

# Resource Center Operation Level Agreement

## Document log

Issue	Date	Comment	Authors
0.1	2020 Apr 06	First draft	WP4
0.2	2020 Sep 15	Section “Information security and data protection” updated. Other minor changes.	WP4
0.3	2020 Oct 05	Integrate corrections approved during 01 Oct’s meeting	WP4
0.4	2020 Oct 08	Integrate corrections approved during today’s meeting	WP4
0.5	2021 Mar 17	<ul style="list-style-type: none"><li>• Added references to security incident team</li><li>• Fix name of incident management document</li><li>• Fix “policies and procedures” URL link</li></ul>	Massimo Sgaravatto
1.0	2021 Apr 13	First version after internal review	WP4

This document defines the minimum set of operational services and the respective quality parameters that a Resource Centre is required to provide in the INFN-Cloud Federation.

The present Operational Level Agreement (“the Agreement”) is made between:

- INFN-Cloud (the Federator)
- The Resource Center: <name of RC> (the RC)

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

Once approved, this Agreement is valid for as long as the RC is part of the INFN-Cloud infrastructure.

Specific agreements between the RC and individual user communities are covered in separate agreements.

## 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 operated by the RC in scope for the Agreement are only the ones relevant with the provision of computing and/or storage resources to the users of the INFN-Cloud federation.

All other services operated by the RC are out of scope.

## 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<sup>1</sup>.

## Service request handling

Service requests (requests to address failures or service degradations, change requests, information requests, etc.) that must be managed by the Resource Provider 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 by the Resource Provider.

---

<sup>1</sup> <https://servicedesk.cloud.infn.it>

Request priority	Acknowledge Time	Target solution time
Low	5 working days	3 months
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 the resource provider 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<sup>2</sup>. In the following table the needed actions and the relevant timing are summarized:

Action/event	Timing
Notify the INFN-Cloud security incident team 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 incident 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 or service component to fulfil its intended function at a specific time or over a calendar month. As reported by INFN-Cloud monitoring services.
- Minimum (as a percentage per month): 90%

### Monthly Reliability

- Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month, excluding scheduled maintenance periods. As reported by INFN-Cloud monitoring services.
- Minimum (as a percentage per month): 95%

<sup>2</sup> <https://www.cloud.infn.it/policies-procedures/>

## Limitations and constraints

The provisioning of the service under the agreed service level targets is subject to the following limitations and constraints:

- Support is provided in following languages: Italian or English
- 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 RC's control, or any other causes beyond the RC'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 Federator	<E-mail address of INFN-CLOUD PMB>
The RC	<E-mail address>

## Violations

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

In case of violating the service targets specified in this document for three consecutive months it is requested to provide justifications and a plan for service enhancement. In case of no or not satisfactory justification and plan for improvement, the RC can be removed (suspended) from the INFN-Cloud infrastructure.

## Escalation and complaints

For complaints, the defined RC contact point shall be used, and the following rules apply:

- Complaints should be directed to the Federator contact.
- The RC contact will be contacted in case of received complaints.

## 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 RC is making every effort to maximize security level of users' data and minimize possible harm in the event of an incident.
- The RC must define and abide by an information security and data protection policy related to the service being provided.
- The RC must meet all requirements of any relevant INFN-Cloud policies or procedures<sup>3</sup> and must be compliant with the relevant national legislation.
- The RC is "data-Processor" ex art. 28 of GDPR, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

## Responsibilities of the RC

Additional responsibilities of the RC are as follow:

- Adhere to all applicable operational and security INFN-cloud policies and procedures<sup>4</sup>.
- Use communication channel defined in the agreement.
- Enable the INFN-Cloud IAM service for user authentication and authorization
- Accept INFN-Cloud monitoring services provided to measure fulfilment of agreed service level targets.
- Enable and support the 'ops' INFN-Cloud IAM user group needed for monitoring and troubleshooting
- Enable operational service monitoring, provided centrally by INFN-Cloud
- Enable central security monitoring, performed by INFN-Cloud.
- Enable remote access via service APIs for troubleshooting and testing.
- Ensure at least one system administrator reachable during working hours of supporting organization.
- Ensure sufficient computational and storage resources and network connectivity to support the proper operation of its services, as indicated by passing all relevant monitoring Service tests.
- Ensure the provisioning of services in itself not create any intellectual property rights in software, information and data provided to the services provided by the RC, or in data generated by the services provided.

---

<sup>3</sup> <https://www.cloud.infn.it/policies-procedures/>

<sup>4</sup> <https://www.cloud.infn.it/policies-procedures/>

## Responsibilities of the Federator

The responsibilities of the Federator are:

- Provide the INFN-Cloud core services, that are used to access RC services.
- Provide monitoring to measure fulfilment of agreed service level targets.
- Collect requirements from the RC and ensure that these issues are properly dealt with.
- Raise any issues deemed necessary to the attention of the RC.
- Provide support by helping in the resolution of advanced and specialized operational problems that cannot be solved by the RC.
- Respond to incident and problem records from the RC in a timely manner.
- Coordinate local operational security activities and provide operational security support.
- Support coordination with other RCs.

## Withdrawals

The RC retains the right to terminate the Agreement.

The RC wishing to withdraw from the INFN-Cloud federation shall, before closing access to any resources that it has been providing, cooperate actively with the Federator to investigate possible alternative arrangements. Anyhow the Federator must be notified no later than 3 months in advance.

The withdrawing RC must support the INFN-Cloud operation team in the migration of services, data, etc. to other resources. After such migration, the withdrawing RC must delete all data pertaining to INFN-Cloud and its users, except the ones that need to be kept by law.

## Reviews of the Agreement

The Federator will promptly inform the RC about changes introduced to the requirements, service levels and targets defined in this document, and will ensure that the impact of the changes is understood.

There will be reviews of the Agreement at least every 2 years (more frequently if required).