

Prime Minister

**French National
Cyber Security Agency**

*Agence nationale de la sécurité
des systèmes d'information*

Cloud computing service providers (SecNumCloud)

Requirements baseline

Version 3.2 dated 8 March 2022



This document is a **courtesy translation** of the initial French document “Prestataires de services d’informatique en nuage (SecNumCloud) – référentiel d’exigences”, available on <https://cyber.gouv.fr/secnumcloud>. In case of conflicts between these two documents, the initial French version is considered as the only reference.

VERSION HISTORY			
DATE	VERSION	DOCUMENT EVOLUTION	EDITOR
08/03/2022	3.2	<i>Published for translated document.</i>	ANSSI

Comments on this document should be sent to:

**Agence nationale de la sécurité des
systèmes d'information**
 SGDSN/ANSSI
 51 boulevard de La Tour-Maubourg
 75700 Paris 07 SP
qualification@ssi.gouv.fr

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	2/55

CONTENTS

1. INTRODUCTION	7
1.1. GENERAL OVERVIEW	7
1.1.1. <i>Context</i>	7
1.1.2. <i>Document subject</i>	7
1.1.3. <i>Document structure</i>	8
1.2. DOCUMENT IDENTIFICATION	8
1.3. ACRONYMS AND DEFINITIONS	8
1.3.1. <i>Acronyms</i>	8
1.3.2. <i>Definitions</i>	9
1.3.3. <i>Roles</i>	10
2. ACTIVITIES COVERED BY THE BASELINE.....	11
2.1. PROVISION OF SAAS SERVICES	11
2.2. PROVISION OF PAAS SERVICES.....	11
2.3. PROVISION OF CAAS SERVICES.....	11
2.4. PROVISION OF IAAS SERVICES.....	11
3. QUALIFICATION OF CLOUD SERVICE PROVIDERS.....	13
3.1. QUALIFICATION SCHEME	13
3.2. SCOPE OF THE QUALIFICATION	13
3.3. WARNINGS	13
3.3.1. <i>Risks Associated with the Lack of Qualification</i>	13
3.3.2. <i>Risks related to information protection</i>	13
4. SECURITY LEVEL	14
5. INFORMATION SECURITY POLICIES AND RISK MANAGEMENT	15
5.1. PRINCIPLES.....	15
5.2. INFORMATION SECURITY POLICY.....	15
5.3. RISK ASSESSMENT	15
6. INFORMATION SECURITY ORGANISATION	17
6.1. INFORMATION SECURITY FUNCTIONS AND RESPONSIBILITIES	17
6.2. SEPARATION OF DUTIES.....	17
6.3. RELATIONS WITH AUTHORITIES	17
6.4. RELATIONS WITH SPECIALIST WORKING GROUPS	17
6.5. INFORMATION SECURITY IN PROJECT MANAGEMENT	18
7. HUMAN RESSOURCES SECURITY	19
7.1. CANDIDATE SELECTION	19
7.2. EMPLOYMENT CONDITIONS	19
7.3. AWARENESS, EDUCATION AND TRAINING ON INFORMATION SECURITY	20
7.4. DISCIPLINARY PROCESS	20
7.5. TERMINATION, EXPIRY OR MODIFICATION OF EMPLOYMENT CONTRACT	20
8. ASSET MANAGEMENT.....	21
8.1. ASSET INVENTORY AND OWNERSHIP	21
8.2. RETURN OF ASSETS.....	21

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	3/55

8.3.	IDENTIFICATION OF INFORMATION SECURITY REQUIREMENTS	21
8.4.	INFORMATION LABELLING AND HANDLING.....	21
8.5.	REMOVABLE MEDIA MANAGEMENT	21
9.	ACCESS CONTROL AND IDENTITY MANAGEMENT	22
9.1.	ACCESS CONTROL POLICY.....	22
9.2.	USER REGISTRATION AND DE-REGISTRATION.....	22
9.3.	ACCESS RIGHTS MANAGEMENT	22
9.4.	USER ACCESS RIGHTS REVIEW	23
9.5.	USER AUTHENTICATION MANAGEMENT	23
9.6.	ACCESS TO ADMINISTRATION INTERFACES	23
9.7.	RESTRICTION OF ACCESS TO INFORMATION.....	24
10.	CRYPTOLOGY	26
10.1.	ENCRYPTION OF STORED DATA.....	26
10.2.	ENCRYPTION OF NETWORK TRAFFIC	26
10.3.	PASSWORD HASHING.....	26
10.4.	NON-REPUDIATION	27
10.5.	SECRET MANAGEMENT	27
10.6.	ROOTS OF TRUST	27
11.	PHYSICAL AND ENVIRONMENTAL SECURITY	28
11.1.	PHYSICAL SECURITY PERIMETERS	28
11.1.1.	<i>Public zones</i>	28
11.1.2.	<i>Private zones</i>	28
11.1.3.	<i>Sensitive zones</i>	28
11.2.	PHYSICAL ACCESS CONTROL.....	28
11.2.1.	<i>Private zones</i>	28
11.2.2.	<i>Sensitive zones</i>	29
11.3.	PROTECTION AGAINST EXTERNAL AND ENVIRONMENTAL THREATS.....	29
11.4.	WORK IN PRIVATE AND SENSITIVE ZONES	30
11.5.	DELIVERY AND LOADING ZONES	30
11.6.	CABLE SECURITY	30
11.7.	EQUIPMENT MAINTENANCE	30
11.8.	ASSET DECOMMISSIONING.....	30
11.9.	SAFE RECYCLE OF EQUIPMENT	31
11.10.	EQUIPMENT AWAITING USE	31
12.	OPERATIONAL SECURITY	32
12.1.	DOCUMENTED OPERATING PROCESS	32
12.2.	CHANGE MANAGEMENT	32
12.3.	SEPARATION OF DEVELOPMENT, TESTING AND PRODUCTION ENVIRONMENTS.....	32
12.4.	MEASURES AGAINST MALICIOUS CODE	32
12.5.	DATA BACKUP	32
12.6.	EVENT LOGGING	33
12.7.	PROTECTION OF LOGGED INFORMATION	33
12.8.	CLOCK SYNCHRONISATION	34
12.9.	EVENT ANALYSIS AND CORRELATION	34
12.10.	INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS.....	34

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	4/55

12.11.	MANAGEMENT OF TECHNICAL VULNERABILITIES	35
12.12.	ADMINISTRATION	35
12.13.	REMOTE DIAGNOSIS AND MAINTENANCE OF INFRASTRUCTURE COMPONENTS	35
12.14.	MONITORING OF OUTBOUND TRAFFIC FROM THE INFRASTRUCTURE	36
13.	COMMUNICATION SECURITY	37
13.1.	INFORMATION SYSTEM MAPPING	37
13.2.	NETWORK SEGMENTATION	37
13.3.	NETWORK MONITORING	38
14.	ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS	39
14.1.	SECURE DEVELOPMENT POLICY	39
14.2.	SYSTEM CONTROL CHANGE PROCEDURES	39
14.3.	TECHNICAL REVIEW OF APPLICATION AFTER CHANGES MADE TO OPERATIONAL PLATFORM	39
14.4.	SECURE DEVELOPMENT ENVIRONMENT	39
14.5.	OUTSOURCED DEVELOPMENT	39
14.6.	SECURITY AND COMPLIANCE TESTING OF THE SYSTEM	39
14.7.	PROTECTION OF TESTING DATA	40
15.	RELATIONS WITH THIRD-PARTIES	41
15.1.	IDENTIFICATION OF THIRD-PARTIES	41
15.2.	SECURITY IN AGREEMENTS CONCLUDED WITH THIRD-PARTIES	41
15.3.	MONITORING AND REVIEW OF THIRD-PARTY SERVICES	41
15.4.	MANAGEMENT OF CHANGES MADE TO THIRD-PARTY SERVICES	41
15.5.	CONFIDENTIALITY COMMITMENTS	41
16.	MANAGEMENT OF INCIDENTS TO INFORMATION SECURITY	42
16.1.	RESPONSIBILITIES AND PROCEDURES	42
16.2.	REPORTS RELATED TO SECURITY OF INFORMATION SECURITY	42
16.3.	ASSESSMENT OF INFORMATION SECURITY EVENTS AND MAKING OF DECISION	42
16.4.	RESPONSE TO INFORMATION SECURITY INCIDENTS	42
16.5.	LEARNING FROM INFORMATION SECURITY INCIDENTS	43
16.6.	EVIDENCE COLLECTION	43
17.	BUSINESS CONTINUITY	44
17.1.	ORGANISATION OF BUSINESS CONTINUITY	44
17.2.	IMPLEMENTATION OF BUSINESS CONTINUITY	44
17.3.	VERIFYING, REVIEWING AND EVALUATING THE BUSINESS CONTINUITY	44
17.4.	AVAILABILITY OF INFORMATION PROCESSING MEANS	44
17.5.	BACKUP OF TECHNICAL INFRASTRUCTURE CONFIGURATION	44
17.6.	PROVISION OF A BACKUP SERVICE FOR THE COMMISSIONING ENTITY'S DATA	44
18.	COMPLIANCE	45
18.1.	IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL REQUIREMENTS	45
18.2.	INDEPENDENT REVIEW OF INFORMATION SECURITY	45
18.2.1.	<i>Continuous review</i>	45
18.2.2.	<i>Initial review</i>	46
18.2.3.	<i>Review of major changes</i>	46
18.3.	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS	46

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	5/55

18.4.	TECHNICAL COMPLIANCE REVIEW	47
19.	ADDITIONAL REQUIREMENTS	48
19.1.	SERVICE AGREEMENT	48
19.2.	DATA LOCATION	49
19.3.	REGIONALISATION	50
19.4.	END OF THE CONTRACT	50
19.5.	PERSONNEL PROTECTION.....	50
19.6.	PROTECTION AGAINST NON-EUROPEAN LAW.....	50
APPENDIX 1	DOCUMENT REFERENCES	52
I.	CODES, LEGISLATIVE AND REGULATORY TEXTS	52
II.	TECHNICAL DOCUMENTS AND STANDARDS.....	52
III.	OTHER DOCUMENT REFERENCES	54
APPENDIX 2	RECOMMENDATIONS FOR COMMISSIONING ENTITIES	55

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	6/55

1. Introduction

1.1. General overview

1.1.1. Context

Cloud computing can be defined as an IT management model that allows access, via a network, to shared and configurable computing resources. These resources are allocated on demand, and sometimes in a self-service manner.

The difference between traditional shared external hosting and cloud-type hosting lies in the fact that the latter is sometimes characterised by the dynamic or automatic provision of resources, without human intervention from the hosting provider.

This baseline applies to both traditional external hosting contexts and cloud-type hosting contexts.

Shared hosting today tends to use cloud computing platforms rather than traditional hosting platforms; for this reason, this baseline will use the term “**cloud computing**” to refer to any type of shared external hosting.

This baseline covers cloud computing services and aims at the qualification of providers offering such services.

Cloud service providers offer various services, typically classified into four types of activity: Infrastructure as a Service (IaaS), Container as a Service (CaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These activities are detailed in Chapter 2.

