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.

INFN Password Policy

CCR_SEC_01
Rev. 01 - 24/08/2025

This document defines the minimum security requirements that must be met when creating and managing user passwords in INFN information systems. Its purpose is to ensure effective protection of user accounts and data, as well as of INFN IT resources.

Where feasible, these requirements shall be enforced and supported by password selection interfaces, to assist users in complying with them.

1. The password used for an INFN account must be different from the passwords used to access external services, such as social media platforms, personal email accounts, commercial platforms, accounts with other institutions, etc.
2. A password is a sequence of characters that must meet the following requirements:
    a. Shall have a minimum length of 10 characters;
    b. Shall contain at least three (3) of the following types of characters:
        i. Lowercase letters: abcdefghijklmnopqrstuvwxyz
        ii. Uppercase letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
        iii. Digits: 0123456789
        iv. Punctuation symbols: ,:;?!
        v. Special characters: -_+*#@^=|\"£$%&/()§°çòàùéèì[]{}€<>
    c. Shall have a maximum validity of 1 year and a minimum validity of 1 day;
    d. Shall be different from the last five (5) passwords used;
    e. Shall not be trivial, such as repetitions of the same character, sequences of adjacent keyboard keys, dictionary words or personal data related to the account;
3. Passwords must never be stored in unencrypted form, whether on electronic or paper media.
4. Credentials for accessing INFN systems are strictly personal: passwords must never be disclosed to anyone.

Information Security Training

CCR_SEC_02
Rev. 02 - 28/09/2025

In order to obtain access to INFN IT resources, applicants are required to complete an information security training course appropriate to the criticality of the resources and to the level of privileges requested.

Training courses may be delivered either in person or online. In all cases, successful completion of the course must be verified through a final assessment.

Where access is granted to individuals external to INFN, information security training may be certified by the relevant affiliated organization, in accordance with the procedures set out in the INFN Regulation on the Use of IT Resources.

This document defines the minimum content that must be covered by information security training in the various cases.

Basic Information Security Training Course

All individuals requesting access to INFN IT resources are required to complete a basic information security training course.

INFN provides its users with a basic training course available online, accessible via INFN authentication, at the following link:

https://elearning.infn.it/course/view.php?id=105

The course covers the following topics:

1. Obligations, Rules of Use, and General Information
   an overview of current legal obligations and applicable regulations concerning users of INFN IT resources
2. Protection of Personal IT Devices
   measures and best practices to protect personal devices against unauthorized access
3. E-mail and Web Usage
   security risks related to the use of email and web browsing, including social engineering attacks (e.g. phishing)
4. Passwords
   guidelines for the selection, management, and protection of access credentials
5. File and Data Protection
   instructions and recommendations to ensure the protection of personal data stored on devices or external storage systems

6. Copyright and file sharing
   awareness-raising on copyright and intellectual property concepts, as well as on the potential consequences of their violation
7. Awareness of Information Security Issues
   promoting awareness of information security risks and of the importance of the information acquired and processed in daily work activities

The training course is subject to periodic review in line with technological developments and emerging security threats. In the event of a revision, users will be required to complete the updated version of the course.

Provisions for the Use of External Services to Host or Process INFN Data and Documents

CCR_SEC_03
Rev. 01 - 24/08/2025

This document sets out the criteria under which users of INFN IT resources may use external services for their activities, including cloud services and Artificial Intelligence platforms, depending on the type of data processed, to ensure an adequate level of confidentiality, including for the processing of personal data in compliance with the GDPR.

1. General guidelines

Whenever possible, it is always preferable to process data using one of INFN's internal services, such as Alfresco (docs.infn.it), Pandora (pandora.infn.it), INFN GitLab (baltig.infn.it), INFN Wiki (confluence.infn.it, wiki.infn.it), or by using applications, even if externally developed, that are installed on INFN resources.

When relying on an external service, users are required to carefully consider the following aspects:

- it is essential to ensure continued access to data for as long as necessary, including in the long term;
- contractual terms relating to intellectual property and the associated rights concerning the use of data and information made available must be carefully evaluated;
- vendor lock-in must be avoided; therefore, a procedure for retrieving data from the external platform in the event of service discontinuation must be planned.

Any service provided by an external supplier and used for administrative or management activities must be certified by the Italian National Cybersecurity Agency (ACN). The catalogue of certified services is available on the ACN website.

Before purchasing any external service, users must consult the relevant IT resources responsible team, the local representative on the Computing and Networks Commission, or the Digital Transition Office, in order to verify service compatibility and to ensure that the required functionality is not already available through internally developed solutions or external services centrally procured by INFN.

