



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO



Istituto Nazionale di Fisica Nucleare

Regulations for the use of IT resources in the data center ReCaS-Bari

May 15, 2020

Rev. July 2020

Rev. August 2021

Rev. October 2021

En. Ver. November 2021

1. GENERAL PRINCIPLES

On 11/02/2021 the National Institute of Nuclear Physics, INFN, and the University of Bari Aldo Moro, UNIBA, signed the "Agreement for the management of the Bari Center of the ReCaS infrastructure" (Management Agreement), located in the University Campus, Via Orabona 4, 70125 Bari at the Inter-University Physics Department "Michelangelo Merlin" of the University of Bari Aldo Moro and of the Polytechnic of Bari (Data Center ReCaS-Bari below).

In force of this agreement, the Data Center ReCaS-Bari manages the resources made available by INFN and UNIBA in accordance with the provisions of art. 4 of the aforementioned Agreement for the management of the Data Center ReCaS.

On the basis of this agreement, in particular Article 3 paragraph 1, INFN and UNIBA, each with its own staff, contribute to the operation of the Data Center Recas-Bari.

The Management Agreement implements the Joint Controller Agreement signed on 21/2/2020 by INFN and UNIBA pursuant to EU Regulation 2016/679 for the management of data processed within the ReCaS-Bari Data Center.

With these Regulations, the Data Center ReCas-Bari intends to safeguard the security of the computer system managed and to protect the confidentiality, integrity and availability of information and data, including personal data, produced, collected or otherwise processed.

This Regulation is compliant with the regulations respectively adopted by INFN and UNIBA and, where there is discrepancy, it adapts to the more restrictive of the two. Furthermore, since Data Center ReCas-Bari uses the services and tools made available to the Consortium GARR - Italian Network of University and Research, it intends to ensure with these Regulations the compliance of its own legislation with those governing the use of the network of the Research managed by the GARR Consortium.

In the Data Center ReCas-Bari, the processing of data collected in relation to the use of computing resources and network services takes place only for specific, explicit and legitimate purposes, in compliance with the principles of necessity, relevance, correctness and not excess as provided by EU Regulation 2016/679 concerning the protection of individuals with regard to the processing of personal data. The information systems and computer programs are therefore configured in such a way as to minimize the use of personal and identification data.

Regulations for the use of IT resources

All those who are allowed access to computing resources and network services are required to comply with the rules set out below, which define and integrate the minimum duties of conduct provided for by the current regulatory framework, as well as conduct based on principles of fairness and diligence.

2. SCOPE OF APPLICATION

This Regulation applies to all those who have been allowed access to the computing resources and network services managed by the Data Center Recas-Bari.

3. DEFINITIONS

For IT resources "managed by ReCaS-Bari" we mean the resources made available by INFN and UNIBA pursuant to art. 4 of the Agreement for the operation of the Data Center ReCas-Bari infrastructure and described in the Technical Annex and its subsequent amendments.

For computing resources and network services we mean:

- computers and similar electronic devices, printers and other peripherals (eg scanners and storage systems) in use at the Data Center ReCas-Bari;
- network equipment and infrastructures in use at the Data Center ReCas-Bari or in any case connected to the Centre's network;
- the connectivity service to local and geographic networks with the exclusion of mere geographic connectivity guaranteed through agreements between Institutions and Federations (eg Eduroam);
- virtual instances of computers or network devices;
- software and data purchased, produced or published in use at the Data Center ReCas-Bari.

In the context of this Regulation, computing resources and network services can be collectively defined as IT resources.

The subjects operating in the Data Center ReCas-Bari with the IT resources made available by INFN and UNIBA are divided into:

- **User:** any person who has access to the computing resources and network services of the Data Center ReCas-Bari, in relation to the functions and activities they perform;
- **User group contact person:** an INFN or UNIBA staff person who, as part of his activity, coordinates the activity of a group of users and the use of IT resources in the context of a research group, an experiment or of a service;
- **Service administrator:** a user who has an access that allows to instantiate resources, or to add users, or to administer a service;
- **System administrator:** professional figure dedicated to the management and maintenance of processing systems with which data processing, including personal data, is carried out, including database management systems, local networks and security equipment;
- **ReCaS-Bari coordinator:** figure who coordinates and supervises the activities of the Center.

