Document Log

Version	date	comment	author
2,0	6 december 2024	first version in EN	Nadina Foggetti

ELIXIR Acceptable Use Policy (AUP) - Conditions for the Utilization of IaaS, PaaS, SaaS, and HPC Services Provided by ELIXIR-IT

The Italian node of the European Research Infrastructure ELIXIR was formally established as a Joint Research Unit (JRU) named the Italian Bioinformatics Infrastructure (ELIXIR-IIB or ELIXIR-IT). ELIXIR-IT is coordinated by the National Research Council (CNR) and currently includes 30 partners, including several universities, research institutes, and public providers of Cloud and High-Performance Computing (HPC) services (for updates on the composition of the partnership, visit the ELIXIR-IT website at https://elixir-italy.org/) (hereinafter referred to as ELIXIR-IT).
The Italian Node of ELIXIR aims to establish the Italian Bioinformatics Research Infrastructure (IIB), distributed across multiple centers. Its goal is to support all Italian researchers working in the fields of Bioinformatics and Life Sciences, promoting the exchange and development of skills, systematizing platforms for the production of omics data and ICT with a rich set of internationally recognized bioinformatics resources that are publicly available, and contributing to their integration within the European infrastructure.
Another primary goal of ELIXIR-IT is to organize training activities, both basic and advanced, in various application areas of Bioinformatics, in order to foster the training of young bioinformaticians, a demand that is growing rapidly at national and international level.
The activities of ELIXIR are divided into technological areas, called platforms. They coordinate the provision of high-quality services for life sciences and lead the integration of national services within the ELIXIR infrastructure.
ELIXIR-IT includes six operational platforms (Compute, Data, Interoperability, Tools, Omics, and Training).
The use of the services provided is open to the entire national scientific community and businesses, upon specific request through the methods and policy defined by ELIXIR-IT, after reading, understanding, and explicitly accepting the terms and conditions outlined in this document.
These AUP (Acceptable Use Policy) apply to the services within the Compute platform.

The Compute platform offers specialized and customizable bioinformatics analysis services, computing, and storage services. These include the Laniakea in-cloud platform as an on-demand workflow management system for the analysis of biological data, the IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) platforms for hosting and distributing bioinformatics tools and services.

Definitions:

Service Manager: The individual who, in coordination with the Compute Platform Leaders of ELIXIR-IT, manages the service offered within the Platform and/or included in the ELIXIR-IT Service Delivery Plan. The Service Manager is responsible for ensuring access, managing, and monitoring the performance of the provided service.

System Administrator of the Compute Platform: Anyone within the entity providing the service in ELIXIR-IT who is assigned to manage the resources on behalf of the Service Manager.

Service Provider: The entity that, as a member of ELIXIR-IT, provides a service within the Compute Platform, such as IaaS, PaaS, SaaS, or HPC.

User: Anyone who is granted access or use of the services instantiated by ELIXIR-IT for any reason.

Service Access Administrator User: A system administrator with the necessary privileges to manage cloud resources, add users, and administer services.

Users of the services offered by the ELIXIR-IT Compute Platform are required to comply with the following terms and conditions:

1. The processing is carried out solely and exclusively based on an agreement/project that allows identifying the purpose of the research activity to be conducted;
2. The User commits to adhering to all of the following conditions and those specified in the document "Acceptable Use Policy - Conditions for the use of IaaS, PaaS, SaaS, and HPC services provided by ELIXIR-IT," which outlines the conditions for using individual services, Terms of Use, QM Policy, ELIXIR-IT Services Privacy Policy, if applicable to the specific service of interest. The user must be identified through Life Science AAI or another equivalent two-factor authentication system;
3. Access is conditioned upon prior approval by the Service Manager;
4. The Service Access Administrator may, at their discretion, grant access to Users for the resources assigned to them under the following conditions: a. The Service Access Administrator commits to identifying any User they grant access to and will be able to provide ELIXIR-IT with the list of such Users at any time; b. The Service Access Administrator commits to having this AUP, as well as the documents listed in point 1), and any updates signed by all Users they grant access to, along with the usage regulations for the IT resources adopted by ELIXIR-IT. The service access administrator must block access for users who do not accept the new versions of the cited documents. They also commit to verifying that users have completed a basic IT security course, possibly delivered through e-learning, as provided by the user's institution/entity; c. The Service Access Administrator DOES NOT share privileged access to the resources assigned to them;
5. The User DOES NOT share their access credentials to the ELIXIR-IT services;
6. The User commits to promptly following any instructions communicated by the Service Manager;
7. The User commits to reporting any violation of these conditions to the Service Manager;
8. The Service Access Administrator agrees that the resources they instantiate will be subject to periodic security scans and commits to promptly resolving or mitigating any vulnerabilities that are flagged, following any suggestions received;
9. The use of resources is granted only for the purposes outlined in the founding act of the ELIXIR-IT JRU;
10. The User accepts that ELIXIR-IT and the Service Provider cannot guarantee the continuity of the service although offering assistance and committing to promptly resolving any service interruption issues;
11. The User accepts that, unless explicitly agreed, ELIXIR-IT and the Service Provider cannot be held responsible for data backup;
12. The User accepts that logs will be kept on the use of the services offered by the ELIXIR-IT Compute Platform according to current regulations and the regulations of CNR and the entities providing the services, as well as based on the Regulation for the use of IT resources in the ICT infrastructure part of ELIXIR-IT;
13. The User accepts that personnel provided by the partner entities of the JRU, contributing to the operation of the center, may monitor the resources used;
14. The Compute Platform Administrators, upon delegation from the Service Manager, may provide support in response to a specific request from the User and after configuring access to the machines via SSH key by the user;
15. If the user requests maintenance intervention, they are responsible for backing up their data, as any potential data deletion following the maintenance intervention will not be charged to the personnel provided by ELIXIR-IT and the Service Provider.

ELIXIR-IT reserves the right to modify this document in the future. The content of the new versions will completely replace the current version and will have the same value as this document. New versions will be published on the ELIXIR-IT website at least one month before they come into effect, and a copy will be sent via email to all Users using the email address registered, giving them the opportunity to decline acceptance. Failure to accept the new version will result in the loss of the right to use the resources. Continuing to use the services provided by the Compute Platform after the new version comes into effect will imply its acceptance.
A violation of this AUP may result in the suspension or revocation of the User's access to the resources offered on the service provided.

Terms of Use (ToU) for the Utilization of IaaS, PaaS, SaaS, and HPC Services Provided by ELIXIR-IT

The Italian Node has been formally established as a Joint Research Unit (JRU), coordinated by the National Research Council (CNR), and includes several universities, research institutes, and public providers of Cloud and High Performance Computing (HPC).
ELIXIR-IT makes available, also to third parties (hereinafter Users), the use of Cloud Resources and data storage.
Hereinafter, "Resources offered by the ICT infrastructure of ELIXIR-IT," within the shared services through the Compute Platform of ELIXIR-IT, refers to resources provided in IaaS, PaaS, SaaS, HPC, and data storage modes.
Access to the Platform is granted under the conditions listed in the Acceptable Use Policy, Terms of Use, QM Policy, and ELIXIR-IT Services Privacy Policy documents.

1. The User declares to possess all the necessary technical knowledge to use the Resources provided by ELIXIR-IT and commits to ensuring that all those to whom they may grant access comply with the provisions set forth in this document and the documents listed in paragraph 3, indemnifying and holding ELIXIR-IT and the Service Provider harmless from any claims or demands for damages from anyone that may arise due to the violation of the aforementioned provisions and, in any case, due to the behavior of the User and/or the individuals to whom they have allowed access to the resources.
2. Authorization for access is granted by the Service Manager or their delegate for a limited period corresponding to the duration of the relationship under which the use of the provided IT resources is permitted.
3. The log files related to access to the services provided will be stored for a period of six months and made available to the Judicial Authority (AJ).
4. The User/System Administrator is permitted to use the Resources in accordance with and within the limits of the Project/Agreement/Contract for which access has been granted. Therefore, it is prohibited:
    a. To use the Resources for commercial purposes or for profit, transmit commercial or advertising material (spamming), or allow third parties to use the Resources for these activities.
    b. To engage in activities that could damage, destroy, or compromise the security of the Resources or that are aimed at violating confidentiality and/or causing harm to third parties.
    c. To engage in activities aimed at circumventing the provisions of this document or those in paragraph 3 of this document or to obtain services in excess of those contracted.
    d. To use IP addresses other than those assigned.
    e. To create, transmit, or store images, data, or any other material that is offensive, defamatory, obscene, indecent, or that violates human dignity, especially if related to sex, ethnicity, religion, political opinions, or personal or social condition.
    f. To access or use any system without authorization, including attempts to scan and check for possible vulnerabilities.
    g. To forge TCP/IP packet headers, email messages, or any part of a message describing its origin or path.
    h. To engage in 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 engage in Virtual Currency Mining activities.
    k. To operate or run any type of game server.
5. The Service Access Administrator undertakes, also on behalf of those to whom they have allowed access to the Resources, to use them exclusively for lawful purposes and in accordance with national, EU, and international law, as well as the regulations and customary usage of the networks and services accessed.

