document – Essential level |
|-----------------------------------------------|------------------|-------------------|-----------------|
| Version | Date       | Circulation criteria | Page |
| 3.0     | 08/12/2016 | Public              | 19/43 |
g) The service provider must include in the access rights management procedure the actions for revoking or suspending rights for any user.

9.4. **Review of user access rights**
   a) The service provider must annually revise the access rights of the users within its scope of responsibility.
   
b) The service provider must provide the client with a tool that facilitates the review of the access rights of users placed under the responsibility of the latter.
   
c) The service provider must revise on a quarterly basis the list of users within its scope of responsibility who can use the technical accounts mentioned in requirement 9.2 b).

9.5. **Management of user authentications**
   a) The service provider must formalise and implement procedures for the management of user authentication. In agreement with the requirements of chapter 10, the latter must in particular cover:
   - the management of the means for authentication (issuing and resetting of passwords, updating CRLs and importing root certificates in case of the use of certificates, etc.).
   - setting up means that allow for an authentication with multiple factors so as to respond to the various cases of use of the reference document.
   - the systems that generate passwords or that verify their robustness, when authentication by password is used. They must follow the recommendations of [NT_MDP].
   
b) Any authentication mechanism must provide for the blocking of an account after a limited number of unsuccessful attempts.
   
c) In the framework of an SaaS service, the service provider must provide its clients with means of authentication with multiple factors for the access for end users.
   
d) When technical accounts that are non-nominative are required, the service provider must set up measures that require the users to be authenticated with their nominative account before being able to access these technical accounts.

9.6. **Access to administration interfaces**
   a) The administration accounts under the responsibility of the service provider must be managed using tools and directories that are separate from those used for the management of user accounts placed under the responsibility of the client.
   
b) The administration interfaces made available to clients must be separate from the administration interfaces used by the service provider.
   
c) The administration interfaces made available to clients must not allow for any connection with accounts of administrators under the responsibility of the service provider.
   
d) The administration interfaces used for the service provider must not be accessible from the public network and as such must not allow for any connection of users under the responsibility of the client.
   
e) If administration interfaces are made available to clients with an access via a public network, the administration flows must be authenticated and encrypted with means in accordance with the requirements of chapter 10.2.
   
f) The service provider must set up a double-factor authentication system for access:
   - to the administration interfaces used by the service provider;
9.7. **Restriction of access to information**

a) The service provider must implement suitable measures for partitioning between its clients.

b) The service provider must implement suitable partitioning measures between the information system of the service and its other information systems (office software, management IT, technical management for the building, physical access control, etc.).

c) The service provider must design, develop, configure and deploy the information system of the service by providing at least a partitioning between on the one hand the technical infrastructure and on the other hand the equipment required for the administration of the services and of the resources that it hosts.
10. **Cryptology**

10.1. **Encryption of the data stored**
   a) The service provider must define and implement an encryption mechanism that prevents the recovery of client data in the event a resource is reallocated or a physical media is recovered.
      - in the case of an IaaS service, this objective can for example be achieved:
        - by encrypting the hard drive or the file system, when the access protocol in file mode guarantees that only empty blocks can be allocated (for example storage of the NAS type wherein a physical block is actually allocated only at the time of writing),
        - by encrypting the volume in case of access in block mode (for example storage of the SAN type of local storage), with at least one key per client;
      - in the case of a PaaS or SaaS service, this objective can be achieved by using an application encryption within the perimeter of the service provider, with at least one key per client.
   b) The service provider must use a data encryption method that complies with the rules of [CRYPTO_B1].
   c) It is recommended to use a data encryption method that complies with the recommendations of [CRYPTO_B1].
   d) The service provider must set up data encryption on the removable media and the backup media intended to leave the physical security perimeter of the information system of the service (in the meaning of chapter 11), according to the data security need (see chapter 8.3).

10.2. **Flow encryption**
   a) When the service provider implements a network flow encryption mechanism, the latter must comply with the rules of [CRYPTO_B1].
   b) When the service provider implements a network flow encryption mechanism, it is recommended that the latter comply with the recommendations of [CRYPTO_B1].
   c) If the TLS protocol is implemented, the service provider must apply the recommendations of [NT_TLS].
   d) If the IPsec protocol is implemented, the service provider must apply the recommendations of [NT_IPSEC].
   e) If the SSH protocol is implemented, the service provider must apply the recommendations of [NT_SSH].