Particularly:

- chairs the Joint Committee and calls its meetings, participating in it with the right to vote;
- adopts the management acts, based on the decisions of the Joint Committee;
- submits to the University of Bari and the National Institute of Nuclear Physics an annual report on the activity carried out through the use of the Centre's resources;
- appoints the Technical Manager and can appoint a Vice-Coordinator; the latter can participate in the meetings of the Scientific Technical Committee, without the right to vote.

4. ACCESS TO IT RESOURCES

The IT resources managed by the Data Center ReCas-Bari are made available in order to achieve the purposes

Regulations for the use of IT resources

of the Center:

- To provide services for scientific calculation for the needs of research activities and projects of common interest of INFN and UNIBA and in support of the institutional activities of INFN and UNIBA and, in particular, in support of the ALICE and CMS experiments in progress at the CERN International Laboratory at the Large Hadron Collider (LHC);
- To provide ICT services to support the institutional activities of INFN and UniBa;
- To provide ICT services to support the scientific communities of other national and international universities and public research bodies, on the basis of specific agreements also defined separately by the Parties, including, in particular, support for the activities of the scientific communities of ELIXIR and Lifewatch;
- To provide ICT services to support public and / or private partners of projects in which INFN and UNIBA participate, even separately;
- To maintain and strengthen the integration and collaboration of the Center with national, European and international e-infrastructures, in particular with ICDI, GARR, WLCG and EGI;
- To develop and implement new technologies for high performance scientific computing to favor the scientific communities of the Parties;
- To promote and carry out dissemination, teaching and higher education activities in the field of high performance computing and data analysis;
- To promote and carry out technology transfer and third party activities with public and private entities to encourage innovation at the local level, both of local public administrations and businesses.

Access to the computing resources and network services of the Data Center ReCas-Bari is allowed, upon identification, to structured personnel (employees and associates) of INFN and UNIBA, as well as to unstructured personnel such as collaborators, guests, PhD students, trainees, fellows, undergraduates, students who carry out their activities with INFN or UNIBA or others authorized, even independently, by INFN and UNIBA in accordance with the provisions of the Management Agreement already referred to and the provisions of these Regulations. For unstructured personnel, access to resources is allowed upon approval of the request by the user group contact.

The access authorization is issued by the Coordinator or by his delegate for a period of time limited to the duration of the relationship on the basis of which activity with the IT resources managed by the Data Center ReCas-Bari is permitted.

Access is personal, it cannot be shared or sold and its use is allowed to each user only in accordance with the rules of this Regulation.

5. GENERAL PROVISIONS FOR THE USE OF COMPUTER RESOURCES

Users are required to make use of the IT resources managed by Data Center ReCas-Bari, making their contribution so that their integrity is preserved and their proper functioning guaranteed.

There are therefore forbidden:

- activities contrary to national, EU and international law or prohibited by the regulations and customs of use of the networks and services accessed;
- commercial, or otherwise lucrative, unauthorized activities, as well as the transmission of unsolicited commercial and / or advertising material (spamming) or the use of its resources by third parties for such activities;
- activities in any case suitable for damaging, destroying, compromising the security of the IT resources managed by Data Center ReCas-Bari or aimed at violating confidentiality and / or causing damage to third parties, including the creation, transmission and storage of images, data or other offensive material, defamatory, obscene, indecent or threatening human dignity, especially if it concerns sex, race, religion, political opinion or personal or social condition;

Regulations for the use of IT resources

- activities in any case not compliant with the purposes of the Data Center ReCas-Bari.

6. SPECIFIC PROVISION FOR THE USE OF COMPUTER RESOURCES

In order to guarantee the security of computing resources and network services, it is forbidden to:

- connect computing resources to the local network or to other services that include network connectivity without the authorization of the ReCaS-Bari Coordinator or his delegate;
- wire, connect or modify network equipment without the authorization of the ReCaS-Bari Coordinator or his delegate;
- use network addresses and names not expressly assigned;
- install systems, hardware or software, which allow access to IT resources without the authorization of the ReCaS-Bari Coordinator or his delegate;
- provide access to IT resources to persons not expressly authorized;
- disclose information on the structure and configuration of IT resources, with particular reference to those that allow remote access;
- access without authorization the premises of the Data Center ReCas-Bari, as well as the premises and areas reserved for network equipment;
- undertake any other action aimed at degrading system resources, preventing authorized parties from accessing resources, obtaining resources greater than those authorized or accessing computing resources by violating their security measures.