2. Ordinary data

Ordinary data refers to data that is essentially public, such as experimental or collaboration data, which does not have specific confidentiality requirements and for which the presence of ordinary personal data is negligible.

Without prejudice to the provisions set out in the section "**General Guidelines**", no specific restrictions apply to this type of data. Any external resource, whether collaborative or commercial, including free services, may be used.

Examples:

- tools managed by organizations with which INFN has collaboration agreements (e.g. CERN, EGI, ...);
- commercial cloud tools and services, including those offered free of charge, such as services provided by Amazon, Google, Microsoft, Dropbox, GitLab, etc.

Processing documents containing this type of data using external artificial intelligence systems, such as OpenAI ChatGPT or Microsoft Copilot, including free versions, is permitted.

3. Confidential scientific data

Confidential scientific data refers to technical and scientific data that is subject to confidentiality requirements. Examples include:

- experimental data not yet publicly released (e.g. data under embargo or subject to closed licenses);
- drafts of scientific publications of particular relevance;
- technological pending patent applications;
- data covered by non-disclosure agreements (NDAs);
- source code, including partial code, subject to any form of reuse license or owned by INFN.

Such data may be processed on external services, whether commercial or non-commercial, provided that a service contract or collaboration agreement is in place that ensures confidentiality.

The currently authorized external services are:

- Office 365 platform on the INFN tenant (Microsoft SharePoint, Teams, OneDrive, etc.);
- in the case of data owned by a scientific collaboration, external storage systems authorized by the collaboration itself.

Processing documents containing this type of data using the following artificial intelligence systems is authorized:

- Microsoft Copilot, licensed version, on the INFN tenant.

Processing on external artificial intelligence systems other than those listed above is not permitted, including unlicensed versions of Copilot on the INFN tenant.

Users are responsible for adopting appropriate measures to ensure data protection, including the correct configuration of permissions and access-sharing links.

It is necessary to consider the characteristics of the services used and to retain control over data protection and availability.

When data is shared by offices or collaborations, the use of private areas—even in cloud environments (e.g. OneDrive)—is strongly discouraged. Shared areas (e.g. SharePoint) should be used instead, to avoid data loss when an account is closed.

External cloud areas must be used exclusively for data and document processing phases and not for long-term storage, for which INFN's document management system—equipped with a backup system—is available.

4. Dati Personal Data and Special Categories of Non-Genetic Data

This category includes data for which the presence of ordinary personal data is significant, or which contains special categories of personal data other than genetic data.

Examples include:

- documents related to recruitment or selection committees;
- documents related to procurement procedures;
- documents managed by AC Directorates;
- documents managed by human resources services;
- documents managed by occupational health and safety services;
- data related to accounting and monitoring of INFN IT resource usage by users;
- data processed to ensure the security of INFN information systems, such as endpoint protection and threat analysis data.

The processing of such data requires compliance with GDPR provisions, which can only be ensured through internal services or through contracted external services that are certified as suitable for hosting cloud services for the Public Administration, or for which a risk assessment has been carried out. Such assessment must verify limitations on data circulation and transfer, the reliability of the provider, the existence of appropriate safeguards for data retention, persistence, and confidentiality, and the allocation of responsibilities under the GDPR.

To ensure the highest level of security, such data must be stored on systems internal to the Institute or by using applications—even if externally developed—that are installed on INFN resources.

The use of external services, duly qualified as described above, is permitted only where necessary, such as for service outsourcing (e.g. payroll, endpoint protection) or for data sharing during processing phases using tools or environments not covered by internal systems.

Users are responsible for adopting appropriate measures to ensure data protection, including correct permission settings and access-sharing configurations.

In all cases, data must be removed from the external platform at the end of the processing phase and deposited for long-term storage on internal systems, such as Alfresco (https://docs.infn.it).

The currently authorized external cloud services are:

- Zucchetti (limited to payroll services);
- Office 365 platform on the INFN tenant (SharePoint, Teams, etc.);
- Microsoft Endpoint Protection (INFN tenant only).

The use of Microsoft OneDrive or other personal areas for data and documents shared by offices or collaborations is strongly discouraged, for the same reasons outlined above.

Processing documents containing this type of data using the following artificial intelligence systems is authorized:

- Microsoft Copilot, licensed version, on the INFN tenant.

Processing on external artificial intelligence systems other than those listed above is not permitted, including unlicensed versions of Copilot on the INFN tenant.

5. Genetic data

In the case of processing genetic data, compliance with national implementing legislation must be ensured in addition to the provisions of the GDPR.