10.3. **Password hashing**
   a) The service provider must store only the hash values of the passwords of the users and of technical accounts.
   b) The service provider must use a hash function that complies with the rules of [CRYPTO_B1].
   c) It is recommended that the service provider implement a hash function that complies with the recommendations of [CRYPTO_B1].
   d) The service provider must generate the hash values of the passwords with a hash function associated with the use of a cryptographic salt that complies with the rules of [CRYPTO_B1].
10.4. **Non-repudiation**

a) When the service provider implements an electronic signature mechanism, the latter must comply with the rules of [CRYPTO_B1].

b) When the service provider implements an electronic signature mechanism, it is recommended that the latter comply with the recommendations of [CRYPTO_B1].

10.5. **Management of secrets**

a) The service provider must implement cryptographic keys that comply with the rules of [CRYPTO_B2].

b) It is recommended that the service provider implement cryptographic keys that comply with the recommendations of [CRYPTO_B2].

c) The service provider must protect access to the cryptographic keys and other secrets used for the encrypting of data by a suitable means: security container (software or hardware) or separate media.

d) The service provider must protect access to the cryptographic keys and other secrets used for the administration tasks by a suitable security container, software or hardware.
11. **Physical and environmental security**

11.1. **Physical security perimeters**
   a) The service provider must document and implement security perimeters, including the marking of areas and the various means of limiting and of controlling access.
   b) The service provider must distinguish public areas, private areas and sensitive areas.

11.1.1. **Public areas**
   a) Public areas can be accessed by all within the limits of the property of the service provider. The service provider must host no resource that is reserved for the service or that allows for access to the components of the latter in the public areas.

11.1.2. **Private areas**
   a) Private areas can host:
      - the platforms and means for development of the service;
      - the administration, operation and supervision stations;
      - the premises from which the service provider operates.

11.1.3. **Sensitive areas**
   a) Sensitive areas are reserved for the hosting of the information system for the production of the service excluding administration, operation and supervision stations.

11.2. **Physical access control**

11.2.1. **Private areas**
   a) The service provider must protect the private areas from unauthorised access. To do this, it must implement physical access control that is based on at least one personal factor: knowledge of the secret, the holding of an object or biometrics.
   b) It is recommended that the service provider complies with the recommendations of [G_SANSCONTACT](#) in order to implement physical access control.
   c) The service provider must define and document the physical access derogations in case of emergency.
   d) The service provider must post at the entrance to private areas a warning concerning the limits and the conditions of access to these areas.
   e) The service provider must define and document the time slots and conditions for accessing private areas according to the profiles of the users.
   f) The service provider must document and implement the means that make it possible to ensure that visitors are systematically accompanied by the service provider during their access and stays in the private area. The service provider must retain a trace of the identity of the visitors in accordance with current legislation and regulations.
   g) The service provider must document and implement mechanisms for monitoring and detecting unauthorised access to private areas.
11.2.2. Sensitive areas

a) The service provider must protect the sensitive areas from unauthorised access. To do this, it must implement physical access control that is based at least on two personal factors: knowledge of the secret, the holding of an object or biometrics.

b) It is recommended that the service provider complies with the recommendations of [G_SANSCONTACT] for the implementing of physical access control.

c) The service provider must define and document the physical access derogations in case of emergency.

d) The service provider must post at the entrance to sensitive areas a warning concerning the limits and the conditions of access to these areas.

e) The service provider must define and document the time slots and conditions for accessing sensitive areas according to the profiles of the users.

f) The service provider must document and implement the means that make it possible to ensure that visitors are systematically accompanied by the service provider during their access and stays in the sensitive area. The service provider must retain a trace of the identity of the visitors in accordance with current legislation and regulations.

g) The service provider must document and implement mechanisms for monitoring and detecting unauthorised access to sensitive areas.

h) The service provider must set up a log of physical access to the sensitive areas. It must conduct a review of these logs at least monthly.

i) The service provider must implement the means that guarantee that no direct access exists between a public area and a sensitive area.

11.3. Protection against outside and environmental threats

a) The service provider must document and implement means that make it possible to minimise the risks inherent with physical losses (fire, water damages, etc.) and natural losses (climate risks, flooding, earthquakes, etc.).

b) The service provider must document and implement measures that make it possible to limit the risks of the start and of the propagation of fire as well as the risks concerning water damage.

c) The service provider must document and implement measures that make it possible to prevent and limit the consequences of an electrical power cut-off and allow for the resuming of the service in accordance with the requirements concerning the availability of the service defined in the service agreement.

d) The service provider must document and implement means that make it possible to maintain conditions of temperature and humidity that are suited to the equipment. In addition, it must implement measures that make it possible to prevent air conditioning breakdowns and to limit the consequences of them.

e) The service provider must document and implement controls and tests on a regular basis for physical protection and detection equipment.

