Regulation
on the Use of INFN IT Resources

October 2025

Rev. 26/10/2025

1. General Principles

INFN considers its computing resources and network services, as well as the data and information processed through them, to be an integral part of its assets and instrumental to the achievement of its institutional objectives in scientific and technological research.

Through this Regulation, INFN aims to safeguard the security of its information system and to protect the confidentiality, integrity, and availability of information and data, including personal data, that are collected, generated, or otherwise processed.

Furthermore, by adhering to the Consortium GARR – the Italian Research and Education Network – and by using its related services and tools, INFN intends, through this Regulation, to ensure that its internal rules comply with those established by the Consortium GARR.

Within INFN, the processing of data collected through the use of computing resources and network services shall take place solely for specified, explicit, and legitimate purposes, in compliance with the principles of necessity, relevance, lawfulness, fairness, and data minimisation, as provided for by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (hereinafter referred to as the "**GDPR**").

In order to achieve its institutional objectives, INFN implements, uses, and manages artificial intelligence systems in compliance with applicable European and national legislation, safeguarding the values, freedoms, rights, and autonomy of the individual, whom it regards as an active and fundamental participant in human and scientific progress.

2. Scope Of Application

This Regulation applies to all individuals who have been granted access to INFN's information technology resources.

The provisions set forth below supplement the minimum duties of conduct established in the INFN Code of Conduct[1].

[1] https://l.infn.it/codicecomportamento

3. Definitions

For the purposes of this Regulation, *IT resources* shall mean:

- computers and similar electronic devices, printers, and other peripherals owned by the Institute or otherwise connected to the Institute's network;
- network devices and infrastructures owned by the Institute or otherwise connected to the Institute's network;
- connectivity services to local and wide area networks, with the exclusion of mere wide area connectivity provided through agreements among institutions and federations (e.g. eduroam);
- virtual instances of computers or network devices;
- databases and the systems for their management;
- infrastructures and services provided by the Institute's Organizational Units and centrally through the Information Systems Directorate and the CCR National Services;
- infrastructures and services provided or managed by the Institute on the INFN cloud (DataCloud) or on external cloud platforms, including commercial ones;
- software and data purchased, produced, or published by the Institute.

The individuals who operate using the Institute's IT resources are classified as follows:

- **user**: any individual who has access to the Institute's IT resources, in relation to the functions and activities carried out within the Institute;
- **privileged user**: any individual who holds administrative credentials for the individual resource assigned to them, without being formally appointed as a system administrator;
- **system administrator**: a professional role, equipped with privileged credentials, dedicated to the management and maintenance of data processing systems through which data, including personal data, are processed; this includes database management systems, web services, local area networks, and security devices;
- IT resources responsible team: the group responsible for the management and security of IT resources, as well as internal and external network connections within each Organizational Unit or other operational context, and for maintenance, installation, development, and support activities; this shall include the Computing Services at the Organizational Units, the Information Systems Directorate (DSI), the INFN DataCloud management group, and any other team designated as such by a governing body of the Institute or by the Reference Director;
- Reference Director: the Director of the Organizational Unit to which the IT resources and the responsible team belong; in the case of distributed infrastructures, the individual expressly appointed by a governing body of the Institute.

4. Access To IT Resources

Access to INFN's IT resources shall be granted, subject to prior identification, to employees and associates, as well as to collaborators, visitors, PhD candidates, postgraduate trainees, research fellows, grant holders, and undergraduate students, including those affiliated with institutions, companies, or organizations partnering with INFN within the framework of projects, collaborations, contracts, or otherwise authorized in accordance with the provisions of this Regulation.

Identification shall be carried out through the verification of a valid identity document or through equivalent procedures or tools.

Access to IT resources shall also be conditional upon acceptance of this Regulation, any supplementary rules of use[2], Acceptable Use Policies (AUPs) and Terms of Use (ToUs) specific to the service, as well as upon successful completion of an information security training course appropriate to the criticality of the resources[3].

Access to IT resources shall be verified through individual authentication credentials.

