User Community
Service Level Agreement

Document log

Issue	**Date**	**Comment**	**Authors**
0.1	2020 Apr 07	First draft	WP4
0.2	2020 Sep 15	Removed the types of services to be supported. Other minor changes	WP4
0.3	2020 Oct 05	Integrate corrections approved during 01 Oct's1 meeting	WP4
0.4	2020 Oct 08	Integrate corrections approved during today's meeting	WP4
0.5	2021 Mar 17	• Fix name of incident management document • Fix "policies and procedures" URL link	Massimo Sgaravatto
1.0	2021 Apr 13	First version (after internal review)	WP4

User Community: <name of user community>

The present Service Level Agreement ("the Agreement") is made between:

- INFN-Cloud (the Federator)
- The User Community: <name of User Community> (the Customer)

to define the provision and support of the provided services, as described hereafter.

The main objective of <name of UC> is <short description of goals and use cases>

This Agreement is valid from <date> to <date>.

The Agreement was discussed and approved by the INFN-Cloud management and the Customer on <date>.

Terminology

For the purpose of this Agreement, the following terms and definitions apply. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", “MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

The Services

The Services provided to the Customer and in scope for the Agreement are the INFN-Cloud core services and the computing and storage Services operated and provided by the following RCs:

Resource center<name of first RC>

Resources provided to the Customer:

- Number of virtual CPU cores:
- Memory per core (GB):
- Local disk (GB) per virtual instance:
- Number of public IP addresses:
- GPUs (number and models):
- Block storage (GB):
- Object storage (GB): ...
- Infrastructure framework used by the RC:
- Other technical information (e.g. CPU characteristics, overcommitment factors, storage configuration, etc.):

Allocation type:

☐ Pledged - Resources are exclusively reserved to the Customer

☐ Opportunistic - Resources are not exclusively allocated, but subject to local availability.

Resource center <name of second RC>

Resources provided to the Customer:

- Number of virtual CPU cores:
- Memory per core (GB):
- Local disk (GB) per virtual instance:

- Number of public IP addresses:
- GPUs (number and models):
- Block storage (GB):
- Object storage (GB): ...
- Infrastructure framework used by the RC:
- Other technical information (e.g. CPU characteristics, overcommitment factors, storage configuration, etc.):

Allocation type:

☐ Pledged - Resources are exclusively reserved to the Customer

☐ Opportunistic - Resources are not exclusively allocated, but subject to local availability.

Service hours and exceptions

IT services according to the service catalogue are in general made available during 24 hours per day, 7 days per week (i.e. 365 days or 8,760 hours). Human IT support is instead provided during the regular working hours of supporting organizations.

The following exceptions apply:

- Planned maintenance windows or service interruptions ("scheduled downtimes") must be notified in a timely manner (at least 24 hours before the start of the outage).
- Unplanned downtimes due to unforeseen circumstances must be notified as soon as possible, anyway within 24 hours.
- Downtime periods exceeding 24 hours need justification.

Support is provided via the INFN-Cloud service desk system[1].

Service request handling

Service requests (requests to address failures or service degradations, change requests, information requests, etc.) are notified through specific INFN-Cloud service desk tickets.

Each ticket reports a priority level which depends on the impact of the raised issue.

The following table summarizes the expected time by which each request must be acknowledged and the time by which the problem should be addressed.

