The INFN makes available an infrastructure and a series of services in Cloud mode, called INFN-Cloud, for scientific research purposes or for the institutional purposes of INFN and other members of the federation. The use of INFN-Cloud is open to employees and associates of the INFN, or to those who have access to it by means of a project, contract or agreement with the INFN after reading, understanding and explicit acceptance of the terms and conditions indicated in this document and who have been explicitly authorized by INFN.

INFN-Cloud users are subject to the following terms and conditions:

**Definitions:**

**User:** Anyone who obtains, for any reason whatsoever, access permissions or use of resources instanced on the INFN-Cloud.

**Service Administrator:** User who has been appointed as System Administrator or who has received an appropriate appointment from the relevant body and who has been given access that allows him to instantiate resources, or to add users, or to administer a service.
Privileged User: User who, despite not having received the appointment as Service Administrator, still has the privileges but only on resources for which Inbound Connectivity has been blocked.

All constraints that apply to the User are also applicable to the Service Administrator and to the Privileged User, unless otherwise expressly indicated in the text.

1. The User undertakes to comply with all the following conditions and those defined in the document that specifies the conditions for using an IaaS, PaaS or SaaS platform.
2. The User must have accepted the rules for the use of IT resources and have completed a basic IT security course at least equivalent to the one required for INFN users.
3. The User must be identified through INFN-AAI or through an Identity Provider with recognition of at least LoA2 level. Access is subject to prior approval by INFN.
4. The Service Administrator may, at his discretion, give Users access to the resources assigned under the following conditions:
   a. The Service Administrator undertakes to verify that users are registered in identity providers that provide at least a LoA2 level of assurance, and will ensure that they accept this AUP, the conditions for using an IaaS, PaaS or SaaS, the rules of use for the use of IT resources and the INFN-Cloud Privacy Policy and who have completed a basic IT security course at least equivalent to the one required for INFN users. The Service Administrator will have to block access to users who do not accept new versions of these documents.
   b. The Service Administrator undertakes to maintain the association between the account of the users to which he will give access and their identities.
   c. The Service Administrator DOES NOT share privileged access to the resources assigned to him.
   d. If the Service Administrator wishes to share administrator responsibility on the resources assigned to him, he must follow the INFN-Cloud procedures as documented on https://www.cloud.infn.it/policies-procedures/
5. The User DOES NOT share his INFN-Cloud login credentials.
6. The User undertakes to promptly follow the instructions that will eventually be communicated to him by the INFN-Cloud security group.
7. The User undertakes to communicate any violation of these conditions to the INFN-Cloud security group.
8. The Service Administrator agrees that the resources he will install are subject to periodic security scans and undertakes to promptly resolve or mitigate any vulnerabilities that will be reported to him by following any suggestions received.
9. The use of the resources is allowed only for the institutional purposes of the INFN and of the other participants in the federation according to detailed agreements in a Project or Contract or in an Agreement.
10. The User accepts the fact that INFN does not offer any guarantee on the availability of the service.
11. The User accepts that logs on the use of the INFN-Cloud are kept in accordance with current regulations and the INFN regulations.
12. The User accepts that INFN may monitor the resources used.
13. The INFN-Cloud Administrators may provide support in response to a specific request by the User and subject to configuration, by the same, of an access to the machines using an ssh key.
14. Assigned Resources may be subject to periodic security scans.
15. Assigned Resources can be configured to transfer all logs to one or more central log servers.
16. The Privileged User must comply with all the rules that apply to Users and Service Administrators, and in addition:
   a) The Privileged User cannot give access to his resources to other Users.
   b) The Privileged User must not modify the log collection system at one or more centralized log servers.
   c) The Privileged User must have followed an intermediate level IT security course.
   d) The resources assigned to the Privileged User must process technical-scientific data. The processing of personal data must not be significant.
   e) The Privileged User will not try to circumvent the isolation measures of the resources assigned to him.

17. INFN reserves the right to modify this document in the future. The content of these new versions will completely replace this version and will have the same value as this document. These new versions will be published on the INFN-Cloud website at least one month before the entry into force and communication will be sent, using the email box used to register, to all Users who will have the option of not accepting it. Failure to accept the new version will result in the
forfeiture of the right to use the resources. Continuing to use the INFN-Cloud resources after the entry into force of the new version will imply its acceptance.

Violation of this AUP can lead to a suspension or revocation of access to the resources offered on the INFN-Cloud.

The list of IdPs that provide a level of assurance at least equal to Loa2 and whose users have taken a basic IT security course at least equal to that mandatory for INFN users can be consulted at the following address:

https://baltig.infn.it/infn-cloud/policies_and_procedures/-/raw/master/IdP-CorsoBase.txt

The list of IdPs that provide a level of assurance at least equal to Loa2 and whose users have taken an intermediate IT security course (therefore sufficient for the role of Privileged User) can be consulted at the following address:

https://baltig.infn.it/infn-cloud/policies_and_procedures/-/raw/master/IdP-CorsoIntermedio.txt

The most updated version of this document can be found at https://www.cloud.infn.it/policies-procedures/