11.4. Working in private and sensitive areas

a) The service provider must incorporate the physical security elements into the security policy and the risk assessment in accordance with the level of security required by the category of the area.

b) The service provider must document and implement procedures concerning work in private and sensitive areas. It must forward these procedures to the users involved.
11.5. Delivery and loading areas

The delivery and loading areas and the other points through which unauthorised persons can penetrate into the premises without being accompanied are considered to be public areas.

a) The service provider must isolate the access points from these areas to the private and sensitive areas, so as to prevent unauthorised access, or, otherwise, implement compensatory measures that make it possible to provide the same level of security.

11.6. Wiring security

a) The service provider must document and implement measures that make it possible to protect the electrical and telecommunication wiring from physical damage and from the possibilities of interception.

b) The service provider must establish a wiring scheme and keep it up to date.

c) It is recommended that the service provider implement measures that make it possible to identify the wires (for example colour coding, labels, etc.) in order to facilitate operation and limit handling errors.

11.7. Hardware maintenance

a) The service provider must document and implement measures that make it possible to ensure that the conditions for installation, maintenance and servicing of the equipment of the information of the service hosted in private and sensitive areas are compatible with the requirements of confidentiality and availability of the service defined in the service agreement.

b) The service provider must take out maintenance contracts that make it possible to have security updates for the software installed on the equipment of the information system of the service.

c) The service provider must ensure that the media can be returned to a third party only if the client data stored on it is encrypted in accordance with chapter 10.1 or has been destroyed beforehand using a secure deletion mechanisms by rewriting random patterns.

d) The service provider must document and implement measures that make it possible to ensure that the conditions for installation, maintenance and servicing of the related technical equipment (electrical power, air conditioning, fire, etc.) are compatible with the requirements of the availability of the service defined in the service agreement.

11.8. Disposal of assets

a) The service provider must document and implement a procedure for transferring client data, hardware and software off the site. This procedure must require the management of the service provider to give its approval in writing. In any case, the service provider must implement means that make it possible to guarantee that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site.

11.9. Secured recycling of hardware

a) The service provider must document and implement means that make it possible to delete in a secure manner by rewriting random patterns any data media made available to a client. If the storage area is encrypted in the framework of requirement 10.1 a), the deletion can be carried out via a secure deletion of the encryption key.

11.10. Hardware on hold for use

a) The service provider must document and implement a procedure for protecting hardware that is on hold for use.
12. **Security linked to operations**

12.1. **Documented operating procedures**
   a) The service provider must document the operation procedures, keep them up to date and make them available to the employees concerned.

12.2. **Managing change**
   a) The service provider must document and implement a procedure for managing the changes made to the systems and means of information processing.
   
b) The service provider must document and implement a procedure that makes it possible, in case of operations carried out by the service provider and which can affect the security or the availability of the service, to communicate as early as possible to all of its clients the following information:
      - the scheduled date and time for the starting and ending of the operations;
      - the type of operations;
      - the impacts on the security or the availability of the service;
      - the contact within the service provider.
   
c) In the framework of a PaaS service, the service provider must inform the client as early as possible of any upcoming modification to the software elements under its responsibility when full compatibility cannot be guaranteed.
   
d) In the framework of a SaaS service, the service provider must inform the client as early as possible of any upcoming modification to the service elements when this is likely to cause a loss in functionality for the client.

12.3. **Segregation of the development, test and operating environments**
   a) The service provider must document and implement the measures that make it possible to physically segregate the environments linked to the production of the service from the other environments, including development environments.

12.4. **Measures against malicious code**
   a) The service provider must document and implement measures for detecting, preventing and restoring in order to provide protection against malicious code. The scope of application of this requirement on the information system of the service must necessarily contain the user stations under the responsibility of the service provider and the incoming flows on this same information system.
   
b) The service provider must document and implement awareness for its employees to the risks linked to malicious code and to best practices in order to reduce the impact of an infection.