Where access is granted to individuals external to INFN, identification, verification of information security competence and authentication may be delegated to the relevant Organization, subject to an agreement included in the collaboration document ensuring compliance with the above-mentioned requirements.

Authorization for access, for the duration of the relationship under which use of INFN's IT resources is permitted, shall be granted by the reference Director or by a delegate thereof.

Access is strictly personal and may not be shared or transferred.

5. General Provisions

IT resources constitute essential assets for INFN and are made available for the pursuit of its institutional objectives.

Users shall make use of the Institute's IT resources in such a way as to contribute to preserving their integrity and ensuring their proper operation.

The following activities are therefore prohibited:

1. activities that are contrary to national, European Union, or international law;
2. activities prohibited by the regulations and customary rules governing the use of the networks and services accessed;
3. unauthorized commercial or otherwise profit-making activities, as well as the transmission of unsolicited commercial and/or advertising material, or the use of one's own resources by third parties for such activities;
4. activities capable of damaging, destroying, or compromising the security of the Institute's IT resources, or aimed at violating confidentiality or causing harm to third parties, including the creation, transmission, or storage of images, data, or other material that is offensive, defamatory, obscene, indecent, or that infringes upon human dignity, especially where related to sex, ethnicity, religion, political opinions, or personal or social status;
5. activities that may harm the reputation of the Institute;
6. activities that are in any case not consistent with the Institute's institutional objectives.

The use of IT resources for personal purposes is tolerated, provided that it does not violate applicable laws, does not interfere with the proper functioning of the infrastructures, is compatible with the provisions of this Regulation and of the supplementary rules of use[4], and is limited in duration and frequency.

6. Specific Provisions On The Use Of IT Resources

For information security reasons, the following actions are prohibited:

[2] https://security.infn.it/computing-rules

[3] https://security.infn.it/computing-rules/formazione-sicurezza-informatica

[4] https://security.infn.it/computing-rules

1. connecting computing resources to the local network or to other services that include network connectivity without the authorization of the IT resources responsible team;
2. connecting network devices or modifying their configuration without the authorization of the IT resources responsible team;
3. using network addresses or names without the authorization of the IT resources responsible team;
4. installing systems, hardware, or software that allow access to IT resources without the authorization of the IT resources responsible team;
5. granting access to IT resources to individuals who are not expressly authorized;
6. disclosing information classified as confidential concerning the structure and configuration of IT resources, in particular information that enables remote access;
7. accessing, without authorization, premises dedicated to hosting computing resources, as well as areas reserved for network equipment;
8. undertaking any action aimed at degrading system resources, preventing authorized users from accessing them, obtaining resources beyond those authorized, or accessing resources in violation of security measures.

6.1 Users

In addition to the provisions already set forth, **users** shall:

1. act in compliance with the information security guidelines issued by the INFN Cybersecurity Unit (NUCS), by the IT resources responsible team, as well as with the rules established by INFN for the processing of personal data, as published on the Data Protection Officer (DPO) web pages[5];
2. be responsible for the data and software they install on the IT resources entrusted to them, carry out a careful prior assessment thereof, and, under no circumstances, install software that is not covered by valid licenses;
3. protect against unauthorized access the data used or stored in the systems to which they have access;
4. protect their accounts by means of passwords that comply with the relevant security requirements[6];
5. neither disclose nor communicate their passwords, nor allow others to use their accounts;
6. comply with the instructions provided by the IT resources responsible team regarding the periodic backup of data and programs;
7. not circumvent the isolation and security measures applied to the assigned resources;
8. immediately report to the IT resources responsible team any incidents, suspected abuses, or security breaches;
9. use up-to-date antivirus software and ensure that files and programs exchanged over the network, as well as removable media, are scanned for malware prior to use;
10. not maintain unused remote connections, nor leave workstations unattended with open, unprotected connections;
11. where mobile devices are used, comply with the provisions set out in the section **Mobile Devices**;

[5] https://dpo.infn.it

[6] https://security.infn.it/computing-rules/password-policy

12. upon termination of their relationship with INFN, transfer to their supervisor, the Reference Director, or a person delegated by the latter, all data related to their work activities and delete any other data;
13. comply with any further instructions on the matter that may be issued by the Institute.