6. The Service Access Administrator declares to be the exclusive administrator of the Resources (to the extent that the definition of administrator is applicable to the obtained Resources) and therefore the sole responsible party for:
    a. The management of data and/or information and/or content processed on the platform, its security, backup, and any activities necessary to ensure its integrity, undertaking to apply appropriate and adequate security measures.
    b. The content of information and data accessible and/or made available on the platform and, in any case, transmitted or made available online by the User.
    c. Any malfunctions of the Resources due to uses that do not comply with the provisions of this document.
    d. The loss or disclosure of access credentials.
    e. The management of access to the Resources, ensuring that the access credentials are changed at least every 12 months.
7. The User and Service Access Administrator agree to promptly report any non-compliant use of the Resources as specified in this document or any security violations they become aware of.
8. The User and Service Access Administrator agree, also on behalf of those to whom they have allowed access to the Resources, not to install software without a valid license.
9. The User or Service Access Administrator is the sole and exclusive responsible party for any operation carried out without prior formal agreement with ELIXIR-IT, concerning the use, management, and administration of the Resources. In this regard, they undertake to:
    a. Comply with and ensure third parties comply with applicable laws, including the regulations regarding the protection of personal data as per EU Regulation No. 679/2016 and Legislative Decree No. 196/2003 and its amendments, as well as Legislative Decree No. 101/2018 and its amendments.
    b. Indemnify and hold ELIXIR-IT and the Service Provider harmless from any claims or damages, direct or indirect, of any kind or nature, made by any party.
10. The User and Service Access Administrator agree to indemnify and hold ELIXIR-IT and the Service Provider harmless from any claims or damages caused to third parties through the use of the Resources, covering the costs, damages, and legal expenses arising from liability actions, and undertakes to inform ELIXIR-IT of any legal actions initiated against them.
11. ELIXIR-IT and the Service Provider will not be held responsible under any circumstances for the use of the Resources in critical situations, including, but not limited to, risks to personal safety, environmental damage, harm to services for individuals, or damage to facilities.
12. ELIXIR-IT and the Service Provider will not be responsible for any information, data, or content input, transmitted, or processed by the User/Service Access Administrator through the use of the Resources and are entitled to take any action to protect their rights and interests.
13. The entity to which the User belongs remains the sole owner, under EU Regulation No. 679/2016 and Legislative Decree No. 196/2003 as amended by Legislative Decree No. 101/2018, of the data entered and/or processed on the Platform.
14. ELIXIR-IT and the Service Provider reserve the right to activate automatic intrusion detection (IDS) and intrusion prevention (IPS) systems to detect and prevent security rule violations on the Platform.
15. ELIXIR-IT and the Service Provider reserve the right to monitor compliance with the rules of this Policy, including monitoring network traffic and filtering systems on perimeter network devices.
16. ELIXIR-IT and the Service Provider reserve the right to remove or block any content or resource that violates the provisions of this document.
17. The User/Administrator is required to inform the Service Manager and include a thank you or citation to ELIXIR-IT and the Service used if any results, publications, posters, or abstracts arise from the use of the service provided by ELIXIR-IT.
18. ELIXIR-IT and the Service Provider, at their discretion and without the possibility of the User contesting this as a breach or violation of any contract, reserve the right to suspend the availability of the Resources without notice in the event that:
    a. The User/Service Access Administrator violates any of the provisions in the Usage Policy.

b. There are reasonable grounds to believe that the Resources are being used by unauthorized third parties.
c. Cases of force majeure or circumstances that, at the sole discretion of ELIXIR-IT and the Service Provider, require emergency actions or security problem resolution, danger to the network and/or people or property; in such cases, the availability of the Resources will be restored when ELIXIR-IT has determined that the causes leading to the suspension have been addressed.
d. The User is involved in any legal or extra-judicial civil, criminal, or administrative dispute related to acts or behaviors performed through the Resources.
e. Suspension is required by the Judicial Authority.