For this purpose, the processing of genetic data on external services, including for research purposes, may be authorized only on infrastructures or cloud services **explicitly qualified for this purpose**, through certifications or suitability declarations issued by the competent national authorities (ACN).

Processing genetic data on external artificial intelligence platforms is not permitted, even where such platforms are covered by an INFN contract.

Mobile Devices

CCR_SEC_04
Rev. 01 24/08/2025

This document establishes requirements and guidelines for the use of mobile computing devices (smartphones, tablets, laptops), whether personally owned or owned by third parties (BYOD – Bring Your Own Device) or provided by INFN (COPE – Corporate-Owned, Personally Enabled), for accessing INFN IT resources.

Its objective is to preserve information security, ensure compliance with the INFN IT Resources Regulation, and promote responsible use of INFN IT resources, while at the same time ensuring maximum flexibility for staff work activities.

1. Scope

This Regulation applies to all individuals who have been granted access to INFN IT resources and who access such resources via COPE or BYOD devices.

2. General Provisions

The use of BYOD devices for work-related activities is permitted, including access to email, documents and services, to the wired and wireless networks of INFN Operating Units, in compliance with the guidelines set out below.

COPE devices may be used for personal activities within the limits defined in the INFN Regulation on the Use of IT Resources.

When using COPE devices (at all times) and BYOD devices when connected to INFN networks (wired, wireless, or via VPN), it is mandatory to fully comply with the provisions set out in the INFN Regulation on the Use of IT Resources, in particular with regard to the prohibition of illegal activities, activities contrary to accepted network and service usage practices, or activities that may harm the reputation of the Institute.

Unless explicitly stated otherwise, the following provisions shall be considered mandatory for COPE devices and recommended guidelines for BYOD devices.

3. Device protection

- it is not permitted to create user accounts other than the personal account on the device;
- accounts must not be shared (mandatory also for BYOD devices);
- in the case of BYOD devices, the creation of additional privileged accounts is strongly discouraged;
- access to the device must be protected by a sufficiently complex password or PIN, or by biometric authentication (mandatory also for BYOD devices);
- the device must be locked when left unattended, and automatic lock due to inactivity must be configured (mandatory also for BYOD devices);
- the theft or loss of a COPE device must be immediately reported to the relevant IT resources responsible team; in case of BYOD devices, reporting is required only if the device has been registered for direct connection to INFN networks.

4. System and Software Security

- the operating system and applications installed on the device must always be kept up to date with the latest available releases.
- applications must be installed exclusively from certified repositories, such as the Apple App Store, Microsoft Store, or Google Play.
- COPE devices must be associated with the INFN Microsoft XDR protection platform in accordance with the instructions provided by the relevant IT resources responsible team.
  For BYOD devices, the installation of antivirus/anti-malware protection software is strongly recommended.
- it is not permitted to circumvent the security configurations of the device.

5. Data Security

- where possible, disk and data encryption must be configured on the device;
- access to INFN data and documents must be carried out exclusively using secure protocols or applications (mandatory also for BYOD devices);
- it is not permitted to store INFN documents and data on unauthorized external cloud services (mandatory also for BYOD devices);
- backup copies of the device and of the data and configurations contained therein may be stored only in end-to-end encrypted form.
  Where device backups include INFN data, documents, or credentials, this requirement is mandatory also for BYOD devices.

6. Network access

- the use of unencrypted wireless networks to access INFN resources is discouraged.
  Where necessary, such networks may be used provided that an INFN-provided VPN connection is activated or that access to INFN resources is carried out exclusively through encrypted protocols;

- access to wired local networks is permitted only following identification of the device (e.g. MAC address registration) or of the user (e.g. 802.1X), in accordance with the procedures defined by the relevant IT resources responsible team (mandatory also for BYOD devices).

Policy on the Use and Management of Cryptographic Techniques

CCR_SEC_05
Rev. 02 26/10/2025

1. Purpose

This policy defines the principles and rules governing the use of cryptography within the organization in order to:

- ensure the confidentiality, integrity, and authenticity of the information processed;
- protect information and communications, with particular regard to data considered critical (hereinafter referred to as *confidential data*) in relation to the organization's operations (e.g. special categories of personal data under the GDPR, or other sensitive data according to any applicable data classification scheme);
- ensure compliance with applicable regulations and guidelines in force.