6.2 Privileged Users

In addition to complying with the provisions set out above, **privileged users** shall**:**

1. review the documents setting out the technical rules for the use of individual IT devices[7] and comply with the relevant instructions;
2. not grant other users access to the resources assigned to them;
3. not interfere with the log collection system;
4. use up-to-date antivirus software on the systems they manage, ensuring that files and programs exchanged over the network, as well as removable media, are scanned for malware prior to use;
5. comply with any other instructions on the matter that may be issued by the Institute.

6.3 System Administrators

System administrators shall be individually appointed by the Reference Director or by a person delegated by the latter. In the case of external users, the appointment may be made by the relevant affiliated organization, in accordance with the procedures set out in the collaboration agreement.

In addition to complying with the provisions set out above, **system administrators** shall:

1. maintain systems at a level of security appropriate to their intended use;
2. regularly verify the integrity of systems;
3. monitor and retain system logs for the period necessary to verify compliance with security standards;
4. grant access to assigned resources only after verifying that the user complies with the conditions set out in the section **Access to IT Resources**;
5. maintain the association between user accounts and user identities;
6. not share privileged access to the assigned resources;
7. immediately report to the IT resources responsible team any incidents, suspected abuses, or security breaches, and participate in their management;
8. • install and keep antivirus software up to date for operating systems for which such software is applicable;
9. not access personal data or correspondence, except where strictly necessary for technical purposes, and in general always treat such information as strictly confidential;
10. in the event of maintenance activities carried out by external support personnel, prevent, as far as possible, access to information and personal data contained in the administered systems;
11. undertake training activities in technical and operational matters, network, system or service security, and personal data protection;
12. comply with any other instructions on the matter that may be issued by the Institute.

6.4 IT Resources Responsible Team

The **IT resources responsible team** shall:

[7] https://security.infn.it/computing-rules

1. be responsible for the management and security of the IT resources within its area of competence;
2. comply with the information security guidelines issued by the INFN Cybersecurity Unit (NUCS);
3. grant access to assigned resources only after verifying that the user complies with the conditions set out in the section **Access to IT Resources**;
4. ensure that remote access to local resources is carried out exclusively through the use of protocols that provide authentication and encryption of transmitted data;
5. disable non-essential services on the managed systems and limit the number of privileged users to the minimum strictly necessary for network and service coordination, control, and monitoring activities;
6. carry out a review of user accounts at least on an annual basis;
7. monitor the network and the managed systems, including resources used for the provision of cloud services, in order to ensure their functionality and security;
8. implement filtering and logging systems on network perimeter devices;
9. immediately report security incidents to NUCS;
10. provide support to maintain and enhance the security of the resources entrusted to users;
11. comply with any other instructions on the matter that may be issued by the Institute.

7. Artificial Intelligence Systems

The use of Artificial Intelligence Systems shall ensure compliance with applicable laws and with the principles of cost-effectiveness, effectiveness, efficiency, impartiality, openness, transparency, fairness, accountability, security, environmental sustainability, non-discrimination, and the protection of the confidentiality of personal data and intellectual property.

For this purpose, the use of artificial intelligence within the Institute shall be permitted in compliance with applicable regulations and with any specific internal regulations or guidelines developed for this purpose.

In order to ensure the protection of data confidentiality, including with regard to the GDPR, the use of external Artificial Intelligence tools shall be treated as the use of external services in general and shall be governed by the section **Provisions on the Use of External Services.**

8. Provisions On The Use Of External Services

The processing of personal data of any kind, or of data of particular relevance to the Institute, may be carried out through the use of IT services provided by external parties only where INFN, through the Data Protection Officer (DPO), the IT resources responsible team, or other competent roles, has previously assessed the risks and benefits associated with the services offered, the limitations on data circulation and transfer, as well as the reliability of the provider, the existence of appropriate safeguards and measures for data retention, persistence, and confidentiality, and the liability profiles related to data processing, and has defined the qualification of the relationships in accordance with the provisions of the GDPR.