Furthermore, **Users:**

- are required to act in accordance with the law and in compliance with the indications of this Regulation on security, guaranteeing confidentiality in the processing of personal data, also through the strict observance of the rules dictated by the Instructions for the processing of personal data of the Data Center ReCas-Bari;
- in choosing the IT tools they use, they must take into due consideration the indications of the Coordinator of the Data Center ReCas-Bari and the personnel authorized by him, in particular as regards the characteristics relating to safety, favoring the systems and procedures that offer the highest levels of protection;
- are responsible for the software they install on the computers entrusted to them: they carry out a careful preliminary evaluation and do not install software without regular licenses;
- if the data relates to particular categories of data pursuant to Article 9 of the GDPR, as well as data falling within those governed by art. 10 GDPR, they must ensure the adoption of appropriate protection measures guaranteed by national and international legislation;
- are required to accept the ReCaS AUP and these Regulations;
- are solely responsible for the information, data, content entered, transmitted or otherwise processed in the use of the Resources and in general connected to the use of the Resources themselves;
- are required to protect the data used and / or stored in their computers and systems to which they have access from unauthorized access;
- they carefully evaluate the reliability of any external services used, including cloud-type ones, in terms of data security, storage and confidentiality;
- are required to follow the instructions for periodically saving the data and programs used;
- In the event of a request for maintenance, it will be the user's responsibility to make a backup of the data, since any deletion of the data, following the maintenance intervention, can never be charged to the ReCaS-Bari staff committed to carrying it out;
- are required to protect their account with a password that respects the security rules of the ReCaS-Bari Center and, if there are more authentication systems, different for each system;
- must not disclose or communicate their password, or allow others to use their account;

Regulations for the use of IT resources

- if in possession of access codes or magnetic badges for access to the premises of the Data Center ReCaS-Bari, they must not disclose or communicate their access code to others, or allow others to use their badge;
- if for reasons of force majeure they are forced to provide their access codes or badges to others, they are required to promptly notify the coordinator within 24 hours so that the compromised access codes are disabled;
- are required to immediately report incidents, suspected abuses and security violations to the Coordinator of the Data Center ReCaS-Bari;
- for operating systems where it is possible, updated antivirus programs must be used, taking care to scan files and programs exchanged over the network and the removable media used for antivirus scanning;
- they must not maintain unused remote connections or leave the workstation with unsecured open connections;
- at the end of the employment relationship with INFN or UNIBA, or the collaboration with the Data Center ReCaS-Bari, they are required to transfer to their manager, or to the Director of the Structure or to the person delegated by this person, the files of inherent content to the service activity or collaboration and to definitively delete any other files. Within the term of 6 months from the termination of the relationship, the Data Center ReCaS-Bari deletes the data present on the IT resources referable to the user in the manner indicated in the provision of the Italian Data Protection Authority of 13 October 2008. In the event of impossibility or impediment of the User, or where the same, before the termination of the relationship, has not made available the files relating to the service or collaboration activity and has not delegated a colleague to forward them, the Director, or his delegate, can access the resources assigned to him for the period necessary to retrieve the data of interest. In the event of severe sudden unavailability or death of the User, the Director, upon request, may make files with personal content available to persons entitled.

Users who have administrator privileges on their systems (e.g. laptops, servers, virtual machines, etc.) are required to read the related documents with the Rules of Use, in implementation of the AgID Circular 04/18/2017 n. 2/2017, and to strictly follow the indications.

The accesses will take place in compliance with the provisions of the National Authority for the Protection of Personal Data and in particular with the "Measures and precautions prescribed to the owners of the treatments carried out with electronic tools in relation to the attributions of the functions of system administrator - 27 November 2008 (GU No. 300 of 24 December 2008) ".