2. Scope of Application

This policy applies to all INFN information systems and services that process *confidential data* for the purposes of the organization's operations; it identifies and distinguishes obligations, requirements, and best practices applicable to:

- System Administrators and Privileged Users
- Standard Users – employees, associates, guests, and visitors

3. General Principles

The use of cryptography shall in all cases comply with the following fundamental principles:

- **Necessity and proportionality** – Cryptographic measures shall be applied in accordance with the level of risk and any applicable data classification;
- **Use of recognized algorithms** – Only cryptographic algorithms and protocols recognized by international standards and classified therein as secure shall be used;
- **Key security** – Cryptographic keys (personal and service X.509 certificates, SSH keys, keys for data and document encryption) shall be considered critical security assets for the organization and must be generated, managed, and protected appropriately, following, where applicable, the requirements set out below.

4. General Provisions

Protection of Data at Rest:

- Disk encryption is recommended for servers and workstations hosting *confidential data*; disk encryption is mandatory for mobile devices containing *confidential data*;

- Encryption is mandatory for *confidential data* stored on unauthorized external cloud services; encryption keys must not reside on the same devices that store the data to which they relate;
- Cryptographic keys shall, where required, be protected by non-trivial passphrases and stored on secure devices; they shall not be stored on network-shared locations unless strictly necessary for service operation.

Protection of Data in Transit:

- It is mandatory to use exclusively secure protocols (TLS) or secure applications (SSH, VPN) for services that expose *confidential data* (including via APIs) or require authenticated access (web portals, email sending and reading, interactive access);
- Cryptographic keys must not be transmitted over unencrypted channels;
- Any legacy services providing unencrypted access that cannot support secure protocols for technical reasons must be exposed only on private networks and adequately protected by perimeter or local firewalls; exposing services using clear-text authentication protocols (telnet, FTP, authenticated HTTP) on wide-area networks is prohibited;
- The use of end-to-end encryption is mandatory for the transmission of *confidential data* via email;
- When accessing INFN resources and services from public or insecure networks, it is mandatory to use VPN services provided by the relevant IT resources responsible teams or to use exclusively encrypted network protocols.

Backup Protection

- Encryption of backup and archival media, or alternatively the use of backup applications that support data encryption, is **recommended**;
- It is **mandatory** to encrypt backups before transferring them over the network, or to use encrypted transmission protocols.
- It is **mandatory** to encrypt backups stored on external cloud services

5. Provisions for System Administrators and Privileged Users

5.1 SSH/TSL implementation

Management of Certificates and Private Keys

- Keys shall be generated on a trusted, preferably isolated system with sufficient entropy.
- RSA keys must have a minimum length of **2048 bits**; for particularly critical applications, the use of **3072-bit RSA keys** should be considered, or, where performance is a concern, **ECDSA keys of 256 bits or more**.
- The signature hashing algorithm must be at least **SHA-256**.
- For user-facing services, it is **mandatory** to use certificates issued by public Certification Authorities (CAs), and certificates approaching expiration must be renewed in a timely manner.
  The use of self-signed certificates for such services is not permitted.

Permitted Protocols and Recommended Configurations

- The use of **SSL v2** and **SSL v3** (both insecure and obsolete) is explicitly prohibited.
- **TLS v1.0** and **TLS v1.1** are considered legacy protocols, were officially deprecated in January 2020, and should not be used.
- **TLS v1.2** and **TLS v1.3** present no known security issues and should be the primary—and preferably **the only—supported protocols**.
- Only secure cipher suites should be used (preferably with server-side selection), supporting **Perfect Forward Secrecy (PFS)** and strong key exchange mechanisms. For detailed guidance, reference should be made to the *"Cryptographic Functions Guidelines"* published by ACN.
- Exposed services should be periodically reviewed using TLS scanning tools (e.g. *testssl.sh*, *Qualys SSL Server Test*).

5.2. SSH Server Configuration

SSH (minimum supported version: **2.0**) supports multiple key exchange algorithms, encryption algorithms, and message authentication codes to ensure authenticity, confidentiality, and integrity of communications between server and client. Obsolete, weak, or potentially compromised algorithms **must** be disabled, even at the risk of incompatibility with legacy clients.

To assess the security of exposed SSH server configurations, the use of the *ssh-audit* tool (https://github.com/jtesta/ssh-audit, https://www.sshaudit.com/) is recommended, along with the application of the associated hardening guidelines.

5.3. Email Server Configuration

For authenticated mail servers and mail access services, the requirements defined for SSL/TLS configuration apply, with particular care taken to prohibit clear-text access to services. The implementation of **opportunistic TLS** on MTAs is recommended, in order to maximize communication security while maintaining interoperability with MTAs that do not support encryption.