The approach of specifically contracting security for each external hosting project has shown its limitations: offers are most often integrated, making subsequent negotiation by each commissioning entity impractical. Moreover, it can be difficult to encourage each client to carry out regular audits of the services provided.

A centralised approach, defining a baseline that promotes the emergence of qualified services, has therefore been adopted: it lets security issues to be addressed globally and effectively, with service providers having a stable baseline within which to move towards qualification, and users being able to base their trust on this qualification.

This baseline is notably based on the international standard [\[ISO27001\]](#), whose Appendix A structure it also follows. However, this baseline includes additional requirements that differentiate it from the existing standard and do not imply equivalence between the two sets of rules.

1.1.2. Document subject

This document constitutes the requirements baseline applicable to a cloud service provider (SecNumCloud), hereinafter referred to as the "service provider".

It is intended to enable the qualification of this category of service providers according to the procedures described in Chapter 3.

It provides the client with guarantees regarding the service provider's and its staff's skills, the quality of the services offered, and the level of trust the client can place in the service provider.

It may also be used as best practice, outside of any regulatory context.

It does not exclude the application of national laws and regulations, nor the general rules imposed on service providers in their capacity as professionals, including their duty of advice towards their clients.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	7/55

This baseline is designed without presumption regarding the technologies that may be used to implement the services. In particular, the term "cloud computing" used within this baseline does not necessarily imply the use of virtualisation solutions.

1.1.3. Document structure

Chapter 1 outlines the introduction to this baseline.

Chapter 2 describes the activities covered by this baseline.

Chapter 3 presents the qualification procedures, which certify the compliance of cloud service providers with the applicable requirements.

Chapter **Erreur ! Source du renvoi introuvable.** outlines the qualification levels applicable to cloud service providers.

Chapters **Erreur ! Source du renvoi introuvable.** to 19 detail the requirements that must be met by qualified service providers.

Appendix 1 provides the references to legislative, regulatory, normative, and other texts mentioned in this baseline.

Appendix 2 offers recommendations for commissioners of cloud computing services.

1.2. Document identification

The present baseline is entitled "Cloud computing service providers (SecNumCloud) – Requirements control baseline". It can be identified by its name, version number, and update date.

1.3. Acronyms and definitions

1.3.1. Acronyms

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	<i>Agence nationale de la sécurité des systèmes d'information</i> , the French National Cyber Security Agency
CaaS	Container as a service
CNIL	<i>Commission nationale de l'informatique et des libertés</i> , the French Data Protection Authority (DPA)
EBIOS	<i>Expression des besoins et identification des objectifs de sécurité</i> (Expression of requirements and identification of security objectives)
IaaS	Infrastructure as a service
PaaS	Platform as a service
PASSI	<i>Prestataire d'audit de la sécurité des systèmes d'information</i> (cyber security audit service provider)
PDIS	<i>Prestataire de détection des incidents de sécurité</i> (cyber security incident detection service provider)
PRIS	<i>Prestataire de réponse aux incidents de sécurité</i> (cyber security incident response service provider)
SaaS	Software as a service
SDN	Software Defined Network

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	8/55

1.3.2. Definitions

Administration actions – a set of actions involving the installation, removal, modification, and consultation of the configuration of a system participating in the service information system, and likely to modify its operation or security.

Audit – a systematic, independent, and documented process aimed at obtaining evidence and assessing it objectively to determine the extent to which the requirements of a baseline are met.

Asset – any item representing value for the service to be qualified.

Major change - any action planned by the service provider that, by its nature or scope, could compromise the security of the service (e.g., modification of the organisation, change in a procedure, addition, modification, or removal of a component in the technical infrastructure).

Cloud computing – a model that enables easy, usually on-demand, access to a set of shared and configurable IT resources through a network.

Commissioning entity – the entity that engages a cloud service provider.

Container - a user-space execution instance, isolated from other instances by abstraction mechanisms provided by the kernel of an operating system.

State of the art - a set of best practices, technologies, and reference documents related to information system security that are publicly accessible, along with information that can be derived from them in an obvious manner. These documents may be published online by the information security community, distributed by reference organisations, or be of a regulatory origin.

Shared external hosting – a model that provides easy access, typically over a network, to a set of shared and configurable IT resources.

Information security incident – one or more undesirable or unexpected events related to information security, with a high probability of compromising the operations related to the organisation's activity or threatening information security.

Technical infrastructure – the set of hardware and software components necessary for delivering a cloud computing service (IaaS, CaaS, PaaS, SaaS, etc.).

Administration interface – a software interface that allows an entity with the required privileges (an administrator, service account, DevOps developer, etc.) to perform administration actions on an information system.

Middleware - software that resides between an operating system and the applications running on it, facilitating interaction between them.

Threat – a potential cause of an undesirable event that could harm a system or an organisation.

Security measure – a measure that alters the likelihood or severity of a risk. It includes policies, procedures, guidelines, and organisational practices or structures, and can be administrative, technical, managerial, or legal in nature.

Policy – the intentions and direction of an organisation as formalised by its management.

Service provider – an entity offering a cloud computing service and seeking qualification.

Cyber security audit service provider – an organisation performing security audit services for information systems. It is deemed qualified if a certification body has attested to its compliance with the *Requirements Baseline for cyber security audit service provider* (Référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	9/55

Virtualised resources – is the abstraction of a system’s physical resources (e.g., CPU, RAM) provided by the technical infrastructure.

Risk – is an effect of uncertainty on the achievement of objectives. It is expressed in terms of the combination of the consequences of an event and its likelihood.

Information system security – set of technical and non-technical protective measures ensuring an information system maintains the availability, integrity, and confidentiality of data processed or transmitted, as well as the related services provided or made accessible by these systems.

IT supervision – monitoring the proper functioning of an information system or service. It involves data collection (metrics, alerts, etc.) but does not allow interaction with the monitored element (which falls under administration tasks).

Technical support – a set of diagnostic actions aimed at resolving issues encountered by the commissioning entities. By default, no access to the commissioning entities' data is permitted in the course of these tasks. If resolving the issue requires an action from the service provider, this then falls under administration and must be performed under the appropriate conditions.

Information system – an organised set of resources (hardware, software, personnel, data, and procedures) that enables the processing and dissemination of information.

Vulnerability – A weakness in an asset or measure that could be exploited by a threat or a group of threats.

1.3.3. Roles

Administrator – a user with privileged rights allowing them to perform the administration tasks assigned to them.

Infrastructure administrator – an administrator responsible for managing and maintaining the operational and security conditions of the service's technical infrastructure.

User – any person with an account within the scope of the service. This generic term includes both end users and administrators.

End user – the person ultimately benefiting from the implemented service. This could be the staff of the commissioning entity in the case of an internal service, or the commissioning entities themselves if the service is offered externally.

The role of Infrastructure Administrator always remains the responsibility of the service provider.

Depending on the shared responsibility model between the service provider and the commissioning entity, as described in the service agreement, roles such as Security Administrator, System Administrator, Network Administrator, etc., may fall under the responsibility of either the provider or the commissioning entity.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	10/55

2. Activities covered by the baseline

This Chapter outlines the various activities addressed by the baseline.

2.1. Provision of SaaS services

This service involves the service provider offering applications hosted on a cloud computing platform. The commissioning entity does not have control over the underlying cloud platform. The service provider manages all technical aspects requiring IT expertise, transparently to the commissioning entity. However, the commissioning entity retains the ability to make some business-specific configurations within the application.

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

2.2. Provision of PaaS services

This service involves the service provider offering application hosting platforms. The commissioning entity does not have control over the underlying technical infrastructure, which is managed and operated by the service provider (network, servers, OS, storage, etc.). However, the commissioning entity retains control over the applications deployed on this platform. Depending on the role distribution defined in the service agreement, it may also have control over certain platform services or specific configuration elements.

Example: baselines such as Apache, Tomcat, PHP, and MySQL, enabling the development of web applications

2.3. Provision of CaaS services

This service involves the provision of tools for the deployment and orchestration of containers. The commissioning entity does not have control over the underlying technical infrastructure (network, storage, servers, operating system), which is managed and operated by the service provider. However, the commissioning entity retains control over system tools, libraries, middleware, and the application code.

2.4. Provision of IaaS services

This service involves the provision of abstracted computing resources (CPU power, memory, storage, etc.). The IaaS model allows the commissioning entity to utilise externalised, potentially virtualised, resources. The commissioning entity retains control over the operating system (OS), storage, deployed applications, and certain network components (such as firewalls).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	11/55

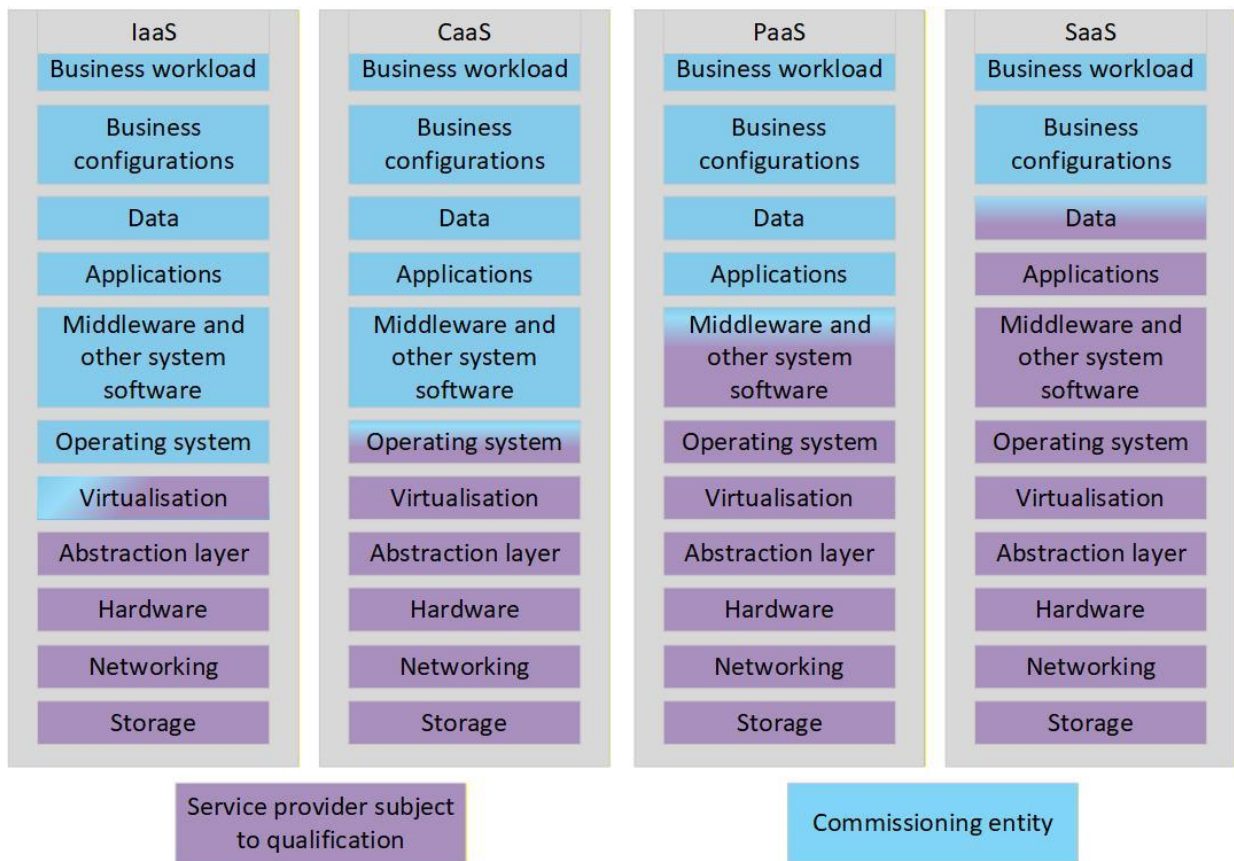


Figure 1 – Responsibility allocation model¹ by service type

¹ Other allocation models exist depending on the technical implementation and may not cover all the service components identified here (e.g., CaaS Baremetal)

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	12/55

3. Qualification of cloud service providers

3.1. Qualification scheme

The baseline sets out the requirements and recommendations intended for cloud computing service providers.