In compliance with the provisions of art. 4 of Law 300/70, the data collected relating to access to IT services will be used guaranteeing the protection of personal data, in accordance with the relevant legislation and in the protection of economic and commercial interests, including intellectual property, copyright and trade secrets according to the specific national and international regulations in force on the subject.

7. IDENTITY AND DUTIES OF THE SYSTEM ADMINISTRATORS

System Administrators are appointed on the recommendation of the Coordinator of the Data Center ReCaS-Bari, by the Director of the Facility or Department of affiliation with a specific provision.

In addition to complying with all the previous provisions, **System Administrators** are required to:

- keep the systems at the security level appropriate for their use;
- regularly check the integrity of the systems;
- check and keep system logs for the time necessary to verify the conservation of safety standards;
- immediately report suspected abuses to the ReCaS-Bari Coordinator security breaches and participate in their management;
- install and keep up-to-date antivirus programs for the operating systems that provide it;
- not to view personal data and correspondence of which they become aware and in any case to consider them strictly confidential and not to report, duplicate or transfer information on their

Regulations for the use of IT resources

- existence or content to unauthorized persons;
- in the event of maintenance, prevent, as far as possible, access to information and personal data in the managed systems;
- follow training activities in technical-managerial and network security matters, as well as in the field of personal data protection and confidentiality of correspondence.

8. PROVISIONS FOR THE USE OF EXTERNAL SERVICES

The processing of personal data of any type or of particular importance for the Data Center ReCaS-Bari can be carried out through the use of external services, including cloud services, only if the risks and benefits associated with the services offered have been previously verified, limits in the circulation and transfer of data, as well as the reliability of the supplier, the existence of guarantees and precautions for the conservation, persistence and confidentiality of data in addition to the profiles of responsibility in the processing and after appointment of the related external managers pursuant to Article 29 of the 2016/679 EU Regulation GDPR.

9. PROCESSING OF DATA COLLECTED IN RELATION TO THE USE OF CALCULATION RESOURCES AND ACCESS TO NETWORK SERVICES.

The Data Center ReCaS-Bari, in compliance with the principles of freedom and dignity, does not allow the installation of hardware and software instruments aimed at controlling users and prohibits the processing carried out using pre-ordered remote control equipment such as:

- the systematic reading and recording of e-mail messages, beyond what is necessary to perform the e-mail service;
- the reproduction and possible systematic storage of the web pages viewed by the user;
- reading and recording of characters entered via keyboard or similar devices;
- to cover analysis of laptops entrusted in use.

With reference to access to the network, the delegated staff for the purposes indicated in the next point collects information relating to the association between address, computer name and user; it does not record the content of the connections, it can however collect some information relating to the transactions performed such as: node addresses, transaction start and end times and quantity of data transferred.

The data referred to in the previous paragraph are kept for a period not exceeding six months and can be used by delegated and competent personnel only for purposes of security control and system optimization.

The Structures in which proxy servers or other session control systems are installed can keep log files containing information relating to web pages, internal or external, accessed by local nodes. This information, kept for a period not exceeding seven days by the delegated staff, is examined or processed only when the need to ensure the safety or proper functioning of the system is identified.

10. DATA COLLECTION FOR THE E-MAIL SERVICE

First of all, it should be noted that the Data Center ReCaS-Bari manages an e-mail service exclusively for the functioning of the center. In particular, it does not manage mailboxes for users but only those of the figures provided for by the management agreement (coordinator, deputy coordinator, technical manager), to receive support requests from users, and any requests regarding the management of personal data by the interested parties.

For organizational needs related to the functioning, security and safeguarding of the e-mail service, the date, time, addresses of the sender and recipient of e-mails are recorded, as well as the result of the analysis of the anti-virus and anti-spam software.

The recorded data, also used for statistical processing, are kept for a period not exceeding one year and can only be accessed by specifically appointed personnel of the Data Center ReCaS-Bari.

The mailboxes will be deactivated with the closing of the center.

11. DATA COLLECTED IN RELATION TO THE VIDEO SURVEILLANCE SERVICE

Access to the Data Center ReCaS-Bari is subject to a video surveillance system. The use of the cameras is aimed at protecting the safety of the staff working at the Data Center ReCaS-Bari and of the subjects who access it, as well as the protection of the assets therein with respect to possible illegal actions. The data is processed in accordance with the provisions of art. 6 par. 1, letter f of the GDPR.