6. Provisions for Users

Management of Certificates and Private Keys

RSA certificate keys must have a minimum length of 2048 bits; however, it is recommended to request certificates with larger key sizes (3072 or 4096 bits) or, where supported by the target systems, certificates using ECDSA keys of 128 or 256 bits.

Management of SSH Private Keys

The SSH keys that currently offer the best balance between security and performance are traditional RSA keys and the more recent EdDSA keys based on elliptic curves. RSA keys must have a minimum length of 2048 bits, corresponding to approximately 112-bit security (on RedHat–like systems version 9 or later, the default is 3072 bits, equivalent to 128-bit security). Elliptic curve–based keys have a fixed length.

End-to-End Encryption

The use of end-to-end encryption is mandatory for the transmission of sensitive data. This requirement is particularly stringent for email, as it ensures long-term confidentiality of mailbox contents.

Use of Public Wireless Networks and VPNs

The use of unencrypted public wireless networks to access organizational resources is discouraged. Where necessary, such networks may be used only if exclusively encrypted protocols are employed to access INFN data and services, or if a VPN connection provided by the relevant organizational unit is activated.

INFN
Istituto Nazionale di Fisica Nucleare

Rules for the Use of Linux Operating Systems

V 2.0 – 15/10/2025

Table of Contents:

1. Introduction

This guide sets out procedures, actions and configurations aimed at implementing the requirements described by AgID Circular No. 2/2017 of 18 April 2017, "**Minimum ICT Security Measures for Public Administrations** (Directive of the President of the Council of Ministers of 1 August 2015)" (Official Gazette, General Series No. 103 of 5 May 2017), by the **General Data Protection Regulation (GDPR)**, as implemented in Italy by Legislative Decree No. 101/2018, by the recent **NIS2 Directive**, as transposed in Italy by Legislative Decree No. 138/2024, and, finally, by the **INFN Regulation on the Use of IT Resources**.

2. Recommendations for the Use of Personal Devices

Holders of an administrative account on one or more personal devices may limit themselves to following the recommendations set out in this section. Individuals who have been formally appointed as system administrators shall implement all the measures established in this document.
For the purposes of this document, personal devices shall mean desktop or laptop computers assigned to users in the context of their work activities, on which no accounts of other users are present and on which confidential data are not stored on a continuous basis.
For such devices, the appointment of a system administrator by the Reference Director is not required.

Users of personal devices shall:

a) use operating systems that are currently supported and authorized by the relevant IT resources responsible team (see Section 4);

b) regularly apply operating system security updates (see Section 7.a);

c) ensure that operating system protection software (firewall, antimalware, etc.) is enabled and kept up to date (see Sections 5, 10, and 14);

d) ensure that access to the operating system is protected by a strong password and is in any case compliant with the password policies adopted by INFN;

e) not install software obtained from unofficial sources or repositories, for which an appropriate license is not held, or that is expressly prohibited by the relevant IT resources responsible team;

f) lock access to the system and/or configure automatic screen locking when leaving the workstation unattended;

g) not click on links or attachments contained in suspicious emails and apply appropriate measures for malware protection (see Section 9);

h) connect only to mobile storage devices (USB drives, external hard disks, etc.) whose origin is known (new devices, previously used devices, or devices provided by the relevant IT resources responsible team);

i) configure disk encryption on laptops and configure disk encryption on desktop systems that store confidential or personal data (see Section 12).

3. Responsibilities of the System Administrator

Procedures, actions and configurations aimed at implementing the requirements, limited to the minimum security level, shall be identified by the following keywords and enclosed within a box (in the case of measures required only for multi-user systems, the text background shall be grey):

IT IS MANDATORY,
MUST,
IT MUST BE.

It shall be the duty and responsibility of the system administrator to implement the measures so identified.
All indications not marked by the above-mentioned keywords are recommendations not explicitly required under the minimum security level set out in the Circular, but are nevertheless advised in order to improve system security.

4. Installation and Configuration of the Operating System

In order to use standard secure configurations for the protection of operating systems, it is recommended to coordinate the installation and configuration of GNU/Linux operating systems with the relevant IT resources responsible team, in accordance with the procedures established by the team itself.

Systems that are preinstalled or whose configuration is not fully known, should not be connected to the network

Where physical access to the machine is not controlled, it is recommended to:

- set a password to access the BIOS;
- disable booting from external devices in the BIOS;
- set a password in the boot loader (e.g. **grub**).

a. Installation

If a semi-automated installation system provided by the relevant IT resources responsible team is not used, only installation images obtained from official repositories or provided by the team **MUST** be used, and their checksums **MUST** be verified against those published in the repository.