The qualification of a cloud service provider is carried out in accordance with the trust service provider qualification process [\[PROCESS_QUALIF\]](#) and serves to certify the provider's compliance with the requirements of the baseline.

The requirements must be met by service providers in order to obtain qualification. The recommendations are provided as best practices and are not subject to assessment as part of the qualification process.

3.2. Scope of the qualification

To be qualified, a service provider must meet all the requirements of this baseline for the chosen scope. The scope is defined by all or part of the activities described in Chapter 2.

Qualified service providers retain the ability to carry out services outside the scope for which they are qualified, but in such cases, they may not claim the qualification for these services.

A qualified cloud service provider may be associated with the provision of additional services (development, security product integration, etc.) without losing the benefit of the qualification.

3.3. Warnings

3.3.1. Risks Associated with the Lack of Qualification

An unqualified cloud service provider may potentially increase the exposure of the commissioning entities to certain risks, including the leakage of confidential information, compromise, loss, or unavailability of their information system.

Therefore, in the case of an unqualified service, the commissioning entity should request from the service provider a document listing all the requirements of this baseline that are not covered by the service, in order to understand the risks to which the commissioning entities are exposed.

3.3.2. Risks related to information protection

Compliance with the SecNumCloud baseline does not replace the legal or regulatory requirements applicable to certain specific data, such as *Diffusion Restreinte* data or health data.

The clauses in this baseline referring to qualified products apply only insofar as these products exist.

Furthermore, this baseline is based on an objective of protecting the commissioning entity's data, but it does not provide strong technical guarantees against the service provider accessing data processed on the service information system; it only establishes contractual commitments. Commissioning entities wishing to ensure the technical protection of their data against service provider access must therefore implement additional encryption measures under their control.

Finally, it should be noted that the virtualisation commonly used in cloud IT services should not be considered equivalent to physical separation as a means of isolation.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	13/55

4. Security level

Compliance with the SecNumCloud baseline aims at achieving a level of security suitable for storing and processing data for which a security incident would have a significant impact on the commissioning entity. It notably ensures adherence to IT security best practices, as described in the ANSSI's guideline [\[HEALTHY\]](#).

Compliance of a cloud service provider with this baseline does not certify its conformity with the baseline *Politique de sécurité des systèmes d'information de l'État* (State information systems security policy) [\[PSSIE\]](#).

The commissioning entity's use of a SecNumCloud qualified service for hosting data subject to legal or regulatory requirements (such as *Diffusion Restreinte* data, health data, etc.) requires compliance with additional requirements, which must be determined as part of an authorisation process including, in particular, a risk assessment (see Chapter 3.3.2).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	14/55

5. Information security policies and risk management

5.1. Principles

- a) The service provider must operate the service according to state of the art for the selected type of activity: use stable software that benefits from ongoing security patch management, and configured to achieve an optimal level of security.
- b) The service provider must comply the guideline for a healthy information system of ANSSI [\[HEALTHY\]](#), at the enhanced level, to information system of the service.

5.2. Information security policy

- a) The service provider must document and implement an information security policy applicable to the service.
- b) The information security policy must identify the service provider's commitments regarding compliance with the applicable national laws and regulations, according to the nature of the information that may be entrusted by the commissioning entity to the service provider. However, it remains the commissioning entity's responsibility to ensure compliance with the legal and regulatory requirements applicable to the data they actually entrust to the service provider.
- c) The information security policy must cover, in particular, the topics addressed in Chapters 6 to 19 of this reference baseline.
- d) The service provider's management must formally approve the information security policy.
- e) The service provider must review the information security policy annually, and upon any major change that may impact the service.

5.3. Risk assessment

- a) The service provider must document a risk assessment covering the entire scope of the service.
- b) The service provider must take into account the following in the risk assessment:
 - the management of the commissioning entity's information with varying security requirements;
 - risks that could impact the rights and freedoms of the individuals concerned in case of unauthorised access, unwanted modification, or loss of personal data;
 - risks of failure in the isolation mechanisms for shared technical infrastructure resources (memory, processing, storage, network) between commissioning entities;
 - risks related to incomplete or insecure deletion of data stored in memory or storage spaces shared between commissioning entities, particularly during reallocation of memory and storage spaces;
 - risks related to the exposure of administration interfaces on a public network;
 - risks to the confidentiality of commissioning entity data from third-parties involved in providing the service (suppliers, subcontractors, etc.);
 - risks related to natural events and physical disasters;
 - risks related to segregation of tasks (see 6.2.a);

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	15/55

- risks associated with development environments (see 14.4.b).
- c) The service provider must list, in a specific document, the residual risks related to the existence of non-European laws aimed at collecting data or metadata from the commissioning entities without their prior consent.
- d) The service provider must make available to the commissioning entity, upon request, the elements for assessing the risks related to subjecting the commissioning entity's data to the laws of a non-European Union country.
- e) When there are specific legal, regulatory, or sectoral requirements related to the types of information entrusted by the commissioning entity to the service provider, the service provider must take these into account in their risk assessment, ensuring compliance with all the requirements of this reference baseline on one hand, and ensuring that the level of security established by complying with the requirements of this reference baseline is not lowered on the other.
- f) The service provider's management must formally accept the residual risks identified in the risk assessment.
- g) The service provider must review the risk assessment annually, and upon any major change that could impact the service.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	16/55

6. Information security organisation

6.1. Information security functions and responsibilities

- a) The service provider must document and implement an internal security governance baseline to ensure the definition, deployment, and ongoing operational oversight of information security throughout its organisation.
- b) The service provider must appoint a chief information security officer and a security officer.
- c) The service provider must define and assign information security responsibilities for all personnel involved in the delivery and operation of the service.
- d) Following any major change that may impact the service, the service provider must ensure that the allocation of information security responsibilities remains appropriate and up to date.
- e) The service provider must define and assign responsibilities relating to the protection of personal data, in accordance with its role in personal data processing (data controller, data processor, or joint controller).
- f) Where the service provider processes a large volume of data that includes special categories of personal data as defined under the [\[GDPR\]](#), it must appoint a Data Protection Officer (DPO).
- g) Regardless of the volume of personal data processed, the service provider should appoint a Data Protection Officer.
- h) The service provider must conduct, or contribute to, a Data Protection Impact Assessment (DPIA) when processing is likely to result in a high risk to the rights and freedoms of data subjects (e.g., processing of special categories of personal data as defined in the [\[GDPR\]](#), large-scale data processing, etc.). This assessment must include a legal evaluation of compliance with fundamental principles and rights, as well as a more technical analysis of the controls and security measures implemented to safeguard individuals against privacy risks.

6.2. Separation of duties

- a) The service provider must identify risks associated with the accumulation of responsibilities or tasks, incorporate these risks into its risk assessment, and implement appropriate measures to mitigate them.

6.3. Relations with authorities

- a) The service provider should establish appropriate relationships with the competent authorities responsible for information security and personal data protection, and, where applicable, with relevant sectoral authorities depending on the nature of the information entrusted to the service provider by the commissioning entity.

6.4. Relations with Specialist Working Groups

- a) The service provider should maintain suitable contacts with expert groups or recognised sources of information, in particular to monitor emerging threats and identify appropriate security measures to address them.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	17/55

6.5. Information security in project management

- a) The service provider must document a risk assessment prior to any project that may have an impact on the service, regardless of the nature of the project.
- b) Where a project affects, or is likely to affect, the security level of the service, the service provider shall notify the commissioning entity and inform it in writing of potential impacts, measures implemented to mitigate those impacts, and residual risks applicable to it.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	18/55

7. Human resources security

7.1. Candidate selection

- a) The service provider must document and implement a personnel background-verification procedure in compliance with applicable laws and regulations.

Such verifications must apply to all individuals involved in the delivery of the service and must be proportional to the sensitivity or specificity of the commissioning entity information entrusted to the service provider, as well as to the risks identified.

- b) For personnel with high-privilege administration access to the software and hardware components of the infrastructure, the service provider must apply enhanced screening measures to ensure that their background is not incompatible with the functions they are required to perform.

High-privilege administration access includes the ability to perform actions enabling privilege escalation, actions without technical traceability, or actions allowing the disabling or alteration of technical logs or audit trails.

7.2. Employment conditions

- a) The service provider must maintain an ethics charter, incorporated into its internal regulations, which must include in particular the following provisions:

- services must be performed with loyalty, discretion, and impartiality, and in conditions ensuring the confidentiality of the information processed;
- personnel must use only the methods, tools, and techniques approved by the service provider;
- personnel must commit not to disclose to any third-party—whether anonymised or decontextualised—any information obtained or generated in the course of the service, except with the commissioning entity’s formal written authorisation;
- personnel must commit to reporting to the service provider any manifestly unlawful content discovered during the performance of the service;
- personnel must commit to complying with applicable national laws and regulations, and with best practices relevant to their duties.

- b) The service provider must require all individuals involved in the delivery of the service to sign the ethics charter.

- c) The service provider must include, in the employment contract of any personnel with high-privilege administration access to the components or hardware of the service infrastructure, a responsibility clause referring to labour laws governing the protection of trade secrets and intellectual property. High-privilege administration access includes actions enabling privilege escalation, actions that leave no technical trace, or actions that can disable or alter technical logs or audit trails.

- d) The service provider must, upon request from a commissioning entity, make its internal regulations and the ethics charter available to that commissioning entity.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	19/55

7.3. Awareness, education and training on information security

- a) The service provider must ensure that all individuals involved in the delivery of the service receive awareness on information security and on risks relating to personal data protection. The service provider must communicate to them any updates to the relevant policies and procedures applicable to their duties.
- b) The service provider must document and implement a training plan on information security that is appropriate to the service and to the responsibilities of the personnel concerned.
- c) The service provider's chief information security officer must formally validate the information security training plan.

7.4. Disciplinary process

- a) The service provider must document and implement a disciplinary process applicable to all individuals involved in the delivery of the service who breach the information security policy.
- b) The service provider must, upon request from a commissioning entity, make available the sanctions applicable in the event of a breach of the information security policy.