In the case of cloud services intended for the Institute's administrative and management activities, such services shall be qualified for use by Public Administrations.

The list of approved external services, categorized by type of use[8], shall be kept up to date by the Computing and Networks Commission.

[8] https://security.infn.it/computing-rules/servizi-esterni

9. Data Collected In Relation To The Use Of IT Resources

INFN does not allow the installation of hardware or software tools specifically aimed at monitoring users and prohibits processing carried out by means of equipment designed for remote monitoring.

INFN prohibits the processing of personal data acquired for any purpose for the monitoring and profiling of users' activities, except as provided for and within the limits set out below.

9.1 User Data

INFN provides users with systems for the storage of their data that support tools for read and write access protection. It is the user's responsibility to apply the necessary configurations in order to ensure adequate protection of such data.

The IT resources responsible team may access such data in the event of malfunctions, for the purpose of creating backup copies, or when explicitly requested by the user.

Such information may contain personal data.

9.2 Backup And Restore

In order to ensure the resilience of data relating to systems, services, and users, the IT resources responsible team acquires and stores daily and/or weekly backup copies.

Such data may contain personal data.

This processing is carried out solely for the purpose of restoring data availability when necessary.

Backups shall be retained for a period not exceeding 12 months, after which they shall be permanently deleted from the storage systems.

9.3 Log Data

In order to ensure the operational functionality of IT systems and services, the IT resources responsible team collects and stores application and network connection log data.

Such data may contain personal data.

Logs shall be stored on systems accessible only to authorized members of the team and may be analyzed for the purpose of addressing and resolving any malfunctions or information security incidents.

Logs shall be retained for a period not exceeding six months, after which they shall be permanently deleted.

9.4 Data For Information Security

In order to counter attempts at unauthorized access and to best support the protection and security of data and services, NUCS and the IT resources responsible team may automatically collect information relating to the configuration of devices connected to INFN networks, network connections, and user activities.

The collected information, which may contain personal data, shall be stored on systems dedicated to cybersecurity, on internal resources, or on external cloud services. Where external cloud services are used, such resources shall comply with the requirements set out in the section **Provisions on the Use of External Services**.

The relevant data shall be exclusively available to NUCS and the IT resources responsible team and shall be processed solely for the purpose of identifying, managing, or preventing information security incidents.

Data shall be processed by automated tools. In the event of a potential anomaly, the relevant data shall be analyzed manually; in such cases, the users concerned shall be informed of matters within their competence and may be requested to provide further information regarding the incident.

Users shall cooperate with NUCS personnel or the team and provide all information available to them.

Data collected for information security activities shall be retained for a period not exceeding six months, after which they shall be permanently deleted.

In the event of a significant-impact incident, the relevant data may be retained in encrypted form for longer periods, in order to enable compliance with ensuing obligations and to facilitate audits and inspections by the competent Authorities.

9.5 Electronic Mail

The automatic forwarding of an entire INFN email mailbox to non-INFN domains, in particular to commercial domains, is not permitted.

Metadata relating to electronic mail (logs) shall be processed as described in the section **Log Data**, but for a period not exceeding 21 days.

The email mailbox shall be deactivated upon expiry of the authorization period for access to INFN resources, activating, where possible, a system that informs correspondents of alternative addresses related to the user's professional activity.

The contents of the mailbox shall be deleted within 12 months from the expiry of the authorization period for access. This period may be extended by the Reference Director for duly justified reasons related to service requirements.

9.6 Special Categories Of Data

Pursuant to the GDPR, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data concerning health, sex life or sexual orientation, as well as data relating to criminal convictions and offences, require a higher level of security and protection.

The processing of personal data and special categories of data shall be carried out only by personnel who have been expressly appointed and are adequately trained.

The transmission of special categories of data shall in any case always be carried out using state-of-the-art encryption protocols, in accordance with the policies defined in the supplementary documents.

In the case of the processing of genetic data, compliance with national implementing legislation, in addition to the provisions of the GDPR, shall be ensured. For this purpose, the processing of genetic data, including for research purposes, shall be authorized only on infrastructures and by personnel expressly qualified for such activities. INFN infrastructures dedicated to such processing shall be qualified through standard ISO certifications.