If preconfigured virtual images, containers, or Docker images are used, administrative credentials **MUST** be changed before connecting the system to the network.[1]

If the installation image has not been provided by the relevant IT resources responsible team, it **MUST** be stored on media kept offline.

Only supported and stable versions **MUST** be installed, avoiding the use of obsolete or testing versions. Where it is necessary to keep non-upgradable systems in production, risk mitigation measures **MUST** be applied, such as isolating the device from the rest of the network.

It is recommended to periodically verify the operating system end-of-life (EOL) date through authoritative sources, such as the vendor's official website or online aggregators (e.g. https://endoflife.date/).

In the case of servers, it is recommended to perform a minimal operating system installation, avoiding the installation of software that is not strictly necessary for the operation of the services provided.

In the case of servers providing centralized services, **IT IS MANDATORY** to compile and keep up to date an inventory of the software in use and their respective versions.

In accordance with the provisions set out in the INFN Regulation on the Use of IT Resources, the IP addresses in use **MUST** be assigned by the relevant IT resources responsible team, either directly or through DHCP servers.

b. Configuration and First Boot

The passwords of all administrative accounts:

- **MUST** comply with the password policy adopted by INFN.

Any form of root login outside the virtual consoles (tty*), including access via SSH, **MUST** be disabled.

1 For example, by disabling the network interface and performing the operation as an administrator via the virtual console.

It is recommended to perform the following actions at first boot:

- ensure that the package management system verifies package signatures using **GPG**, in order to reduce the risk of installing suspicious packages;
- close all services that are not strictly necessary and prevent them from starting at boot time; in particular, on laptops, disable the Bluetooth service and enable it only when required;
- if not required, remove the following user accounts: adm, ftp, games, gopher, halt, lp, mail, news, operator, shutdown, userdel, uucp;
- if not required, remove the following groups: adm, dip, games, groupdel, lp, mail, news, uucp;
- disable special system accounts (e.g. nobody, sync) required for system operation by setting their shell in /etc/passwd to /bin/false;
- verify that the root password is required when the system is started in single-user mode; if this is not the case, enforce authentication in single-user mode as well, especially where uncontrolled physical access to the machine may be possible;
- control access to services and resources by specific IP addresses through nftables or firewalld rules;
- control access to services and resources by specific users through PAM libraries (e.g. pam_access via the /etc/security/access.conf file) or through centralized authorization systems such as SSSD.

c. Filesystem sharing

Where it is necessary to share a filesystem (via CIFS, NFS, etc.), the following guidelines shall be followed:

- prevent root access (where possible)[2];
- mount the filesystem in read-only mode (where possible)
- always limit filesystem exposure to the strictly necessary hosts;
- periodically review access status (for example, for NFS, by using the showmount command);
- where the filesystem is defined in /etc/fstab, use the nosuid option;
- where possible, filter access ports by allowing access only from authorized devices, using a firewall (e.g. nftables or firewalld).

2 This requirement is very stringent and, in most cases, practically difficult to apply. Its feasibility should nevertheless be evaluated in order to improve protection against ransomware (e.g. Reveton, CryptoLocker, WannaCry, etc.)

5. Remote Access to the System

To access the system remotely, only software that uses secure protocols **MUST** be used (e.g. **SSH, SCP, RDP, VNC over TLS**).

In order to simplify authentication and authorization processes, some services and applications allow remote machines to be configured as “trusted” machines, from which it is possible to access the service or application directly, including in a non-interactive manner. The configuration of such trust relationships is generally discouraged.

Automatic remote access for configuration purposes or other operations **MUST** be implemented through asymmetric key mechanisms and **MUST** be restricted exclusively to the intended IP addresses.

6. Maintenance

a. System Update

The system **MUST** be kept continuously up to date. All security patches **MUST** be applied as soon as they become available. To this end, automatic update mechanisms (e.g. via cron) may be configured both for distribution packages and for external software.

Where the use of automatic updates is deemed inappropriate, an alerting mechanism **MUST** nevertheless be in place to verify the availability of updates. In such cases, it is mandatory to assign a priority level to vulnerability remediation actions based on the associated risk. Patches **MUST** be applied starting with the most critical ones.