7.5. Termination, expiry or modification of employment contract

- a) The service provider must define and assign roles and responsibilities relating to the termination, expiry, or modification of any employment contract with personnel involved in the delivery of the service.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	20/55

8. Asset management

8.1. Asset inventory and ownership

- a) The service provider must maintain an up-to-date inventory of all equipment used to deliver the service. For each item of equipment, this inventory must specify:
 - the equipment's identification information (names, IP addresses, MAC addresses, etc.);
 - the function of the equipment;
 - the equipment model;
 - the location of the equipment;
 - the owner of the equipment;
 - the need of security of the information (as defined in Chapter 8.3).
- b) The service provider must maintain an up-to-date inventory of all software used to deliver the service. This inventory must identify, for each software, its version and the equipment on which it is installed.
- c) The service provider must ensure the validity of software licences throughout the duration of the service.

8.2. Return of assets

- a) The service provider must document and implement an asset return procedure to ensure that each person involved in the delivery of the service returns all assets in their possession at the end of their employment period or contract.

8.3. Identification of information security requirements

- a) The service provider must identify the various information security requirements relating to the service
- b) When the client entrusts the provider with data subject to specific legal, regulatory, or industry-specific constraints, the provider must identify the specific security requirements associated with these constraints.

8.4. Information labelling and handling

- a) The service provider should document and implement a procedure for labelling and handling of all information involved in the delivery of the service, in accordance with its security requirements as defined in Chapter 8.3.

8.5. Removable media management

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

When removable media are used on the technical infrastructure or for administration tasks, such media must be dedicated to a single usage.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	21/55

9. Access control and identity management

Unless explicitly stated otherwise, this Chapter concerns access control and identity management of users:

- under the responsibility of the service provider (its employees and, where applicable, third-parties involved in the delivery of the service);
- under the responsibility of the commissioning entity, but for whom the provider implements access control mechanisms (notably by providing the commissioning entity with an interface for managing accounts and access rights).

Users for whom the client implements access control and identity management mechanisms are outside the scope of this baseline.

9.1. Access control policy

- a) The service provider must document and implement an access control policy based on the results of its risk assessment, and responsibility sharing.
- b) The service provider must review the access control policy annually and whenever any major change occurs that may impact the service.

9.2. User registration and de-registration

- a) The service provider must document and implement a user registration and de-registration procedure based on an interface for managing accounts and access rights. This procedure must specify which data must be deleted when a user leaves.
- b) The service provider must assign nominative accounts when registering users under its responsibility.
- c) The service provider must implement measures ensuring that the de-registration of a user results in the removal of all their access to the service information system resources, as well as the deletion of their data in accordance with the registration and de-registration procedure (see requirement [9.2 a\)](#)).

9.3. Access rights management

- a) The service provider must document and implement a procedure ensuring the assignment, modification, and removal of access rights to the service information system resources.
- b) The service provider must make available to its commissioning entities the tools and mechanisms that allow for the differentiation of user roles within the service, for example according to their functional role.
- c) The service provider must maintain an up-to-date inventory of users under its responsibility who have administration rights over the service information system resources.
- d) The service provider must be able to provide, for any given resource involved in delivering the service, the list of all users who have access to it—whether they are under the responsibility of the service provider or the client with the access rights assigned to them.
- e) The service provider must be able to provide, for any given user, whether under responsibility of the service provider or the client, the list of all their access rights to the various components of the service information system.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	22/55

- f) The service provider must define a list of mutually incompatible access rights. When granting access rights to a user, the provider must ensure that the user is not assigned any rights that are incompatible according to this predefined list.
- g) The service provider must include within the access rights management procedure the actions required to revoke or suspend any user's rights.

9.4. User access rights review

- a) The service provider must make available to the commissioning entity a tool facilitating the review of access rights for users under the commissioning entity's responsibility.
- b) The service provider must make available to the commissioning entity a tool facilitating the review of access rights for users under the commissioning entity's responsibility.
- c) The service provider must quarterly review the list of users within its scope of responsibility who are authorised to use the technical accounts mentioned in requirement 9.2 b).

9.5. User authentication management

- a) The service provider must formalise and implement procedures for managing user authentication. In accordance with the requirements of Chapter 10, these procedures must in particular cover:
 - the management of authentication means (password issuance and reset, updating CRLs and importing root certificates when certificates are used, etc.);
 - the implementation of mechanisms enabling multi-factor authentication to address the different use cases covered by the baseline;
 - systems that generate passwords or verify their strength when password-based authentication is used. Such systems must follow the recommendations of [\[G AUTH\]](#).
- b) Any authentication mechanism must provide for blocking an account after a limited number of unsuccessful attempts.
- c) In the context of a SaaS service, the service provider must offer its commissioning entities multi-factor authentication mechanisms for end-user access.
- d) When non-nominal technical accounts are required, the service provider must implement measures requiring users to authenticate using their nominative accounts before being allowed to access these technical accounts.

9.6. Access to administration interfaces

- a) Administration accounts under the responsibility of the service provider must be managed using tools and directories separate from those used to manage user accounts under the responsibility of the commissioning entity.
- b) Administration interfaces made available to commissioning entities must be separate from the administration interfaces used by the service provider.
- c) Administration interfaces made available to commissioning entities must not allow any connection with administrator accounts under the responsibility of the service provider.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	23/55

- d) Administration interfaces used by the service provider must not be accessible from a public network and must therefore not allow any connection from users under the responsibility of the commissioning entity.
- e) If administration interfaces are made available to commissioning entities with access via a public network, administration traffic must be authenticated and encrypted using means in accordance with the requirements of Chapter 10.2.
- f) The service provider must implement a strong multi-factor authentication system for access to:
 - administration interfaces used by the service provider;
 - administration interfaces dedicated to commissioning entities.
- g) For a SaaS service, administration interfaces made available to commissioning entities must be separate from interfaces used for end-user access.
- h) Whenever an administration interface is accessible from a public network, the authentication process must take place before any interaction between the user and the interface.
- i) When the service provider uses an IaaS service as the foundation for another type of service (CaaS, PaaS, or SaaS), the resources allocated for the service provider's use must under no circumstances be accessible via the public interface provided to other commissioning entities of the IaaS service.
- j) When the service provider uses a CaaS service as the foundation for another type of service (PaaS or SaaS), the resources allocated for the service provider's use must under no circumstances be accessible via the public interface provided to other commissioning entities of the CaaS service.
- k) When the service provider uses a PaaS service as the foundation for another type of service (typically SaaS), the resources allocated for the service provider's use must under no circumstances be accessible via the public interface provided to other commissioning entities of the PaaS service.

9.7. Restriction of access to information

- a) The service provider must implement appropriate segregation measures between its customers.
- b) The service provider must implement appropriate segregation measures between the service information system and its other information systems (office IT, management IT, building management systems, physical access control, etc.).
- c) The service provider must design, develop, configure, and deploy the service information system ensuring at least a segregation between, on the one hand, the technical infrastructure and, on the other hand, the equipment necessary for the administration of the services and the resources it hosts.
- d) In the context of technical support, if the actions required to diagnose and resolve an issue encountered by a customer require access to the customer's data, the service provider must:
 - only authorise access to customer's data after obtaining the customer's explicit consent;
 - verify that the person to whom access is to be granted has satisfied the checks specified in requirement [7.1.b](#) ;
 - in the case of a remote intervention by a person located outside the European Union, implement a secure gateway (jump host) through which the person must connect, allowing

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	24/55

real-time supervision (authorisation or denial of actions, requests for explanations, etc.) by a person who has themselves satisfied the checks specified in requirement 7.1(b). The secure gateway must meet the security objectives² specified in [\[G_EXT\]](#), adapted to the context of technical support actions;

- consider the actions performed, once access has been granted, as administration actions and log them accordingly;
- delete the authorisation to access the commissioning entity's data at the end of these actions.

² Security goals of the secure gateway [\[G_EXT\]](#):

- Authenticate the remote machine and the person responsible for support;
- Prevent the exploitation of vulnerabilities or backdoors on the remote maintenance device;
- Ensure the confidentiality and integrity of data within the information system;
- Maintain a trusted audit trail of actions performed by the support centre technician;
- Ensure the safety of the remote maintenance function with respect to the system being remotely diagnosed as well as connected systems;
- Ensure that no information leaks externally.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	25/55

10. Cryptology

10.1. Encryption of stored data

- a) The service provider must define and implement an encryption mechanism preventing recovery of the commissioning entity's data in the event of resource reallocation or physical media retrieval.
 - In the case of an IaaS or CaaS service, this objective may, for example, be achieved by:
 - disk or file system encryption, where the file-mode access protocol ensures that only empty blocks can be allocated (e.g., NAS storage in which a physical block is actually assigned only at the time of writing);
 - volume-level encryption in the case of block-mode access (e.g., SAN storage or local storage), with at least one key per commissioning entity.
 - in the case of a PaaS or SaaS service, this objective may be achieved by using application-level encryption within the service provider's scope, with at least one key per commissioning entity.
- b) The service provider must use a data encryption method that complies with the rules defined in [\[CRYPTO B1\]](#).
- c) The service provider should use data encryption method that follows the recommendations of [\[CRYPTO B1\]](#).
- d) The service provider must implement encryption of data on removable media and backup media leaving the physical security perimeter of the service information system (as defined in Chapter 10), according to the required data security level (see Chapter 8.3).

10.2. Encryption of network traffic

- a) When the service provider implements a network traffic encryption mechanism, it must comply with the rules defined in [\[CRYPTO B1\]](#).
- b) When the service provider implements a network traffic encryption mechanism, the recommendations [\[CRYPTO B1\]](#) should be followed.
- 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) The service provider must generate password hashes using a hashing function combined with a cryptographic salt that complies with the rules defined in [\[NT_SSH\]](#).

10.3. Password hashing

- a) The service provider must only store the hash of user and technical account passwords.
- b) The service provider must implement a hashing function that complies with the rules defined in [\[CRYPTO B1\]](#).
- c) The service provider should implement a hashing function that follows the recommendations of [\[CRYPTO B1\]](#).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	26/55

- d) The service provider must generate password hashes using a hashing function combined with a cryptographic salt that complies with the rules defined in [\[CRYPTO B1\]](#).

10.4. Non-repudiation

- a) When the service provider implements an electronic signature mechanism, it must comply with the rules defined in [\[CRYPTO B1\]](#).
- b) When the service provider implements an electronic signature mechanism, the service provider should follow the recommendations of [\[CRYPTO B1\]](#).

10.5. Secret management

- a) The service provider must implement cryptographic keys that comply with the rules defined in [\[CRYPTO B2\]](#).
- b) The service provider should implement cryptographic keys that follow the recommendations of [\[CRYPTO B2\]](#)
- c) The service provider must protect access to cryptographic keys and other secrets used for data encryption by an appropriate means: security container (software or hardware) or isolated medium.
- d) The service provider must protect access to cryptographic keys and other secrets used for administration tasks with an appropriate security container, software or hardware.

10.6. Roots of trust

- a) On the technical infrastructure, the service provider must only use public key certificates issued by a certification authority of a European Union member state (the master key generation ceremonies must take place in an EU member state and in the presence of the service provider).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	27/55

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 access restriction and control.
- b) The service provider must distinguish public areas, private areas, and sensitive areas.