19. If users use ELIXIR-IT Resources for storing and processing human genetic data, compliance with the provisions of the GDPR and national legislation, including the measures outlined by the Data Protection Authority in the General Authorizations Nos. 1/2016, 3/2016, 6/2016, 8/2016, and 9/2016 as compatible with the Regulation and Legislative Decree No. 101/2018 is guaranteed.
20. The transfer of human genetic data to access the services is carried out through protected communication channels, specifically requiring the use of an encrypted channel based on the SSH protocol for data transmission.
    a. Users access and can view genetic data only through login with User ID and Password.
    b. Users accessing the Resources:

        1. Must ensure that the use of the data does not violate any third-party rights.
        2. Must ensure the anonymization or pseudonymization of the data in compliance with the GDPR.
        3. Must ensure the separate processing of genetic and health data from other personal data that could identify the data subject.

    c. The entity/center to which the User belongs must appoint a data processing officer, if this specific service is used.
21. In the event that research activities conducted using the services provided by the ELIXIR-IT Platform Compute lead to a publication/poster/abstract or any scientific result submitted for publication, the user/Service Access Administrator agrees to cite the services used and ELIXIR-IT within the scientific publication.

ELIXIR-IT reserves the right to modify this document in the future. The content of such new versions will entirely replace the current version and will have the same legal value. These new versions will be published on the ELIXIR-IT website (https://elixir-italy.org/) at least one month before they come into effect. Failure to accept the new version will result in the termination of the right to use the Resources.

Application notes:
This Terms of Use (ToU) and Acceptable Use Policy (AUP) template for services is intended to be a "Template" containing key requirements that should be common to all services offered by ELIXIR-IT, in compliance with current regulations.

22. Each Service Provider can personalize the proposed documentation by adding their own identification and reference data.
23. Each Service Provider customizes the document according to the services offered, excluding the application of the Terms to services that do not fall within the scope of the document.
24. Each Service Provider must also add their own logo, in addition to the ELIXIR-IT logo.
25. The ToU and AUP must be signed together with the Privacy Policy for the services and referenced in any contracts/agreements that govern access to the services.

Privacy Policy for Services (IPS)

Why this notice

In accordance with EU Regulation 2016/679 (hereinafter "Regulation") and Legislative Decree No. 196 of June 30, 2003, as amended by Legislative Decree 101/2018, this notice describes how personal data of users accessing the services of ELIXIR-IT through the entities that provide them are processed. These entities are identified within the Service Delivery Plan (SDP):

ELIXIR-IT

The Italian node of the European ELIXIR Infrastructure is organized as a Joint Research Unit (JRU) named the Italian Bioinformatics Infrastructure (ELIXIR-IT). It is coordinated by the National Research Council (CNR) and currently includes several partners, including universities, research institutes, and public providers of Cloud and High-Performance Computing (HPC) services. (hereinafter ELIXIR-IT).

The Italian ELIXIR Node aims to establish an Italian Bioinformatics Infrastructure (IIB) distributed across multiple centers and intends to support Italian researchers in the field of Bioinformatics, promoting the exchange and development of skills, systematizing various internationally recognized and publicly available bioinformatics resources, and contributing to their integration into the European infrastructure.

ELIXIR-IT also provides both basic and advanced training activities in various application areas of Bioinformatics to support the training of young bioinformaticians, a growing demand at national and international level.

The activities of ELIXIR-IT are divided into technological areas, called platforms. They coordinate the provision of high-quality computational services for life sciences and lead the integration of national services into the ELIXIR-IT infrastructure. ELIXIR-IT includes six operational platforms (Compute, Data, Interoperability, Tools, Omics, and Training).

The services provided are open to employees and associates of the entities that are members of the JRU and to third-party personnel participating in activities defined in a contract or agreement with ELIXIR-IT or with any JRU member, as authorized by the JRU manager, upon reading, understanding, and explicitly accepting the terms and conditions specified in this document.

Data Controller

Name of the Service Provider: (e.g., Institute of Biomembranes, Bioenergetics and Molecular Biotechnologies (CNR-IBIOM))
Address of the Service Provider: Via Giovanni Amendola, 122/O 70126 Bari (BA), Italy
Email: segreteria@ibiom.cnr.it
PEC: protocollo.ibiom@pec.cnr.it

Data Protection Officer

Data Protection Officer (for the Service Provider): Dr. Ing. Roberto Puccinelli
Email: rpd@cnr.it or dpo@cnr.it
PEC: rpd@pec.cnr.it

Processing of Personal Data for Service Use

ELIXIR-IT provides an infrastructure and a set of services for scientific research purposes or for the purposes outlined in the agreement for the establishment of the JRU or defined by other participants in the JRU.