Following significant system changes (e.g. the addition of new services), **IT IS MANDATORY** to agree with the relevant IT resources responsible team on the execution of a security scan in order to identify any additional vulnerabilities. Once the scan has been completed, all necessary actions **MUST** be taken to remediate the identified vulnerabilities or, where this is not possible, to document the accepted risk and notify the Computing Service accordingly.

b. Verification of Accounts and Credentials

It is recommended to periodically perform checks on user accounts using dedicated tools. John the Ripper is a useful tool for assessing password strength in Linux and Unix environments; as of 2025, its Jumbo version supports modern hash algorithms and GPU acceleration. However, tools such as Hashcat, Hydra, and Patator provide advanced capabilities for distributed checks, online testing, and protocol-specific assessments.

7. User Management

Administrative privileges **MUST** be restricted to users who possess the appropriate competencies and an operational need to modify system configurations.

IT IS MANDATORY to maintain an inventory of all administrative accounts, ensuring that each of them is duly and formally authorized.

Administrative accounts **MUST** be used exclusively to perform operations that require elevated privileges, and every access **MUST** be logged. For this purpose, **IT IS MANDATORY** to always use sudo to execute administrative commands.

IT IS MANDATORY to ensure a clear separation between privileged and non-privileged accounts of administrators, which **MUST** be associated with different credentials. In other words, if a user of a system also holds the role of system administrator, such user **MUST** have two separate accounts, only one of which shall be a member of the *sudoers* group and used to perform administrative commands.

IT IS MANDATORY that all accounts, particularly administrative ones, be nominative and attributable to a single individual.

IT IS MANDATORY that all accounts created be authorized in accordance with the INFN Regulation on the Use of IT Resources**.**

8. Management of Files Containing Critical or “Institute-Relevant” Data

Files containing data subject to specific confidentiality requirements (Institute-relevant data) or critical information such as personal certificates, server certificates, **SSH** private keys, **GPG** keys, etc. **MUST** be stored with permissions set to 600 (rw- --- ---) or 400 (r-- --- ---).

It is recommended to protect private keys with a password (for example, using openssl), to store them on an encrypted filesystem (e.g. LUKS, ext4 fscrypt), and, where possible, to use different keys for different service accounts.

9. Malware Protection

IT IS MANDATORY to install and properly configure integrated anti-malware systems (e.g. Microsoft EDR/XDR, Wazuh XDR, etc.).

IT IS MANDATORY to use a *firewall* (e.g. Nftables or Firewalld)

IT IS MANDATORY to restrict the use of external devices exclusively to situations that are strictly necessary for the performance of work activities.

It is recommended to disable the automatic opening of email messages and the automatic preview of file contents.

10. Backups

IT IS MANDATORY to perform at least weekly backups of the "information strictly necessary for the complete restoration of the system".

In the case of cloud-based backups, or where it is not possible to ensure the confidentiality of the information contained in backup copies through adequate physical protection of the storage media, **IT IS MANDATORY** to:

- encrypt the backups prior to transmission
- ensure that the backup site is not permanently accessible over the network

in order to prevent attacks on the system from affecting all backup copies.

11. Data encryption

For laptops, the use of an encrypted file system is recommended. It is also advisable for desktop workstations on which data requiring specific confidentiality requirements are stored. It is recommended to enable encryption during the operating system installation.

The Institute's guidelines regarding the types of files that **MUST** be protected through encryption **SHALL** be complied with, ensuring that private keys are adequately protected.

12. System Compromise

In the event of a system compromise, the relevant IT resources responsible team **MUST** be informed immediately.

System restoration **MUST** be carried out using the images saved at the conclusion of the installation and configuration phase, or by performing a new installation.

13. Log Files

Periodic analysis of log files is a practice that helps resolve security issues as well as system misconfiguration problems.

It is therefore recommended to adjust the logging level of each machine and the log retention period according to the criticality of the system, within the limits defined by the Regulation.

Where possible, it is recommended to keep a copy of log messages on another machine (remote logging).

14. Additional Recommendations

Do not use setuid scripts; always use sudo instead.

Install software for monitoring the integrity of system files, such as *ossec* or AIDE.

It is recommended to filter all system services except those that are strictly necessary.

E-mail servers **MUST NOT** be activated.
The system administrator **MUST** agree on the activation of web services with the relevant IT resources responsible team.