11.1.1. Public zones

- a) Public zones are accessible to all within the boundaries of the service provider's property. The service provider must not host any resources dedicated to the service or that provide access to its components within public zones

11.1.2. Private zones

- a) Private zones can host:
 - platforms and means for service development;
 - administration, operations, and supervision workstations;
 - premises from which the service provider operates.

11.1.3. Sensitive zones

- a) Sensitive zones are reserved for hosting the production information system of the service, excluding administration, operation and supervision workstations.

11.2. Physical access control

11.2.1. Private zones

- a) The service provider must protect private zones from unauthorised access. To do so, they must implement a physical access control mechanism based on at least one personal factor: knowledge of a secret, possession of an object, or biometrics.
- b) The service provider should respect the guidelines of [\[G CVAP\]](#) for implementing physical access control.
- c) The service provider must define and document physical access measures for emergency situations.
- d) The service provider must display a warning at the entrance to private zones regarding the access limits and conditions for these zones.
- e) The service provider must define and document the time slots and access conditions to private zones based on the profiles of the involved personnel.
- f) The service provider must document and implement measures to ensure that visitors are always accompanied by the service provider when accessing and staying in private zones. The service provider must keep a record of visitors identities in accordance with applicable laws and regulations
- g) In case of intervention (diagnostic, maintenance, or administration actions) in a private zone by a third-party visitor, the service provider must have their actions supervised (monitored, authorised, denied, questioned) by personnel who have met the requirements outlined in [7.1.b](#).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	28/55

- h) The service provider must document and implement mechanisms for monitoring and detecting unauthorised access to private zones.

11.2.2. Sensitive zones

- a) The service provider must protect sensitive zones from unauthorised access. To do so, they must implement a physical access control mechanism based on at least two personal factors: knowledge of a secret, possession of an object, or biometrics.
- b) The service provider should respect the guidelines of [\[G_CVAP\]](#) for the implementation of physical access control.
- c) The service provider must define and document physical access measures for emergency situations.
- d) The service provider must display a warning at the entrance to sensitive zones regarding the access limits and conditions for these zones.
- e) The service provider must define and document the time slots and access conditions to sensitive zones based on the profiles of the involved personnel.
- f) The service provider must document and implement measures to ensure that visitors are always accompanied by the service provider when accessing and staying in sensitive zones. The service provider must keep a record of visitors identities in accordance with applicable laws and regulations.
- g) In case of intervention (diagnostic, maintenance, or administration actions) in a sensitive zone by a third-party visitor, the service provider must have their actions supervised (monitored, authorised, denied, questioned) by personnel who have met the requirements outlined in requirement [7.1.b](#).
- h) The service provider must document and implement mechanisms for monitoring and detecting unauthorised access to sensitive zones.
- i) The service provider must implement a logging mechanism for physical access to sensitive zones. These logs must be reviewed at least monthly.
- j) The service provider must implement measures to ensure that no direct access exists between a public zone and a sensitive zone.

11.3. Protection against external and environmental threats

- a) The service provider must document and implement measures to minimise the risks inherent to physical disasters (fire, water damage, etc.) and natural hazards (climatic risks, floods, earthquakes, etc.).
- b) The service provider must document and implement measures to limit the risks of fire initiation and spread, as well as the risks of water damage.
- c) The service provider must document and implement measures to prevent and mitigate the consequences of a power outage and ensure service recovery in accordance with the service availability requirements defined in the service agreement.
- d) The service provider must document and implement measures to maintain temperature and humidity conditions suitable for the equipment. Additionally, they must implement measures to prevent cooling system failures and limit their consequences.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	29/55

- e) The service provider must document and implement regular checks and testing of physical detection and protection equipment.

11.4. Work in private and sensitive zones

- a) The service provider must integrate physical security elements into the security policy and risk assessment, in accordance with the required security level for the category of the zone.
- b) The service provider must document and implement procedures for work in private and sensitive zones. These procedures must be communicated to the relevant personnel.

11.5. Delivery and loading zones

- a) Delivery and loading zones, as well as other points through which unauthorised persons could enter the premises without being accompanied, are considered public zones.
- b) The service provider must isolate access points from these zones to private and sensitive zones, in order to prevent unauthorised access. If this is not feasible, compensatory measures must be implemented to ensure the same level of security.

11.6. Cable security

- a) The service provider must document and implement measures to protect electrical and telecommunications cabling from physical damage and the potential for interception.
- b) The service provider must establish and maintain an up-to-date cabling plan.
- c) The service provider should implement measures to identify cables (such as colour coding, labelling, etc.) in order to facilitate operation and minimise handling errors.

11.7. Equipment maintenance

- a) The service provider must document and implement measures to ensure that the installation, maintenance, and servicing conditions of the information system equipment hosted in private and sensitive zones are compatible with the confidentiality and availability requirements of the service defined in the service agreement.
- b) The service provider must subscribe to maintenance contracts to ensure the availability of security updates for the software installed on the information system equipment of the service.
- c) The service provider must ensure that media can only be returned to a third-party if the commissioning entity's data stored on them is encrypted in accordance with section 10.1, or if it has been previously destroyed using a secure erasure mechanism through random pattern overwriting.
- d) The service provider must document and implement measures to ensure that the installation, maintenance, and servicing conditions of ancillary technical equipment (such as power supply, air conditioning, fire prevention, etc.) are compatible with the service availability requirements defined in the service agreement.

11.8. Asset decommissioning

- a) The service provider must document and implement a procedure for the off-site transfer of commissioning entity data, equipment, and software. This procedure must require written authorisation from the service provider's management. In all cases, the service provider must implement measures to ensure that the level of protection in terms of confidentiality and integrity of assets during transport is equivalent to the protection on-site.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	30/55

11.9. Safe recycle of equipment

- a) The service provider must document and implement measures to securely erase any data media provided to a commissioning entity by overwriting with random patterns. If the storage space is encrypted under the requirements of section 10.1.a), erasure may be performed by securely erasing the encryption key.

11.10. Equipment awaiting use

- a) The service provider must document and implement a procedure to protect equipment awaiting use.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	31/55

12. Operational security

12.1. Documented operating process

- a) The service provider must document operating procedures, keep them up to date, and make them accessible to the relevant personnel.

12.2. Change management

- a) The service provider must document and implement a change management procedure for changes made to information processing systems and means.
- b) The service provider must document and implement a procedure to ensure that, in the case of operations carried out by the service provider that may impact the security or availability of the service, the following information is communicated to all commissioning entities as soon as possible:
 - scheduled start and end date and time of the operations;
 - nature of the operations;
 - impacts on service security or availability;
 - contact person within the service provider's organisation.
- c) In the case of a PaaS service, the service provider must inform the commissioning entity as soon as possible of any upcoming changes to software elements under its responsibility when complete compatibility cannot be ensured.
- d) The service provider must inform the commissioning entity as soon as possible of any upcoming changes to service elements if such changes are likely to cause a loss of functionality for the commissioning entity.

12.3. Separation of development, testing and production environments

- a) The service provider must document and implement measures to physically separate environments related to service production from other environments, including development environments.

12.4. Measures against malicious code

- a) The service provider must document and implement measures for detection, prevention, and recovery to protect against malicious code. The scope of this requirement for the service information system must include user workstations under the responsibility of the service provider and incoming data traffic to this information system.
- b) The service provider must document and implement an awareness programme for its employees regarding the risks associated with malicious code and best practices for reducing the impact of an infection.

12.5. Data backup

- a) The service provider must document and implement a data backup and restoration policy for data under its responsibility within the scope of the service. This policy must ensure daily backups of all data (information, software, configurations, etc.) under the service provider's responsibility within the service.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	32/55

- b) The service provider must document and implement measures to protect backups in accordance with the access control policy (see Chapter 9). This policy must include a monthly review of access logs to the backups.
- c) The service provider must document and implement a procedure to regularly test the restoration of backups.
- d) The service provider must locate backups at sufficient distance from main equipment, in line with the results of the risk assessment, and in a way that allows for recovery from major disasters. Backups are subject to the same localisation requirements as operational data. The backup site(s) must meet the same security requirements as the main site, particularly those listed in Chapters **Erreur ! Source du renvoi introuvable.** et **Erreur ! Source du renvoi introuvable.**. Communications between the main site and backup site must be protected by encryption, in accordance with the requirements of Chapter 10.

12.6. Event logging

- a) The service provider must document and implement a logging policy that includes at least the following elements:
 - list of collection sources;
 - list of events to be logged by source;
 - purpose of logging for each event;
 - collection frequency and time base used;
 - local and centralised retention duration;
 - log protection measures (including encryption and duplication);
 - log location.
- b) The service provider must generate and collect the following events:
 - user activities related to information security;
 - modification of access rights within the scope of responsibility;
 - events from malware protection mechanisms (see section 12.4);
 - exceptions;
 - failures;
 - any other event related to information security.
- c) The service provider must retain events generated by logging for a minimum period of six months, subject to compliance with legal and regulatory requirements.
- d) The service provider must provide, upon request from a commissioning entity, all events concerning it.
- e) The logging system implemented by the service provider should respect the recommendations of [\[NT LOG\]](#).

12.7. Protection of logged information

- a) The service provider must protect logging equipment and logged events from threats to their availability, integrity, or confidentiality, in accordance with section 3.2 of [\[NT LOG\]](#).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	33/55

- b) The service provider must manage the storage capacity for all equipment hosting one or more collection sources to allow for the local retention of logged events as outlined in the event logging policy. This sizing management must consider the evolution of the information system.
- c) The service provider must transfer logged events while ensuring their confidentiality and integrity protection, to one or more dedicated central servers, and must store them on a physical machine separate from the machine that generated them.
- d) The service provider must implement a backup of collected events following an appropriate policy.
- e) The service provider must execute logging and event collection processes using accounts with the necessary and sufficient privileges and must restrict access to logged events in accordance with the access control policy (see Chapter **Erreur ! Source du renvoi introuvable.**).

12.8. Clock synchronisation

- a) The service provider must document and implement a clock synchronisation process for all equipment, using one or more consistent internal time sources. These sources may themselves be synchronised to multiple reliable external sources, except for isolated networks.
- b) The service provider must implement timestamping for each logged event.

12.9. Event analysis and correlation

- a) The service provider must document and implement an infrastructure to analyse and correlate events recorded by the logging system in order to detect events that may impact the security of the service information system, either in real-time or retrospectively for events up to six months old.
- b) The baseline of requirements for cyber security incident detection service provider [\[PDIS\]](#) should be relied for setting up and operating the event analysis and correlation infrastructure.
- c) The service provider must acknowledge alarms notified by the event analysis and correlation infrastructure at least on a daily basis.

12.10. Installation of software on operational systems

- a) The service provider must document and implement a procedure to control the installation of software on the service information system equipment.
- b) The service provider must document and implement a configuration management procedure for software environments provided to the commissioning entity, including ensuring their security maintenance.

The service provider must provide the ability to inspect and, if necessary, remove inputs³ (such as verifying the authenticity and safety of updates, checking the safety of provided tools, etc.) related to the scope of the technical infrastructure:

³ Those inputs are set up with necessary and specific elements for the considered software installation: software components to be installed, provided installation tools, etc.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	34/55

- this inspection and removal capability must generate activity logs and must be subject to code audits.
- the inputs must be handled on dedicated devices operated and maintained by the service provider, hosted in a segregated area from the rest of the infrastructure (such as a demilitarised zone as defined in [\[G_INT\]](#)).

