

Terms of Use of an IaaS, PaaS and SaaS Services

Document log

Issue	Date	Comment	Authors
0.1	2020 Feb 27	First draft	Vincenzo Ciaschini
0.2	2020 Apr 03	Riunificato con documento SaaS. Chiarita meglio clausola di aggiornamento.	Vincenzo Ciaschini, Nadina Foggetti
0.3	2020 Giu 04	Ulteriori modifiche	WP4
1.0	2021 Mar 05	Prima versione	WP4
1.1	2021 Apr 13	Eliminate alcune incongruenze; compliance con lo stato attuale	Vincenzo Ciaschini, Nadina Foggetti

Hereinafter with Resources we mean the resources made available by the INFN-Cloud, in IaaS, PaaS or SaaS mode.

1. The INFN makes the use of Cloud Resources available also to third parties (hereinafter Service Administrators).
2. Access to the Platform is provided on the base of the conditions of use, as compatible, with the GARR Acceptable User Policy, with the Regulations for the use of INFN IT resources, and with the INFN Cloud User Policy
3. The User / Service Administrator declares to have all technical knowledge necessary to ensure the correct use, administration and management of the Resources made available by the INFN, and undertakes to ensure compliance with the subjects which he allows to use the Resources all the provisions set out in this document and the rules referred to therein, indemnifying and holding the INFN harmless from any request or claim for damages from anyone who is entitled to violate the aforementioned provisions and in any case in the behavior of the Service Administrator and / or the subjects to whom it has allowed the use.
4. The User / Service Administrator is allowed to dispose of the Resources in accordance with and within the limits of the Project / Agreement / Contract / Convention for which access has been granted, in compliance with all the rules referred to in point 2). It is forbidden:
 - a. To Carry out commercial, or otherwise lucrative, unauthorized activities, transmit commercial or advertising material (spamming) or allow the use of the Resources by third parties for such activities.
 - b. To carry out activities in any case in measure to damage, destroy, compromise the security of the Resources or aimed at violating confidentiality and / or causing damage to third parties.
 - c. To Implement activities aimed to bypass the provisions of this document or the Policy or the Regulations referred to in point 2 above or to obtain services in excess of those stipulated.

- d. To Create, transmit or store images, data or other material that is offensive, defamatory, obscene, indecent or that undermines human dignity, especially if it relates to sex, ethnic origin, religion, political opinion or personal or social condition.
 - e. To Use IP addresses other than those assigned.
 - f. To access or use any system without authorization, including attempts to scan and check for possible vulnerabilities.
 - g. To Forging the headers of TCP / IP packets, e-mail messages or any part of a message describing its origin or path.
 - h. To Implement port scanning, network scanning, denial of service (DoS) and distributed denial of service (DDoS) activities.
 - i. To Host services that spread unauthorized traffic, such as open relays or TOR exit nodes.
 - j. To Implement Virtual Currency Mining activities.
 - k. To Establish or operate any type of game server.
5. The Service Administrator undertakes, also in the name and on behalf of the subjects to whom he has in any capacity allowed to use the Resources, to use them exclusively for lawful purposes and in compliance with national, EU and international law, as well as regulations and customs of use of the networks and services accessed.
6. The Service Administrator declares that he is the exclusive administrator of the Resources (to the extent that the definition of administrator is appropriate for the Resources obtained) and is therefore solely responsible:
 - a. The management of the data and / or information and / or content processed by the same on the platform, their security, their saving and any useful or necessary activity to guarantee their integrity, undertaking to apply suitable and adequate security measures.
 - b. The content of information and data accessible and / or made available on the platform and in any case for any reason, transmitted or put online;
 - c. Of the malfunctions of the Resources due to uses that do not comply with the requirements set out in this document.
 - d. Loss or disclosure of login credentials.
 - e. Management of access to Resources by changing the access credentials at least every 12 months.
 - f. If the User / Service Administrator wishes to share the responsibility of administrator of the Resources and therefore no longer be the exclusive administrator, he must follow the procedures decided by the INFN-Cloud as documented on <https://www.cloud.infn.it/policies-procedures/> In any case, you will not be able to share your credentials
7. The User / Service Administrator undertakes to report as quickly as possible any use of the Resources that do not comply with the provisions of this document or any security violations he has become aware of.

8. The User / Service Administrator undertakes, also in the name and on behalf of the subjects to whom he has in any capacity allowed to use the Resources, not to install software without a regular license.
9. The User / Service Administrator is solely and exclusively responsible for any operation carried out without prior formal agreement with the INFN, relating to the use, management and administration of the Resources, with reference to which he undertakes to:
 - a. Respect and make third parties comply with the applicable legislation in force, including data protection regulations: EU Regulation no. 2016/679 and Legislative Decree n. 196/2003 as amended and integrated by Legislative Decree 101/2018 and subsequent amendments.
 - b. Indemnify and hold INFN harmless from any and all claims for direct or indirect damages, of any nature or kind, by anyone.
10. The User / Service Administrator undertakes to indemnify and hold INFN harmless from any and all questions or claims of third parties for damages caused to them by or through the use of the Resources, bearing the costs, compensation, legal fees and expenses that may arise from liability actions, undertaking to inform the INFN of the actions taken against them.
11. INFN will not be responsible for the use of the Resources in relation to critical situations that involve, including but not limited to, risks to the safety of people, damage to the environment, to services intended for people or damage to plants.
12. The INFN will not be responsible for the information, data, content entered, transmitted or otherwise processed by the User / Service Administrator in the use of the Resources and in general connected to the use of the Resources themselves. INFN reserves the right to take any initiative and action to protect its rights and interests. Any personal data entered and / or processed on the Platform by the Service Administrator will be managed in accordance with the provisions of EU Regulation no. 2016/679, as well as of Legislative Decree 196/2003 as amended and supplemented by Legislative Decree 101/2018, as well as in application of the Project / Agreement / Contract / Convention. In the absence of a specific agreement, it will be the service administrator's responsibility to notify any processing of the aforementioned data and request the adoption of any required regulatory measures.
13. INFN reserves the right to activate automatic intrusion detection (IDS) and intrusion prevention (IPS) systems to detect and prevent any violations of the security rules of the Platform.
14. INFN reserves the right to remove or block any content or resource that violates the provisions of this document.
15. INFN, at its discretion and without the exercise of this right being contested as breach or violation of any contract, reserves the right to suspend the availability of the Resources, even without prior notice, in the event that:
 - a. the User / Service Administrator violates even one of the provisions contained in this document or in the Policies and in the Regulations referred to in point 2 above;
 - b. There are well-funded reasons to believe that the Resources are being used by unauthorized third parties.
 - c. there are cases of force majeure or circumstances which, at the sole discretion of INFN, require the carrying out of emergency interventions or related to the resolution of security problems, danger for the entire network and / or for people or things; in this

case, the availability of the Resources will be restored when INFN has assessed that the causes that led to its suspension have actually been removed or eliminated.

- d. The User / Service Administrator is involved, for any reason in civil, criminal or administrative litigations, including out-of-court dispute, in the event that said dispute relates to acts and behaviors implemented through the Resources;
 - e. The suspension is requested by the Judicial Authority.
16. 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 a copy will be sent, using the email box used to register, to all the Service Administrators who will have the possibility to do not accept 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.