The video surveillance system is in operation 24 hours a day, 7 days a week. The display and management of images shot through the video surveillance system are reserved for the data controller and / or the persons formally appointed by them. The data is stored with the use of appropriate security measures to prevent access by unauthorized personnel and to ensure the confidentiality and integrity of data.

The images contained in the video recordings are stored, ordinarily, for a maximum of 72 hours from detection, subject to special needs for further conservation in relation to holidays or closure of offices and services, as well as in the event that a specific investigative request must be adhered to. of the judicial authority or police bodies. After this deadline, the images will be automatically deleted.

12. MANAGEMENT OF GENETIC OR GENOMIC DATA

If users use the ReCaS-Bari resources for the storage and processing of genetic data, compliance with the provisions set out in the GDPR as well as with the national implementation legislation will be guaranteed, including the Provision of the Italian Data Protection Authority which identifies the provisions contained in the General authorizations n. 1/2016, 3/2016, 6/2016, 8/2016 and 9/2016 as they are compatible with the Regulation and with the legislative decree n. 101/2018 to adapt the Code of 13 December 2018.

In particular, ReCaS-Bari guarantees compliance with the provisions as:

- Access to the Data Center Recas-Bari is ensured through authentication procedures - access codes - personal, so the staff can be identified at any time;
- safety devices such as surveillance cameras are provided;
- the transfer of genetic data, to access the services, is carried out through the use of protected communication channels, in particular ReCaS-Bari uses an encrypted channel based on the SSH protocol for data transmission;
- the users access and can consult the genetic data only by logging in with the insertion of User Id and Password.

Users accessing resources:

- must ensure that the use of the data does not violate any rights owned by third parties
- must ensure the anonymization or pseudonymization of the data used in accordance with the provisions of the GDPR;
- they must guarantee the separate processing of genetic and health data from other personal data that allow for the identification of the persons concerned.

12. ADDITIONAL MEASURES FOR THE PROTECTION OF INFORMATION SYSTEMS

In order to ensure the functionality, availability, optimization, security and integrity of the information systems and prevent improper use, the Data Center ReCaS-Bari adopts measures that allow the verification of anomalous behavior or conduct not provided for in this Regulation in compliance with the general principles of necessity, relevance and non-excess referred to above. To this end, the Data Center ReCaS-Bari may perform processing on the recorded data aimed at highlighting anomalies in network traffic or conduct not permitted by these Regulations.

Regulations for the use of IT resources

In the event that, despite the adoption of preventive technical measures, harmful events occur, or anomalous or unauthorized behaviors are detected, the Data Center ReCaS-Bari carries out, after informing the interested parties and except in cases of necessity and urgency, further checks and adopts the measures necessary to stop harmful or prohibited conduct.

In cases of recurrence of prohibited and already reported or particularly serious behaviors, the Coordinator of the Data Center ReCaS-Bari arranges for the adoption of all the necessary technical measures, so that the subjects in charge of processing data relating to the use of the internet and mail electronics carry out only the operations strictly necessary for the pursuit of the related purposes, without carrying out remote control activities, not even on their own initiative.

13. BREACH OF RULES

Any conduct in breach of this Regulation may result in the suspension of access to IT and network resources managed by ReCaS-Bari.

The violation of the provisions of this Regulation that causes damage to third parties compensated by one of the Controllers may determine, against the person responsible, the exercise of the right of recourse as established in the Joint Controllers Agreement and in the forms and limits established by law.

14. PRIVACY DISCLAIMER

This Regulation constitutes information on the methods and purposes of the processing of personal data connected to the use of computing resources and network services.

The Data Center ReCaS-Bari ensures the widest dissemination of this Regulation and its subsequent updates to users by publishing it on the web page of the portal www.recas-bari.it, as well as delivering it to everyone electronically, however suitable for demonstrating the successful delivery.

15. CLAUSE OF REVIEW AND POSTPONEMENT

These Regulations, approved by the Joint Committee of the Data Center ReCaS-Bari at its meeting on May 15, 2020, will be periodically updated in relation to the evolution of technology and sector legislation.

For matters not covered by this regulation, please refer to the similar regulation in force at your institution.