Request priority	Acknowledge Time	Target solution time
Low	5 working days	3 months

[1] https://servicedesk.cloud.infn.it/

Normal	3 working days	2 weeks
High	1 working day	5 working days
Critical	1 working day	2 working days

Security incident handling

The detailed procedure that must follow in case of a security incident is reported in the “Scansioni di sicurezza e gestione degli incidenti su INFN Cloud” document available in the “INFN-Cloud policies and procedure” web page[3]. In the following table the needed actions and the relevant timing are summarized:

Action/event	**Timing**
Notify the INFN-Cloud security group about the problem.	No later than 4 hours after finding the problem
Isolate the system(s) involved in the incident. Decide (in collaboration with the INFN-Cloud security team if a detailed analysis is needed.	No later than 1 calendar day after finding the problem
Analyze the security incident.	Start immediately after having isolated the relevant node(s). The activity must be finished no later than 2 weeks after the initial notification about the incident
Send a comprehensive report.	No later than 2 weeks after the incident gets closed

Service level targets

Monthly Availability, defined as the ability of a service to fulfil its intended function at a specific time or over a calendar month. Minimum (as a percentage per month):

- For the INFN-Cloud PaaS central services: 95 %
- For the services provided by all RC: at least 90 %

Monthly Reliability, defined as the ability of a service to fulfil its intended function at a specific time or over a calendar month, excluding scheduled maintenance periods. Minimum (as a percentage per month): <value>%:

- For the INFN-Cloud PaaS central services: 98 %
- For the services provided by all RC: at least 95 %

Limitations and constraints

The provisioning of the services is subject to the following limitations and constraints:

- Support is provided in following languages: Italian or English.
- Availability and Reliability calculations are based on the INFN-Cloud monitoring services.
- Failures in monitoring are not considered as Agreement violations.
- Downtimes caused due to upgrades for fixing critical security issues are not considered Agreement violations.
- Force Majeure. A party shall not be liable for any failure of or delay in the performance of this Agreement for the period that such failure or delay is due to causes beyond its reasonable control. Means any
    - fire, flood, earthquake or natural phenomena,
    - war, embargo, riot, civil disorder, rebellion, revolution

  which is beyond the Federator's control, or any other causes beyond the Federator's control

Communication and contacts

The following contacts will be generally used for communications related to the service in the scope of this Agreement.

The Customer	<e-mail address>
The Federator	<e-mail address of INFN-CLOUD PMB>

Violations

The Federator commits to inform the Customer, if the Agreement is violated or violation is anticipated.

In case of violating the service targets specified in this document for three consecutive months, the Federator is requested to provide justifications to the Customer.

The Customer will notify the supporting Federator in case of suspected violation. The case will be analyzed to identify the cause and verify the violation.

Escalation and complaints

For escalation and complaints, the Federator contact point shall be used.

In case of repeated violation of the Services targets for four consecutive months, a review of the Agreement will take place involving the parties of the Agreement.

Information security and data protection

The following rules for information security and data protection apply:

- Assertion of absolute security in IT systems is impossible. The Federator is making every effort to maximize security level of users' data and minimalize possible harm in the event of an incident.
- The Federator must define and abide by an information security and data protection policy related to the service being provided.
- The parties of the Agreement must meet all requirements of any relevant INFN-Cloud policies or procedures[2] and must be compliant with the relevant national legislation.

Responsibilities of Federator

Additional responsibilities of the Federator are as follows.

- The Federator retains the right to introduce changes in how the Service is provided, in which case the Federator will promptly inform the Customer and update the Agreement accordingly.

Responsibilities of Customer

Additional responsibilities of the Customer are as follows.

- The Customer must not share access credentials with anyone else.
- The data stored in the system by the Customer must not cause any legal violation due to the content type (such as copyright infringement, dual use, illegal material).
- The use must be consistent with the Acceptable Use Policy of the Service.
- The Customer will notify the Federator in case the actual amount of the Service used results in being under- or over-estimated. The Customer will request an update of the Agreement to ensure optimal usage of the Service.

Review, extensions and termination

The Agreement will be annually reviewed until expiration.

If the Customer wishes to extend the duration after the Agreement termination date, an extension will be negotiated with the Federator.

The Federator retains the right to introduce changes in the Service, in which case the Customer retains the right of terminating the Agreement.

The Agreement can be terminated at any time upon agreement of the parties.

[2] https://www.cloud.infn.it/policies-procedures/