12.5. **Information backup**
   a) The service provider must document and implement a backup and restore policy for the data under its responsibility in the framework of the service. This policy must provide a daily backup of all of the data (information, software, configurations, etc.) under the responsibility of the service provider in the framework of the service.
   
b) The service provider must document and implement measures for protecting the backups in accordance with the access control policy (see chapter 9). This policy must provide for a monthly review of the tracking of access to the backups.
c) The service provider must document and implement a procedure that makes it possible to test the restoration of backups on a regular basis.

d) The service provider must store the backups at a sufficient distance from the main hardware in coherence with the results of the risk assessment and which makes it possible to handle major losses. Backups are subject to the same requirements in terms of location as operating data. The backup site or sites are subject to the same security requirements as the main site, in particular those listed in chapters 8 and 11. The communications between the main site and the backup site must be protected by encryption, in accordance with the requirements in chapter 10.

12.6. Logging of events

a) The service provider must document and implement an logging policy that includes at least the following elements:
   - the list of the collection sources;
   - the list of events to be logged by source;
   - the object of the logging by event;
   - the collection frequency and time base used;
   - local and centralised retention time;
   - measures for protecting logs (including encryption and duplication);
   - the location of the logs.

b) The service provider must generate and collect the following events:
   - the activities of the users linked to information security;
   - modification of access rights within the perimeter of its responsibility;
   - the events coming from mechanisms for fighting malicious code (see 12.4);
   - exceptions;
   - failures;
   - any other event linked to information security.

c) The service provider must retain the events coming from the log for a minimum period of six months subject to compliance with legal and regulatory requirements.

d) The service provider must provide, when requested by the client, all of the events that concern it.

e) It is recommended that the logging system set up by the service provide comply with the recommendations of [NT_JOURNAL].

12.7. Protection for logged information

a) The service provider must protect the logging hardware and the logged events from attacks concerning their availability, integrity or confidentiality, in accordance with chapter 3.2 of [NT_JOURNAL].

b) The service provider must manage the size of the storage area for all of the hardware that hosts one or several collection sources in order to allow for the local storage of the logged events provided for by the event logging policy. This management of the size must take the changes made to the information system into account.
c) The service provider must transfer the logged events by ensuring their protection in terms of confidentiality and integrity, over one or more dedicated central servers and must store them on a physical machine that is separate from that which generated them.

d) The service provider must set up a backup for the collected events according to a suitable policy.

e) The service provider must run the processes for logging and for collecting events with the accounts that have the required and sufficient privileges and must limit access to the logged events in accordance with the access control policy. (see chapter 8).

12.8. Clock synchronisation

a) The service provider must document and implement a synchronisation of the clocks of all of the hardware on one or more internal time sources that are coherent with each other. These sources can themselves be synchronised over several reliable external sources, except for isolated networks.

b) The service provider must set up time/date stamping for each event logged.

12.9. Analysis and correlation of events

a) The service provider must document and implement an infrastructure that allows for the analysis and the correlation of the events recorded by the logging system in order to detect events that can affect the security of the information system of the service, in real time or a posteriori for events going back as far as six months.

b) It is recommended to use the requirements reference document for security incident detection service providers [PDIS] for the setting up and operation of the infrastructure for analysing and correlating events.

c) The service provider must acknowledge the alarms reported by the infrastructure for analysing and correlating events at least once on a daily basis.

12.10. Installation of software on systems in operation

a) The service provider must document and implement a procedure that makes it possible to control the installation of software on the hardware of the information system of the service.

b) The service provider must document and implement a procedure for managing the configuration of the software environments made available to the client, in particular for maintaining them in a condition of security.

12.11. Technical vulnerability management

a) The service provider must document and implement a monitoring process that makes it possible to manage the technical vulnerabilities of the software and of the systems used in the information system of the service.

b) The service provider must evaluate its exposure to these vulnerabilities by including them in the risk assessment and apply the suitable measures for processing the risk.

12.12. Administration

a) The service provider must document and implement a procedure that requires the administrators under its responsibility to use dedicated terminals for the exclusive execution of the administrative tasks, in accordance with chapter 4.1 entitled "administration network and station" of [NT_ADMIN]. It must control them and keep them up to date.

b) The service provider must set up measures for tightening the configuration of the terminals used for the administrative tasks, in particular those in chapter 4.2 entitled "securing the base" of [NT_ADMIN].
c) When the service provider authorises a situation of mobility for the administrators under its responsibility, it must supervise it via a documented policy. The solution implemented must ensure that the level of security of this situation of mobility is at least equivalent to the level of security outside of a situation of mobility (see chapters 9.6 and 9.7). This solution must in particular include:

- the use of an encrypted tunnel, which cannot be disengaged and which cannot be circumvented, for all of the flows (see chapter 10.2);
- full encryption of the hard drive (see chapter 10.1).
13. **Security of communications**

13.1. **Map of the information system.**

a) The service provider must establish and keep up to date a map of the information system of the service, in liaison with the inventory of the assets (see chapter 8.1 a), comprising at least the following elements:

- the list of the hardware or virtualised resources;
- the names and functions of the applications, that support the service;
- the network architecture diagram at level 3 of the OSI model whereon the nerve centres are identified:
  - interconnection points, especially with third-party and public networks,
  - the networks, sub-networks, in particular the administration networks,
  - the equipment that provides security functions (filtering, authentication, encryption, etc.),
  - the servers that host the data or that provide sensitive functions;
- the matrix of the authorised network flows, specifying:
  - their technical description (services, protocols and ports);
  - the business or infrastructure justification;
  - where applicable, when services, protocols or ports deemed as unsafe are used, the compensatory measures set up, in the logic of in-depth defence.

b) The service provider must revise the map at least once a year.

13.2. **Network partitioning**

a) The service provider must document and implement, for the information system of the service, the partitioning measures (logical, physical or via encryption) in order to separate the network flows according to:

- the sensitivity of the information sent;
- the nature of the flows (production, administration, supervision, etc.);
- the area that the flows belong to (clients – with a distinction per client or set of clients, the service provider, third parties, etc.);
- the technical area (processing, storage, etc.).

b) The service provider must partition, physically or via encryption, all of the internal data flows of the information system of the service with regards to any other information system. When this partitioning is carried out via encryption, it is carried out in accordance with the requirements of chapter 10.2.

c) In the case where the administration network of the technical infrastructure does not benefit from a physical partitioning, the administration flows must be conveyed in an encrypted tunnel, in accordance with the requirements of chapter 10.2.

d) The service provider must set up and configure an application firewall in order to protect the administration interfaces intended for its clients and exposed over a public network.
e) The service provider must implement over all of the administration and monitoring interfaces of the service a filtering mechanism that authorises only legitimate connections identified in the matrix of authorised flows.

13.3. **Network monitoring**

a) The service provider must have one or more probes for detecting security incidents over the information system of the service. These probes must, in particular, make it possible to monitor each of the interconnections of the information system of the service with the information systems of third parties and of public networks. These probes must be sources of collection for the infrastructure for analysing and correlating events (see chapter 12.9).
14. **Acquisition, development and maintenance of information systems**

14.1. **Secure development policy**
   a) The service provider must document and implement rules for the secure development of software and systems, and apply them to internal development.
   
   b) The service provider must document and implement suitable secure development training for the employees concerned.

14.2. **Procedures for controlling changes to the system**
   a) The service provider must document and implement a procedure for controlling the changes made to the information system of the service.
   
   b) The service provider must document and implement a procedure validating the changes made to the information system of the service over a pre-production environment before they are put into production.
   
   c) The service provider must retain a history of the software versions and of the systems (internal or external development, commercial products) that are implemented in order to be able to reconstitute, where applicable in a test environment, a complete environment such as was implemented on a given date. The retention time for this history must be in accordance with that for backups (see chapter 12.5).

14.3. **Technical review of the applications after a change made to the operating platform**
   a) The service provider must document and implement a procedure that makes it possible to test, prior to putting them into production, all of the applications in order to verify the absence of all undesirable effects on the activity or on the security of the service.

14.4. **Secure development environment**
   a) The service provider must implement a secure development environment that makes it possible to manage the entire development cycle of the information system of the service.
   
   b) The service provider must take the development environments into account in assessing the risks and in providing the protection in accordance with this reference document.

14.5. **Outsourced development**
   a) The service provider must document and implement a procedure that makes it possible to supervise and control the outsourced development activity of software and systems. This procedure must ensure that the outsourced development activity is compliant with the secure development policy of the service provider and makes it possible to achieve a level of security of the external development that is equivalent to that of internal development (see requirement 14.1 a).

14.6. **System security and compliance test**
   a) The service provider must subject the information systems, new or updated, to security functionality and compliance tests during development. It must document and implement a test procedure that identifies:
   - the tasks to be carried out;
   - the input data;
- the expected results at the output.