12.11. Management of technical vulnerabilities

- The service provider must document and implement a monitoring process to manage technical vulnerabilities of software and systems used in the service information system.
- The service provider must assess its exposure to these vulnerabilities by including them in the risk assessment and apply appropriate risk treatment measures.

12.12. Administration

- The service provider must document and implement a procedure requiring administrators under its responsibility to use dedicated terminals solely for administration tasks, in accordance with Chapter 4.1 titled "Managing the administration station" of [\[NT_ADMIN\]](#). These terminals must be controlled and kept up to date.
- The service provider must implement hardening measures for the configuration of the terminals used for administration tasks, particularly those outlined in Chapter 4.2 titled "Architecture of the administration station" of [\[NT_ADMIN\]](#).
- When the service provider permits mobility for administrators under its responsibility, it must be governed by a documented policy. The solution implemented must ensure that the security level of the mobility situation is at least equivalent to the security level when not in a mobility situation (see Chapters **Erreur ! Source du renvoi introuvable.** and **Erreur ! Source du renvoi introuvable.**). This solution must specifically include:
 - the use of a non-bypassable, non-disconnectable encrypted tunnel for all traffic (see **Erreur ! Source du renvoi introuvable.**);
 - full disk encryption (see Chapter **Erreur ! Source du renvoi introuvable.**).

12.13. Remote diagnosis and maintenance of infrastructure components

- In the context of remote diagnosis or maintenance of infrastructure components, considering risks to the confidentiality of the commissioning entities' data, the service provider must:
 - verify that the person to whom access is to be granted has satisfied the checks of requirement [7.1.b](#) ;
 - in the case of an intervention performed by a person who has not satisfied the checks of requirement [7.1.b](#), implement a secure gateway (jump host) through which the person must connect, enabling real-time supervision of actions (authorisation or prohibition of actions,

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	35/55

request for explanations, etc.) by a person who has themselves satisfied the checks of requirement 7.1.b. The secure gateway must meet the security goals⁴ specified in [\[G_EXT\]](#);

- consider the actions taken once access is granted as administration actions and log them as such;
- remove access authorisation at the end of the intervention.

12.14. Monitoring of outbound traffic from the infrastructure

a) The service provider must provide the capability to inspect and remove outbound traffic from the technical infrastructure related to the service scope (billing information, any logs required for incident handling, etc.):

- outbound traffic must be purged of data that could compromise the confidentiality of the commissioning entities' data;
- this inspection and removal capability must generate activity logs and should be subject to code audits;
- outbound traffic is handled on dedicated devices operated and maintained by the service provider, hosted in a segregated area of the infrastructure (such as a demilitarised zone as defined in [\[G_INT\]](#)).

⁴ Security goals of the secure gateway [\[G_EXT\]](#) :

- Authenticate the remote machine and the support person in charge;
- Prevent the exploitation of vulnerabilities or backdoors on the remote maintenance device;
- Guarantee the confidentiality and integrity of data within the information system;
- Ensure trusted traceability of actions performed by the support centre technician;
- Guarantee the safety of the remote maintenance function with respect to the system being diagnosed, as well as related systems;
- Guarantee the absence of data leakage to the outside.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	36/55

13. Communication security

13.1. Information system mapping

- a) The service provider must establish and maintain an up-to-date mapping of the service information system, linked to the asset inventory (see Chapter 8.1), which must include at least the following elements:
- a list of physical or virtualised resources;
 - names and functions of the applications supporting the service;
 - network architecture diagram at Layer 3 of the OSI model, identifying key points:
 - interconnection points, especially with third-party and public networks;
 - networks, subnets, including administration networks;
 - devices providing security functions (filtering, authentication, encryption, etc.);
 - servers hosting data or performing sensitive functions;
 - matrix of authorised network traffic, specifying:
 - their technical description (services, protocols, and ports);
 - the business or technical infrastructure justification;
 - where appropriate, if services, protocols, or ports deemed insecure are used, the compensatory measures put in place, in line with a defence-in-depth strategy.
- b) the service provider must review the mapping at least annually.

13.2. Network segmentation

- a) The service provider must document and implement, for the service information system, segmentation measures (logical, physical, or via encryption) to separate network traffic based on:
- sensitivity of transmitted information;
 - nature of traffic (production, administration, supervision, etc.);
 - domain ownership of the traffic (from commissioning entities — with distinction by commissioning entity or group of commissioning entities, from the service provider, from third-parties, etc.);
 - technical domain (processing, storage, etc.).
- b) The service provider must segregate, physically or via encryption, all internal data traffic within the service information system from any other information system. When this segregation is implemented through encryption, it must comply with the requirements of Chapter 10.2.
- c) If the administration network of the technical infrastructure is not physically segregated, administration traffic must pass through an encrypted tunnel, in compliance with the requirements of Chapter 10.2.
- d) The service provider must implement and configure an application firewall to protect the administration interfaces exposed to commissioning entities on a public network.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	37/55

- e) The service provider must implement a filtering mechanism on all administration and monitoring interfaces of the service technical infrastructure, allowing only legitimate connections identified in the authorised flow matrix.

13.3. Network monitoring

- a) The service provider must have one or more security incident detection probes on the service information system. These probes must specifically enable the monitoring of each interconnection between the service information system and third-party information systems and public networks. These probes must serve as data sources for the event analysis and correlation infrastructure (see Chapter 12.9).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	38/55

14. Acquisition, development and maintenance of information systems

14.1. Secure development policy

- a) The service provider must document and implement secure software and system development rules, and apply them to internal developments.
- b) The service provider must document and implement tailored secure development training for relevant employees.

14.2. System control change procedures

- a) The service provider must document and implement a procedure for controlling changes to the service information system.
- b) The service provider must document and implement a procedure for validating changes made to the service information system in a pre-production environment before they are released to production.
- c) The service provider must maintain a history of software and system versions (both internal and external developments, commercial products) deployed, to allow for the recreation of a complete environment as it was implemented at a given date, if necessary, in a testing environment. The retention period for this history must align with that of the backups (see Chapters 12.5).

14.3. Technical review of application after changes made to operational platform

- a) The service provider must document and implement a procedure to test all applications before they are released to production, in order to verify the absence of any adverse effects on the service's operation or security.

14.4. Secure development environment

- a) The service provider must implement a secure development environment that allows management of the entire development lifecycle of the service information system.
- b) The service provider must consider development environments in the risk assessment and ensure their protection in accordance with the present baseline.

14.5. Outsourced development

- a) The service provider must document and implement a procedure to supervise and control outsourced software and system development activities. This procedure must ensure that outsourced development activities comply with the service provider's secure development policy and achieve a level of security in the external development equivalent to that of an internal development (see requirement [14.1 a](#)).

14.6. Security and compliance testing of the system

- a) The service provider must subject new or updated information systems to security compliance and functionality tests during development. The service provider must document and implement a testing procedure that identifies:
 - tasks to be performed;

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	39/55

- input data;
- expected output results.

14.7. Protection of testing data

- a) The service provider must document and implement a procedure to ensure the integrity of test data used in pre-production.
- b) If the service provider wishes to use the commissioning entity’s production data for testing purposes, the service provider must obtain prior approval from the commissioning entity and anonymise the data. The service provider must ensure the confidentiality of the data during anonymisation.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	40/55

15. Relations with third-parties

15.1. Identification of third-parties

- a) The service provider must maintain an up-to-date comprehensive list of third-parties involved in the implementation of the service (hosting provider, developer, integrator, archiver, subcontractor operating on-site or remotely, cooling system suppliers, etc.). This list must specify the third-party's contribution to the service and the processing of personal data. It must also take into account cases of multi-level subcontracting scenarios.
- b) The service provider must make available to the commissioning entity the list of all third-parties who may access the data and inform them of any changes to subcontractors as per Article 28 of the [\[GDPR\]](#), so that the commissioning entity can raise any objections.

15.2. Security in agreements concluded with third-parties

- a) The service provider must require that third-parties involved in the implementation of the service provide a level of security at least equivalent to the security level the service provider commits to maintaining in its own security policy. They must do this through requirements tailored to each third-party and their contribution to the service, included in the service specifications or security clauses of partnership agreements. The service provider must include these requirements in contracts concluded with third-parties.
- b) The service provider must contractually include audit clauses with each third-party involved in the implementation of the service, allowing a qualification body to verify that these third-parties comply with the requirements of this baseline.
- c) The service provider must define and assign roles and responsibilities relating to the modification or termination of the contract with any third-party involved 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 to regularly monitor the measures put in place by third-parties involved in the implementation of the service to ensure they comply with the requirements of this baseline, in accordance with Chapter 18.3.

15.4. Management of changes made to third-party services

- a) The service provider must document and implement a procedure to track changes made by third-parties involved in the implementation of the service that may affect the security level of the service information system.
- b) If a change in a third-party involved in the implementation of the service affects the service's security level, the service provider must inform all commissioning entities without delay, in accordance with Chapter 12.2, and implement measures to restore the previous security level.

15.5. Confidentiality commitments

- a) The service provider must document and implement a procedure to review at least annually the confidentiality or non-disclosure agreement requirements for third-parties involved in the implementation of the service.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	41/55

16. Management of incidents to information security

16.1. Responsibilities and procedures

- a) The service provider must document and implement a procedure to ensure prompt and effective responses to security incidents. These procedures must define the means and timeframes for communicating security incidents to all concerned commissioning entities, as well as the level of confidentiality required for such communication.
- b) The service provider must inform its employees and all third-parties involved in the implementation of the service about this procedure.
- c) The service provider must document any personal data breach and inform its commissioning entity. The breach must be notified to the relevant French data protection authority (CNIL⁵) if it presents a risk to the rights and freedoms of affected individuals. The individuals concerned must be informed when the risk to their privacy is high.

16.2. Reports related to security of information security

- a) The service provider must document and implement a procedure requiring its employees and third-parties involved in the implementation of the service to report any actual or suspected security incident or security vulnerability.
- b) The service provider must document and implement a procedure allowing all commissioning entities to report any actual or suspected security incidents or vulnerabilities.
- c) The service provider must promptly communicate security incidents to the commissioning entities, along with recommendations to mitigate the impact. It must allow the commissioning entity to choose the severity levels of incidents for which it wishes to be informed.
- d) The service provider must communicate security incidents to the relevant authorities in accordance with applicable legal and regulatory requirements.

16.3. Assessment of information security events and making of decision

- a) The service provider must assess information security events and decide whether they must be classified as security incidents. For this assessment, the service provider must rely on one or more scales (such as estimation, evaluation, etc.) shared with the commissioning entity.

Note: Security incidents include personal data breaches.

- b) The service provider must use a classification system that clearly identifies security incidents affecting the commissioning entities' data, in accordance with the results of the risk assessment. This classification must include personal data breaches.

16.4. Response to information security incidents

- a) The service provider must manage security incidents until they are resolved and must inform commissioning entities in accordance with procedures.