The service is available to JRU members and their employees, or those with access through a project, contract, or agreement with the entity providing the service, as outlined in the Service Delivery Plan of ELIXIR-IT, upon reading, understanding, and explicitly accepting the terms and conditions specified in this document.

The services to which this notice applies are all those described in the technical annex to this contract.

Processing refers to any operation or set of operations regarding the collection, registration, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, deletion, and distribution of data related to the users of the services.

The Service Provider collects information to improve or develop services, generate technical insights, and ensure support.

The data processed for the use of the services are of the types specified below.

Types of Data Processed

Data provided by the user

These are all personal data provided by the user during navigation on the website, such as when registering, accessing a reserved area, or using a service.
Processing for these purposes is carried out with the explicit consent provided by the user, and the data is kept only for the duration of the requested activity. Specific notices may be published for the provision of certain activities.
The optional, explicit, and voluntary sending of emails to the addresses indicated on this site results in the subsequent acquisition of the sender's address, necessary to respond to requests, as well as any other personal data included in the message.
Sensitive or judicial data, if provided by the user, will be deleted.

Accounting Data

To access the ICT services provided by ELIXIR-IT through the Service Provider (e.g., CNR-IBIOM), user registration is required through a Life Science AAI authentication service or an identity provider recognized by CNR, as defined in the agreement/contract.

Monitoring Data

As part of the service activities, the Service Provider's personnel responsible for monitoring and managing user support interventions or conducting periodic security scans may process data related to access logs (including SSH access data).

Communication and Dissemination

The data may be communicated by the Data Controller in the course of their activities and to provide their services, to:

- Public Administrations;
- Service providers, hosting providers, and cloud service providers;
- Judicial Authority.

The collected data will not be disseminated or communicated to third parties, except as provided by the notice and the law, and in any case, only in the manner allowed by them. The data may be accessed by the Service Provider's personnel within their respective functions and in compliance with the received instructions, solely for achieving the purposes outlined in this notice.
Recipients will be appointed, if necessary, as Data Processors by the Data Controller, who may be asked for an updated list of the Data Processors. These Data Processors, under the contract, are required to use the personal data exclusively for the purposes indicated by the Data Controller, not to retain them beyond the specified duration, nor to transfer them to third parties without explicit authorization.

Methods of Processing

Personal data processing is primarily carried out using electronic procedures and supports, and in a lawful, correct, and appropriate manner, limited to what is necessary to achieve the purposes of the processing, for only the time necessary to fulfill the purposes for which they were collected, and in any case, in compliance with the principles outlined in Article 5 of EU Regulation 2019/679 GDPR.
Specific security measures are implemented to prevent data loss, unlawful or incorrect use, and unauthorized access.

Location of Data Processing

Personal data processing related to the ELIXIR-IT services provided by the Service Provider takes place at the Service Provider's facilities and is managed solely by technical staff of the office responsible for processing or by Data Processors appointed by the Data Controller who operate within the European Union. The User's personal data may be transferred to a country other than the one where the User is located. The User can verify whether any of the transfers described above occur by reviewing the section of this document related to details on the processing of Personal Data or by requesting information from the Data Controller by contacting them through the provided contact details.

Duration of Processing

The Service Provider processes the personal data collected for the time necessary to enable the use of the requested service and in any case, no longer than 12 months from the cessation of its use.

Rights of the Data Subject
Data subjects have the right to request access to personal data, rectification or deletion of data, limitation of processing, or to object to processing as provided in Articles 15 and following of the Regulation. The request must be submitted by contacting the Data Protection Officer at the contact details provided above.
Data subjects also have the right to lodge a complaint with the Data Protection Authority (https://garanteprivacy.it) or take appropriate legal action (Articles 77 and 79 of the Regulation).

Updates
This notice is subject to updates in accordance with national and EU regulations. It is recommended to consult it periodically. In case of failure to accept the changes made to this notice, the user can request the deletion of their personal data from the Data Controller.
Unless otherwise specified, the privacy policy published on the site continues to apply to the processing of personal data collected until its replacement.

Application notes:
This privacy policy template for services aims to be a "Template" containing key requirements common to all services offered by ELIXIR-IT to ensure compliance with current regulations. The privacy policies for services are mandatory.

- Each Service Provider can personalize the privacy policies by including the identification and reference data of the Data Protection Officer and the entity itself.
- Each Service Provider customizes it according to the services offered.
- Each Service Provider is required to include their own logo (in addition to the ELIXIR-IT logo).
- These policies must be signed together with the ToU and AUP for service access and referenced in any contracts/agreements governing access to the services.