**14.7. Protection of test data**

a) The service provider must document and implement a procedure that makes it possible to ensure the integrity of the test data used in pre-production.

b) If the service provider wants to use client data coming from production to carry out tests, the service provider must first obtain approval from the client and anonymise it. The service provider must provide confidentiality for the data during anonymisation.
15. **Relations with third parties**

15.1. **Identification of third parties**

   a) The service provider must maintain an up-to-date list of all of the third parties that participate in the implementation of the service (host, developer, integrator, archiver, subcontractor operating on site or remotely, air-conditioning suppliers, etc.). This list must be complete, specify the contribution of the third party to the service and take account of subcontracting at several levels.

15.2. **Security in the agreements made with third parties**

   a) The service provider must require from the third parties that participate in the implementation of the service, in their contribution to the service, a level of security that is at least equivalent to that which it commits to maintain in its own security policy. It must do this through requirements, adapted to each third party and to its contribution to the service, in the specifications or in the security clauses of the partnership agreements. The service provider must include these requirements in the contracts signed with third parties.

   b) The service provider must contractualise, with each one of the third parties participating in the implementation of the service, audit clauses that allow an approval entity to check that these third parties comply with the requirements of this reference document.

   c) The service provider must define and allocate the roles and the responsibilities concerning the modification or the end of the contract that binds it to a third party participating in the implementation of the service.

15.3. **Monitoring and review of third party services**

   a) The service provider must document and implement a procedure that makes it possible to check on a regular basis the measures set up by the third parties participating in the implementation of the service in order to comply with the requirements of this reference document, in accordance with chapter 18.3.

15.4. **Managing changes made in the services of third parties**

   a) The service provider must document and implement a procedure for monitoring the changes made by the third parties participating in the implementation of the service that can affect the level of security of the information system of the service.

   b) When a change in the third party participating in the implementation of the service affects the level of security of the service, the service provider must inform all of the clients without delay in accordance with chapter 12.2 and implement the measures that make it possible to re-establish the previous level of security.

15.5. **Confidentiality undertakings**

   a) The service provider must document and implement a procedure that makes it possible to revise at least once a year the requirements in terms of non-disclosure or confidentiality undertakings with regards to third parties participating in the implementation of the service.
16. **Managing incidents linked to information security**

16.1. **Responsibilities and procedures**
   
a) The service provider must document and implement a procedure that makes it possible to provide fast and effective responses to security incidents. These procedures must define the means and the timeframes for communicating security incidents to all of the clients concerned as well as the level of confidentiality required for this communication.

b) The service provider must inform its employees and all of the third parties participating in the implementation of the service of this procedure.

16.2. **Reporting linked to information security**
   
a) The service provider must document and implement a procedure that requires its employees and third parties participating in the implementation of the service to report to it any security incident, established or suspected as well as any security breach.

b) The service provider must document and implement a procedure that allows all of the clients to report any security incident, established or suspected and any security breach.

c) The service provider must forward the security incidents and the associated recommendations in order to limit the impacts of them to the clients without delay. It must allow the client to choose the levels of severity of the incidents for which it wants to be informed.

d) The service provider must forward the security incidents to the competent authorities in accordance with the legal and regulatory requirements in effect.

16.3. **Assessment of events linked to information security and decision making**
   
a) The service provider must assess the events linked to information security and decide if they need to be qualified as security incidents. For the assessment, it must use one or more scales (estimation, assessment, etc.) shared with the client.

b) The service provider must use a classification that makes it possible to clearly identify the security incidents that affect data with respect to clients, in accordance with the results of the risk assessment.

16.4. **Response to incidents linked to information security**
   
a) The service provider must process the security incidents until they are resolved and must inform the clients in accordance with the procedures.

b) The service provider must archive the documents that provide details on the security incidents.

c) It is recommended that the service provider call upon a security incident response service provider [PRIS] that is approved to process security incidents that require additional expertise.

16.5. **Learning from incidents linked to information security**
   
a) The service provider must document and implement a continual improvement process in order to reduce the occurrence and the impact of the types of security incidents that have already been processed.

16.6. **Collecting proof**
   
a) The service provider must document and implement a procedure that makes it possible to record the information concerning security incidents and which could be used as evidence.
17. **Continuity of activity**

17.1. **Organisation of the continuity of activity**
   a) The service provider must document and implement a continuity of activity plan that takes information security into account.
   
b) The service provider must revise the continuity of activity plan annually and at each major change that can affect the service.

17.2. **Implementing continuity of activity**
   a) The service provider must document and implement procedures that make it possible to maintain or restore the operation of the service and to ensure the availability of the information at the level and within the timeframes for which the service provider has made a commitment with the client in the service agreement.