5 Online notification: <https://notifications.cnil.fr/notifications/index>

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	42/55

- b) The service provider must archive documents detailing security incidents.
- c) The service provider should engage a qualified Security Incident Response Service [\[PRIS\]](#) provider to handle security incidents requiring additional expertise.

16.5. Learning from information security incidents

- a) The service provider must document and implement a continuous improvement process aimed at reducing the occurrence and impact of types of security incidents that have already been handled.

16.6. Evidence collection

- a) The service provider must document and implement a procedure to record information related to security incidents that may serve as evidence.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	43/55

17. Business continuity

17.1. Organisation of business continuity

- a) The service provider must document and implement a business continuity plan that includes information security.
- b) The service provider must review the service's business continuity plan annually and after any major changes that may impact the service.

17.2. Implementation of business continuity

- a) The service provider must document and implement procedures to maintain or restore service operation and ensure information availability at the levels and within the timeframes the service provider has committed to in the service agreement with the commissioning entity.

17.3. Verifying, reviewing and evaluating the business continuity

- a) The service provider must document and implement a procedure to test the business continuity plan to ensure that it is relevant and effective in a crisis situation.

17.4. Availability of information processing means

- a) The service provider must document and implement measures to meet the availability requirements of the service as defined in the service agreement (see Chapter 19.1).

17.5. Backup of technical infrastructure configuration

- a) The service provider must document and implement an offline backup procedure for the technical infrastructure configuration.

17.6. Provision of a backup service for the commissioning entity's data

- a) The service provider must document and provide the commissioning entity with a data backup service for its data.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	44/55

18. Compliance

18.1. Identification of applicable legislation and contractual requirements

- a) The service provider must identify the applicable legal, regulatory, and contractual requirements in force for the service. In France, the service provider must at least consider the following texts:
- personal data [\[LOI IL\]](#), [\[GDPR\]](#);
 - professional secrecy [\[CP ART 226 13\]](#), where applicable, without prejudice to the application of Article 40, paragraph 2 of the Code of Criminal Procedure concerning reporting to a judicial authority;
 - breach of the trust [\[CP ART 314-1\]](#);
 - privacy of the correspondence [\[CP ART 226-15\]](#);
 - breach of privacy [\[CP ART 226-1\]](#);
 - fraudulent access or maintenance of an information system [\[CP ART 323-1\]](#).
- b) Depending on its role in the processing of personal data (data controller, data processor, or joint controller), the service provider must justify and document the choices of technical and organisational measures implemented to meet the personal data protection requirements of this baseline (see section 19.5).
- c) The service provider must document and implement procedures to comply with applicable legal, regulatory, and contractual requirements for the service, as well as specific security needs (see Chapter 8.3 **Erreur ! Source du renvoi introuvable.**
- d) Upon request from a commissioning entity, the service provider must make all of these procedures accessible to them.
- e) The service provider must document and implement an active monitoring process for the legal, regulatory, and contractual requirements in force applicable to the service.

18.2. Independent review of information security

18.2.1. Continuous review

- a) The service provider must document and implement a three-year audit programme defining the scope and frequency of audits in line with change management, policies, and risk assessment results.

The audit programme must include one qualified audit per year conducted by a qualified cyber security audit service provider [\[PASSI\]](#) provider. The entire audit programme must notably cover:

- audit of the technical infrastructure configuration of the service. This audit is conducted by sampling and must include all types of equipment and servers present in the service information system;
- penetration testing of administration interfaces exposed on a public network;
- penetration testing of the user interface for SaaS services;
- if the service includes internal developments, source code auditing of the implemented security features (a continuous approach is recommended).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	45/55

- b) The service provider should implement automated configuration audit mechanisms suitable for the service’s technical infrastructure.

18.2.2. Initial review

- a) Prior to the service qualification assessment, the service provider must have an initial independent review of information security conducted by a qualified cyber security audit service provider [\[PASSI\]](#). This initial review must notably cover⁶:
 - for services other than IaaS (CaaS, PaaS, SaaS, etc.), an audit of the configuration of virtual or physical resources, operating systems, and core software (OS, middleware, databases, etc.) within the service scope;
 - a penetration test of the service’s administration interfaces made available to the commissioning entities;
 - for a SaaS service, a penetration test of the interface provided to end users, as well as a source code audit of the implemented security features (authentication, session management, isolation management in multi-tenant mode). If the SaaS provides an information security service, a dedicated product certification⁷ is required.

18.2.3. Review of major changes

- a) In the event of a major change that may affect the service, the service provider must have an independent change review carried out by a qualified cyber security audit service provider [\[PASSI\]](#). This independent change review must in particular cover the following audit activities:
 - architecture audit;
 - organisational and physical audit;
 - audit of the configuration of the service’s technical infrastructure;
 - a penetration test of the service’s administration interfaces made available to the commissioning entities;
 - for a SaaS service, a penetration test of the interface made available to end users as part of the service catalogue, as well as a source code audit of the implemented security features (authentication, session management, isolation management in multi-tenant mode). If the SaaS provides an information security service, a dedicated product certification is required.

18.3. Compliance with security policies and standards

- a) The service provider, through the information security manager, must regularly ensure the proper execution of all security procedures under their responsibility in order to guarantee compliance with security policies and standards.

⁶ The architecture audit, physical security audit, and information security organisational audit are not necessary as part of the initial review, as they are addressed elsewhere in the baseline

⁷ The issuance of the certificate is contingent upon the correction of any critical vulnerabilities identified during the initial review.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	46/55

18.4. Technical compliance review

- a) The service provider must document and implement a policy to verify the technical compliance of the service with the requirements of this baseline. This policy must define the objectives, methods, frequencies, expected results, and corrective measures.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	47/55

19. Additional requirements

19.1. Service agreement

- a) The service provider must establish a service agreement with each of the commissioning entities of the service. Any modification of the service agreement must be submitted to the commissioning entity for approval
- b) The service provider must identify on the service agreement:
 - obligations, rights, and responsibilities of each party: service provider, third-parties involved in the service delivery, commissioning entities, etc.;
 - elements explicitly excluded from the responsibilities of the service provider within the limits set by applicable legal and regulatory requirements, particularly Article 28 of the [\[GDPR\]](#);
 - service location. Support location must be specified if it is provided from a non-EU country, as allowed by requirement [19.2.e](#).
- c) The service provider must propose a service agreement applying the law of an EU Member State. The applicable law must be identified in the service agreement.
- d) The service agreement must specify that data collection, handling, storage, and more generally processing carried out during pre-sales, implementation, maintenance, and termination of the service, are done in accordance with the requirements set out by applicable legislation.
- e) The service agreement must specify that the service provider must make available to the commissioning entity, upon request, the elements for assessing the risks related to the submission of the commissioning entity's data to the law of a non-EU country (see 5.3.e).
- f) The service provider must describe in the service agreement technical and organisational measures it implements to ensure respect with applicable law.
- g) The service provider must include in the service agreement a revision clause, which includes, in particular, termination without penalty for the commissioning entity in case of loss of the qualification granted to the service.
- h) The service provider must include in the service agreement a reversibility clause enabling the commissioning entity to recover all of its data (either provided directly by the commissioning entity or produced as part of the service using the commissioning entity's data or actions).
- i) The service provider must ensure reversibility via one of the following technical methods:
 - making available files in one or more documented formats that are usable outside of the service provided by the service provider;
 - implementing technical interfaces letting access to the data in a documented and usable format (such as API or pivot format).The technical methods of reversibility must be specified in the service agreement.
- j) The service provider must specify in the service agreement the service availability level.
- k) The service provider must specify in the service agreement that it cannot dispose of the data transmitted and generated by the commissioning entity, as such data remains the property of the commissioning entity.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	48/55

- l) The service provider must specify in the service agreement that it does not disclose any information related to the service to third-parties, except upon formal written consent of the commissioning entity.
- m) The service provider must specify in the service agreement whether the commissioning entity's data is automatically backed up. If not, the service provider must raise awareness with the commissioning entity about the associated risks and clearly indicate the actions the commissioning entity must take to ensure their data is backed up.
- n) The service provider must specify in the service agreement whether remote access is permitted for administration or support actions on the service information system.
- o) The service provider must specify in the service agreement that:
 - the service is qualified and include the qualification certificate;
 - the commissioning entity can file a complaint regarding the qualified service with ANSSI;
 - the commissioning entity authorises ANSSI and the qualification body to audit the service and its information system to verify that they respect the requirements of this baseline.
- p) The service provider must specify in the service agreement that the commissioning entity authorises, in accordance with this baseline (see Chapter **Erreur ! Source du renvoi introuvable.**), a qualified cyber security audit service provider [\[PASSI\]](#) appointed by the service provider to audit the service and its information system as part of the control plan.
- q) The service provider must specify in the service agreement that it commits to making available all the necessary information for carrying out audits of compliance with the dispositions of Article 28 of the [\[GDPR\]](#), conducted by the commissioning entity or a third-party appointed by them.
- r) The third-party appointed for the audits should be qualified by a cyber security audit service provider [\[PASSI\]](#).

19.2. Data location

- a) The service provider must document and communicate to the commissioning entity the location of storage and processing of its data.
- b) The service provider must store and process the commissioning entity's data within the European Union.
- c) Administration and supervision operations of the service must be carried out from the European Union.
- d) The service provider must store and process technical data (such as the identities of beneficiaries and administrators of the technical infrastructure, data manipulated by the Software Defined Network, infrastructure logs, directory, certificates, access configurations, etc.) within the European Union.
- e) The service provider may perform support operations for commissioning entities from a non-EU country. It must document the list of operations that can be carried out by the support from a non-EU country and the mechanisms that ensure access control and supervision from within the European Union.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	49/55

19.3. Regionalisation

- a) The service provider must ensure that the service interfaces accessible to the commissioning entity are at least available in French.
- b) The service provider must provide first-level support in French.

19.4. End of the contract

- a) At the end of the contract linking the service provider and the commissioning entity, whether the contract has expired or for any other reason, the service provider must ensure secure deletion of all the commissioning entity's data. This deletion must be subject to a formal notice to the commissioning entity from the service provider with a notice period of twenty-one calendar days. The deletion may be carried out using one of the following methods, within a timeframe specified in the service agreement:
 - full overwriting of any storage media that hosted the data;
 - deletion of the keys used to encrypt the commissioning entity's storage spaces, as described in Chapter 10.1;
 - secure recycling, under the conditions outlined in Chapter 11.9.
- b) At the end of the contract, the service provider must delete the technical data related to the commissioning entity (such as directory, certificates, access configuration, etc.).

19.5. Personnel protection

- a) The service provider must justify compliance with data protection principles for personal data processing carried out on its own behalf. At a minimum, it must justify the following points:
 - processing purposes are explicitly and legitimately determined;
 - traceability of processing activities carried out on the behalf of the service provider and the commissioning entity;
 - the lawful basis for processing;
 - the prohibition of purpose misappropriation in processing activities;
 - the data used respects the principle of data minimisation, ensuring it is necessary and sufficient for processing, and is therefore adequate, relevant, and limited;
 - the quality of the data used for processing is maintained, with data being accurate and kept up to date;
 - retention periods are defined and limited.
- b) The service provider must justify, for personal data processing carried out on its own behalf, compliance with the rights of data subjects. At a minimum, it must justify the following points:
 - informing users through fair and transparent processing;
 - obtaining users' consent: explicit, demonstrable, and withdrawable;
 - allowing users to exercise their rights of access, rectification, and erasure;
 - allowing users to exercise their rights to restriction of processing, data portability, and objection.
- c) When acting as a processor within the meaning of Article 28 of the [\[GDPR\]](#), the service provider must provide assistance and advice to the commissioning entity, informing it if any instruction from the commissioning entity constitutes a breach of data protection rules.