9.7 Urgent And Non-Deferrable Access To Work-Related Information

Where it is necessary and non-deferrable to access data or messages related to work activities that are in the exclusive possession of a user, and only in cases of prolonged unavailability or serious impediment, the Reference Director or a delegate thereof may access the user's data and messages in order to identify and extract information relevant to the performance of work activities.

A formal record of such access shall be drawn up, and the user shall be informed as soon as possible.

9.8 Expiry Of Employment Or Collaboration Relationship

Upon termination of the employment or collaboration relationship, access to IT resources shall be revoked. By that time, the user shall be required to make collaboration-related data available to colleagues and to transfer personal data elsewhere.

At the user's request, the Reference Director may authorize an extension of access for a maximum period of two months solely for the purpose of completing such transfers.

Within 12 months from the termination of the employment or collaboration relationship, INFN shall proceed with the deletion of data stored on IT resources that are attributable to the user.

In the event of serious unavailability or death of the user, the Reference Director may, upon request, make personal-content data available to entitled parties, in the cases and in accordance with the procedures provided for by applicable law.

10. Mobile Devices

The use of mobile devices entails specific risks related to their portability and their possible use for personal purposes.

INFN adopts the measures necessary to comply with the obligations set out in this Regulation with respect to mobile devices owned by the Institute (Corporate-Owned, Personally-Enabled – COPE). The user to whom a COPE device is assigned shall be held responsible for any damage caused by negligent use or in cases where the security measures adopted by the Institute have been reduced or removed.

In order to safeguard employees' privacy, the security of the Institute's infrastructures, and the data processed in connection with work activities, the use of personal mobile devices (Bring Your Own Device – BYOD) for work-related purposes shall be permitted exclusively subject to prior acceptance of, and compliance with, specific policies governing device management, data and network security, acceptable use practices, and data backup and restore procedures.

11. Additional Measures For The Protection Of Information Systems

In order to ensure the functionality, availability, optimization, security, and integrity of information systems and to prevent improper use, INFN, following the provision of an appropriate information notice in accordance with the GDPR, adopts measures that allow the verification of anomalous behavior or conduct not permitted under this Regulation, in compliance with the general principles of necessity, relevance, and data minimization referred to above. For this purpose, the IT resources responsible team or NUCS may carry out processing of recorded data in order to detect anomalies in network traffic or conduct that is not permitted.

Where harmful events occur or prohibited conduct is detected, the IT resources responsible team or NUCS shall, following notification to the data subjects and except in cases of necessity and urgency, carry out further investigations and adopt the measures necessary to interrupt such harmful or prohibited conduct.

In cases of repeated prohibited behavior or of particular seriousness, the IT resources responsible team shall adopt all necessary technical measures and shall immediately notify the Reference Director, who shall order further actions in accordance with the section **Violation of the Rules**.

12. Violation Of The Rules

Any conduct carried out in violation of this Regulation may result in the suspension of access to IT resources, without prejudice to any disciplinary, civil, or criminal actions.

Any breach of the provisions of this Regulation that causes damage to third parties for which INFN has provided compensation may result in the exercise of the right of recourse against the responsible party, in the forms and within the limits established by law.

13. Final Provisions

This Regulation repeals and fully replaces all previous regulations adopted on the same subject matter.

INFN shall ensure the widest possible dissemination of this Regulation and of any subsequent updates to users by publishing it on the web page of each organizational unit, as well as by delivering it to each user in electronic or paper form, in any case in a manner suitable to demonstrate proof of delivery.

The supplementary documents referred to in the preceding sections, as well as any others that may become necessary as a result of technological developments, shall constitute an integral part of this Regulation.

Such documents shall be updated by the Computing and Networks Commission, in coordination with the Digital Transition Officer, and shall be available at the following address: https://security.infn.it/computing-rules.

14. Review Clause

This Regulation shall be periodically updated in accordance with the evolution of technology and of the applicable regulatory framework.