17.3. **Check, review and evaluate the continuity of activity**
   a) The service provider must document and implement a procedure that makes it possible to test the continuity of activity plan in order to ensure that it is pertinent and effective in a crisis situation.

17.4. **Availability of the means for information processing**
   a) The service provider must document and implement measures that allow it to respond to the need for the availability of the service defined in the service agreement (see chapter 19.1).
18. **Compliance**

18.1. **Identification of the legislation and of the contractual requirements that apply**
   a) The service provider must identify the legal, regulatory and contractual requirements in effect that apply to the service. In France, the service provider must consider at least the following texts:
      - personal data [LOI_IL];
      - professional confidentiality [CP_ART_226-13], where appropriate, without prejudice to the application of article 40, paragraph 2, of the Code of Criminal Procedure, relating to alerting a legal authority;
      - abuse of trust [CP_ART_314-1];
      - the confidentiality of private [CP_ART_226-15];
      - invasion of privacy [CP_ART_226-1];
      - fraudulent access to or presence in an information system [CP_ART_323-1].
   b) The service provider must document and implement procedures that make it possible to comply with the legal, regulatory and contractual requirements in effect that apply to the service, as well as the specific security needs (see requirement 8.3b)).
   c) The service provider must, when requested by a client, provide it with all of these procedures.
   d) The service provider must document and implement an active monitoring process of the legal, regulatory and contractual requirements in effect that apply to the service.

18.2. **Independent review of information security**
   a) The service provider must document and implement an audit programme over three years that defines the perimeter and the frequency of the audits in accordance with the management of change, policies, and the results of the risk assessment.
   b) The service provider must include in the audit programme one approved audit per year conducted by an approved audit service provider for information system security [PASSI]. The entire audit programme must in particular cover:
      - the audit of the configuration of the servers and network equipment included in the perimeter of the service. This audit is conducted by sampling and must include all of the types of equipment and servers present in the information system of the service;
      - the intrusion test for external access to the service;
      - if the service benefits from internal developments, the audit of the source code concerning the security functions implemented.

18.3. **Compliance with security policies and standards**
   a) The service provider via the information security manager must ensure on a regular basis the correct execution of all of the security procedures placed under its responsibility so as to guarantee that they comply with security policies and standards.

18.4. **Technical compliance examination**
   a) The service provider must document and implement a policy that makes it possible to verify the technical compliance of the service with the requirements of this reference document. This policy must define the objectives, methods, frequencies, expected results and corrective measures.
19. **Additional requirements**

19.1. **Service agreement**

a) The service provider must establish a service agreement with each one of the clients of the service. Any modification to the service agreement must be submitted to the client for approval.

b) The service provider must identify the following in the service agreement:

- the responsibilities of each of the parties: service provider and third parties involved in the supply of the service, clients, etc.;
- elements that are explicitly excluded from the responsibilities of the service provider;
- the location of the service. The location of the support must be specified when it is carried out from a State outside of the European Union, as provided for in requirement 19.2 d).

c) The service provider must propose a service agreement that applies the law of a Member State of the European Union. The applicable law must be identified in the service agreement.

d) The service provider must describe in the service agreement the technical and organisational means that it implements in order to provide compliance within the applicable law.

e) The service provider must include in the service agreement a clause for revising the agreement that calls in particular for termination without penalty for the client in the case of loss of approval granted to the service.

f) The service provider must include in the service agreement a reversibility clause that allows the client to recover all of its data (supplied directly by the client or produced in the framework of the service from data or actions of the client).

g) The service provider must provide this reversibility via one of the following technical methods:

- making files available in one or several documented formats that can be used outside of the service provided by the service provider;
- the setting up of technical interfaces that allow for access to the data according to a documented and usable diagram (API, pivot format, etc.).

The technical particulars for the reversibility are mentioned in the service agreement.

h) The service provider must indicate in the service agreement the level of availability of the service.

i) The service provider must indicate in the service agreement that it cannot avail itself of the ownership of the data transmitted and managed by the client. This data is the property of the client.

j) The service provider must indicate in the service agreement that it does not disclose any information concerning the provision of service to third parties, except with formal authorisation in writing from the client.

k) The service provider must indicate in the service agreement if it authorises remote access for administration or support actions to the information system of the service.

l) The service provider must specify in the service agreement that:

- the service is approved and include the proof of approval;
- the client can file a complaint concerning the approved service with ANSSI;
- the client authorises ANSSI and the approval entity to audit the service and its information system of the service in order to check that they comply with the requirements of this reference document.

m) The service provider must specify in the service agreement that the client authorises, in accordance with this reference document (see requirement 18.2 b), an approved audit service provider for information system security [PASSI] mandated by the service provider to audit the service and its information system in the framework of the control plan.