19.6. Protection against non-European law

- a) The statutory headquarters, central administration, and main establishment of the service provider must be located within a Member State of the European Union.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	50/55

- 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 held at more than 39%;
- by third-party entities whose statutory headquarters, central administration, or main establishment are located in a non-EU country.

If the capital held by these third-party entities takes the form of shares admitted to trading on a regulated market, the said third-party entities are those declared in accordance with Article L.233-7(I) of the French Commercial Code.

The aforementioned third-party entities must not, either individually or collectively:

- pursuant to a contract or articles of association, hold a veto right;
- pursuant to a contract or statutory provisions, designate the majority of the members of the service provider’s administrative, management, or supervisory bodies.

- c)** Where the service provider, in the context of the services provided to the commissioning entity, uses the services of a third-party company — including a subcontractor — having its statutory headquarters, central administration, or main establishment in a non-EU country, or belonging to or being controlled by a third-party company established outside the European Union, that said third-party company must not have the technical capability to access the data processed through the service.

The data concerned includes data entrusted to the service provider by the commissioning entities, 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.) containing information relating to the commissioning entities.

For the purposes of this article, the notion of control is understood as defined in Article L.233-3(II) of the French Commercial Code.

- d)** Within the scope of requirement 19.6.c, any third-party company used by the service provider to deliver all or part of the service to the commissioning entity must guarantee the service provider continuous operational autonomy in the delivery of the cloud service it operates, or must be SecNumCloud qualified.

For the purposes of this article, operational autonomy is understood as the ability to maintain the delivery of the Cloud service by relying on the service provider’s own capabilities or by using services available from at least two third-party companies.

- e)** The service provided by the service provider must comply with applicable legislation on fundamental rights, and with European Union values relating to respect for human dignity, freedom, equality, democracy, and the rule of law. In assessing the above-mentioned compliance, consideration may be given to whether the service provider maintains links with a foreign government or public body.

- f)** The service provider must formally inform the commissioning entity, within one month, of any legal, organisational, or technical change that may have an impact on the compliance of the service with the requirements of Chapter 19.6.

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	51/55

Appendix 1 Document references

I. Codes, legislative and regulatory texts

Reference to	Document
[LOI_IL]	Law of 6 January 1978 on Data Processing, Files, and Freedoms. Available on http://www.legifrance.gouv.fr (French)
[GDPR]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available on https://eur-lex.europa.eu (French)
[CP_ART_314-1]	Article 334-1 of the penal code on breach of trust. Available on http://www.legifrance.gouv.fr (French)
[CP_ART_226-1]	Article 226-1 of the penal Code on breach of privacy. Available on http://www.legifrance.gouv.fr (French)
[CP_ART_226-13]	Article 226-13 of penal Code pénal on professional secrecy. Available on http://www.legifrance.gouv.fr (French)
[CP_ART_226-15]	Article 226-15 of penal Code on the Secrecy of Correspondence. Available on http://www.legifrance.gouv.fr (French)
[CP_ART_323-1]	Article 323-1 of penal Code relating to fraudulent access or maintenance in an automated data processing system. Available on http://www.legifrance.gouv.fr (French)
[IGI_1300]	Interministerial General Instruction n° 1300/SGDSN/PSE/PSD of 9 August 2021 on the protection of national defence secrecy. Available on http://www.legifrance.gouv.fr (French)
[II_910]	Interministerial Instruction on controlled items of information systems security (<i>Articles Contrôlés de la Sécurité des Systèmes d'Information - ACSSI</i>), n°910/SGDSN/ANSSI, 22 October 2013. Available on https://www.legifrance.gouv.fr/ (French)
[PSSIE]	State information systems security policy (<i>Politique de sécurité des systèmes d'information de l'État - PSSIE</i>), carried out by Prime Minister's circular n°5725/SG of 17 July 2014. Available on https://www.legifrance.gouv.fr/ (French)

II. Technical documents and standards

Reference to	Document
[AUTHENTICATION]	Recommendations on Multi-factor authentication and passwords (<i>Recommandations relatives à l'authentification multifacteur et aux mots de passe</i>), ANSSI guideline n° ANSSI-PG-078 du 08 février 2021, ANSSI. Available on https://cyber.gouv.fr/ (French)
[CRYPTO_B1]	Rules and recommendations on the selection and sizing of cryptographic mechanisms (<i>Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques</i>), ANSSI, current version. Available on https://cyber.gouv.fr/ (French)

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	52/55

Reference to	Document
[CRYPTO_B2]	Rules and Recommendations on the Management of Keys Used in Cryptographic Mechanisms (<i>Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques</i>), ANSSI, current version. Available on https://cyber.gouv.fr/ (French)
[HOMOLOGATION]	Security accreditation in nine simple steps (<i>L'homologation de sécurité en neuf étapes simples</i>), ANSSI, current version. Available on https://cyber.gouv.fr/ (French)
[HEALTHY]	Guideline for a healthy information system in 42 measures, ANSSI, current version. Available on https://cyber.gouv.fr/
[INTERNET]	Recommendations on the interconnection of an information system to the internet (<i>Recommandations relatives à l'interconnexion d'un système d'information à Internet</i>), ANSSI guidelines n° ANSSI-PA-066 of 19 June 2020, ANSSI. Available on https://cyber.gouv.fr/ (French)
[NT_IPSEC]	Recommendations for securing networks with IPsec , technical note n° DAT-NT-003/ANSSI/SDE/NP of 3 August 2015, ANSSI. Available on https://cyber.gouv.fr/
[NT_TLS]	Security recommendations for TLS, technical note n° SDE-NT-35/ANSSI/SDE/NP of 19 August 2016, ANSSI. Available on https://cyber.gouv.fr/
[NT_SSH]	(Open)SSH secure use recommendations, technical note n° DAT-NT-007/ANSSI/SDE/NP of 17 August 2015, ANSSI. Available on https://cyber.gouv.fr/
[NT_LOG]	Security recommendations for the implementation of a logging system (<i>Recommandations de sécurité pour la mise en œuvre d'un système de journalisation</i>), technical note n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013, ANSSI. Available on https://cyber.gouv.fr/
[NT_ADMIN]	Recommendations to secure administration of IT systems, ANSSI guidelines n° ANSSI-PA-022 of 11 may 2021, ANSSI Available on http://www.cyber.gouv.fr
[G_AUTH]	Recommendations on multi-factor authentication and passwords (<i>Recommandations relatives à l'authentification multifacteur et aux mots de passe</i>), ANSSI guidelines n° ANSSI-PG-078 of 8 October 2021, ANSSI Available on https://cyber.gouv.fr/
[G_CVAP]	Recommendations on securing physical access control and video surveillance systems (<i>Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection</i>), ANSSI guidelines n° ANSSI-PA-72 of 04 March 2020, ANSSI Available on https://cyber.gouv.fr/
[G_EXT]	Outsourcing guideline (<i>Guide de l'externalisation</i>), ANSSI guidelines of 03 December 2010, ANSSI Available on https://cyber.gouv.fr/

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	53/55

Reference to	Document
[G_INT]	Recommendations on the interconnection of an information system to the internet (<i>Recommandations relatives à l'interconnexion d'un système d'information à Internet</i>), ANSSI guidelines n°ANSSI-PA-066 of 16 June 2020, ANSSI Available on https://cyber.gouv.fr/
[PASSI]	Cyber security audit service provider, ANSSI, current version Available on https://cyber.gouv.fr/
[PDIS]	Cyber security incident detection service providers, ANSSI, current version Available on https://cyber.gouv.fr/
[PRIS]	Cyber security incident response service providers Requirements baseline, ANSSI, current version Available on https://cyber.gouv.fr/
[ISO27001]	International Standard ISO/IEC 27001:2013: Information Technology – Security Techniques – Information Security Management Systems – Requirements Available on http://www.iso.org

III. Other document references

Reference to	Document
[PROCESS_QUALIF]	Service qualification process (<i>Processus de qualification d'un service</i>), current version. Available on https://cyber.gouv.fr/ (French)
[GUIDE_ACHAT]	Purchasing qualified security products and trusted services guidelines (Guide d'achat de produits de sécurité et de services qualifiés), current version. Available on https://cyber.gouv.fr/ (French)
[GUIDE_CNIL]	Recommendations for companies considering subscribing to Cloud Computing services (<i>Recommandations pour les entreprises qui envisagent de souscrire à des services de cloud computing</i>). Available on https://www.cnil.fr/fr/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	54/55

Appendix 2 Recommendations for commissioning entities

This appendix lists ANSSI recommendations for commissioning entities of Cloud computing service providers.

- a) The commissioning entity may, when it is an administrative authority or a vital importance operator, request ANSSI's participation in defining the specifications subject to a call for tenders or a contract.
- b) The commissioning entity should choose its service provider from the catalogue of qualified service providers published on ANSSI website, the qualification of a service provider certifying its compliance with all the requirements of this baseline.
- c) To benefit from a qualified service, i.e., one that complies with all the requirements of this baseline, the commissioning entity must:
 - choose the provider from the catalogue of qualified service providers published on ANSSI's website;
 - require the provider to specify in the service agreement that the service delivered is a qualified service.

Indeed, a qualified provider retains the ability to deliver non-qualified services. Using a provider from the catalogue of qualified service providers is therefore a necessary but not sufficient condition to benefit from a qualified service; the commissioning entity must also specifically require a qualified service.

- d) The commissioning entity should use the Guide for Purchasing Security Products and Trusted Services [\[GUIDE ACHAT\]](#), which is intended to assist the purchasing function of commissioning entities during calls for tenders.
- e) The commissioning entity may, in accordance with the qualification process for trusted service providers [\[PROCESS QUALIF\]](#), submit a complaint to ANSSI against a qualified provider if it considers that the provider has not complied with one or more requirements of this baseline in the context of a qualified service.

If, following the investigation of the complaint, it is found that the provider did not comply with one or more requirements of this baseline in the context of a qualified service, the provider's qualification may be suspended, withdrawn, or its scope of qualification reduced, depending on the severity.

- f) Provider qualification does not certify its ability to access or hold classified defence information [\[IGI 1300\]](#).
- g) Provider qualification does not certify its ability to access or hold controlled items of information systems security (ACSSI) [\[II 910\]](#).
- h) Compliance of the provider's service with the SecNumCloud baseline does not substitute for legal or regulatory requirements applicable to certain specific data, such as *Diffusion Restreinte* data or health data.
- i) For access to service management interfaces, the commissioning entity should use dedicated means (terminals, servers) for administration tasks and compliant with the recommendations of the guide [\[NT_ADMIN\]](#).

Cloud computing service providers (SecNumCloud) – Requirements baseline			
Version	Date	Distribution criterion	Page
3.2	08/03/2022	Public	55/55