19.2. **Location of data**

a) The service provider must document and forward to the client the location of the storage and of the processing of the data.

b) The service provider must store and process the client data within the European Union.

c) The administration and supervision operations of the service must be carried out from the European Union.

d) The service provider can conduct support operations for clients from a State outside of the European Union. It must document the list of operations that can be carried out by client support from a State outside of the European Union, and the mechanisms that make it possible to ensure the access control to it and supervision from the European Union.

19.3. **Regionalisation.**

a) The service provider must ensure that the interfaces of the service that are accessible to the client are at least available in French.

b) The service provider must provide first-level support in French.

19.4. **End of contract**

a) At the end of the contract that binds the service provider and the client, whether the contract has reached its term or for any other cause, the service provider must ensure a secure deletion of all of the data of the client. This deletion can be carried out according to one of the following methods, and this within a period of time mentioned in the service agreement:

- erasure by full re-writing of any media that has hosted this data;
- deletion of the keys used for encrypting storage areas of the client described in chapter 10.1;
- secure recycling, in the conditions set forth in chapter 11.9.

b) At the end of the contract, the service provider must delete the technical data concerning the client (directory, certificates, access configuration, etc.).
# Appendix 1 Documentary references

## I. Codes, laws and regulations

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document</th>
</tr>
</thead>
</table>

## II. Standards and technical documents

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SNC_AVANCE]</td>
<td>Cloud IT service providers (SecNumCloud), reference documentation on requirements – Advanced Level, ANSSI, current version. Available at <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a></td>
</tr>
<tr>
<td>[EX_DONNEES]</td>
<td>Documents on additional requirements that apply to Cloud IT service providers who wish to host data pertaining to a specific regulation, ANSSI, current version. Available at <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a></td>
</tr>
<tr>
<td>Reference</td>
<td>Document</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[NT_SSH]</td>
<td>Recommendations for a secure use of (Open) SSH, technical note no. DAT-NT-007/ANSSI/SDE/NP of 17 August 2015, ANSSI. Available at <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a></td>
</tr>
</tbody>
</table>

III. Other documentary references

<table>
<thead>
<tr>
<th>Reference</th>
<th>Document</th>
</tr>
</thead>
</table>
Appendix 2 Recommendations to commissioning entities

This annex lists ANSSI’s recommendations for commissioning entities in relation to cloud IT services.

a) When the commissioning entity is an administrative authority or an operator of critical importance, it can ask ANSSI to take part in defining the list of specifications that is the subject of a call for tender or of a contract.

b) It is recommended that the commissioning entity choose its service provider from among those listed in the catalogue of approved service providers published on ANSSI’s website, with the approval of a cloud IT service provider demonstrating its compliance with all of the requirements of this reference document.

c) To benefit from an approved provision of service, i.e. one that complies with all the requirements of this reference documentation, the commissioning entity must:
- choose the service provider from the catalogue of approved service providers published on the ANSSI site;
- require the service provider to stipulate in the service agreement that the service provided is an approved service.

Approved service providers retain the ability to provide non-approved services. Using a service provider from among those listed in the catalogue of approved service providers is therefore a necessary condition but not a sufficient one for receiving an approved service: the commissioning entity must also require an approved service.

d) It is recommended that the commissioning entity use the guide to purchasing security products and [GUIDE_ACHAT] which aims at supporting the commissioning entity’s purchasing functions during calls for tender.

e) In accordance with the process for approving trusted service providers [PROCESS_QUALIF] make a complaint to ANSSI against a service provider that the commissioning entity considers to have not complied with one or more requirements of this reference documentation as part of an approved provision of service.

If, following investigation of the complaint, it is determined that the service provider has not complied with one or more of the requirements of this reference document in providing an approved service, and depending on the severity of such breach, the service provider’s approval may be suspended or revoked, or the scope of its approval may be reduced.

f) Approval of a service provider does not attest to its capacity to access or hold classified defence information [IGI_1300].

g) A service provider’s approval does not attest to its ability to access or hold controlled information system security items (ACSSI) [II_910].