Examples of periodic checks:

- Verify that network interfaces (both Ethernet and wireless) are not operating in promiscuous mode;
- Verify that the /dev/mem and /dev/kmem devices are not readable by all users;
- Verify that all device files are owned by the root user, with the exception of terminal devices;
- Verify that no "regular files" are present in the /dev directory;
- Install software for monitoring the integrity of system files (File Integrity Monitoring), such as *ossec*;
- Verify the presence of files with the SUID/SGID bit enabled
  ```
  find / -type f \( -perm -04000 -o -perm -02000 \) -exec ls -l {} \;
  ```
- Verify the presence of files with unusual names, such as "..." (three dots), ".. " (dot-dot-space), or "..^G" (dot-dot-control-G):
  ```
  find / -name ".. " -print -xdev
  find / -name ".*" -print -xdev | cat -v
  ```
- Verify the presence of world-writable files and directories:
  ```
  find / -type f \( -perm -2 -o -perm -20 \) -exec ls -lg {} \;
  find / -type d \( -perm -2 -o -perm -20 \) -exec ls -ldg {} \;
  ```
- Verify the presence of files that do not belong to any user (excluding those that may appear in the /devdirectory):
  ```
  find / -nouser -o -nogroup
  ```
- Verify the presence of *.rhosts* files; if such files are required to exist, ensure at least that they do not contain wildcards or comment lines.
- Verify user umask settings (the root user's umask should be at least 0x22).

Rules for the Use of Windows Operating Systems

v 2.0 – 01/10/2025

Table of Contents:

Introduction

This guide sets out procedures, actions, and configurations aimed at implementing the requirements laid down by AgID Circular No. 2/2017 of 18 April 2017, "**Minimum ICT Security Measures for Public Administrations** (Directive of the President of the Council of Ministers of 1 August 2015)" (Official Gazette, General Series No. 103 of 5 May 2017), by the General Data Protection Regulation (GDPR), as implemented in Italy by Legislative Decree No. 101/2018, by the recent **NIS2 Directive**, as transposed in Italy by Legislative Decree No. 138/2024, and, finally, by the **INFN Regulation on the Use of IT Resources.**

Responsibilities of the System Administrator

Procedures, actions, and configurations aimed at implementing the requirements laid down in the AgID Circular, limited to the minimum security level, shall be identified by the following keywords and enclosed within a box (in the case of measures required only for multi-user systems, the background shall be grey):

IT IS MANDATORY,
MUST / MUST BE,
[NOT] IT MUST BE / [NOT] IT MUST BE.

It shall be the duty and responsibility of the system administrator to implement the measures so identified. The obligations set out in the section *User Management* apply only to multi-user systems.

All indications not marked by the above-mentioned keywords are recommendations not explicitly required under the minimum security level set out in the Circular, but are nevertheless advised in order to improve system security.

Installation and Configuration of the Operating System

In order to use standard secure configurations for the protection of operating systems [ABSC ID 3.1.1, 3.2.1], the installation and configuration phase of Windows operating systems must be coordinated with the Computing Services operating within the relevant Operational Unit, in accordance with the procedures established by such services, in addition to those set out in this guide.

Where virtual images or preconfigured installations are used, administrative credentials
MUST be changed before connecting the system to the network

.

Preinstalled systems, or systems whose configuration is not fully known, should not be connected to the network.

Where the machine will operate in environments with unrestricted physical access by students or other individuals not subject to INFN information security policies, it is recommended to:

- set a password to access the BIOS;

- disable booting from floppy disks, CDs, or USB devices in the BIOS;
- enable Secure Boot.

Installation

If it is not possible to use a semi-automated installation system provided by the relevant IT resources responsible team, only installation images obtained from official repositories or provided by the team **MUST** be used, and their checksums **MUST** be verified against those published in the repository.

If the installation image has not been provided by the team, it **MUST** be stored on offline media.

Only supported and stable versions should be installed, avoiding obsolete, unmaintained, or testing versions.

In the case of servers providing centralized services, **IT IS MANDATORY** to compile and keep up to date an inventory of the software in use and their respective versions.

In accordance with the INFN Regulation on the Use of IT Resources, with regard to network configuration, where a DHCP server is present, systems must be configured to obtain network configuration via such service, where static IP addresses are used, only IP addresses assigned by the relevant IT resources responsible team MUST be used.

In all cases, arbitrary IP addresses not assigned by the team **MUST NOT** be used, whether assigned directly to the user or via DHCP.

Configuration and first boot

In order to increase operating system security, it is recommended to perform the following actions at first boot, preferably while disconnected from the network.

Operating System Version

For laptops and desktop systems, the use of Windows Home editions **is prohibited**, as they are not supported by Microsoft's endpoint protection platform.

Computer Name

The computer name (hostname) must be agreed with the relevant IT resources responsible team in order to facilitate system identification.

User Name

During initial setup, Windows requests the creation of a Microsoft account. It is recommended instead to configure a local account by selecting “Sign-in options” and then “Domain join instead”.

Package Signature Verification

Ensure that the package management system verifies package signatures in order to reduce the risk of installing suspicious software.

Removal of Unnecessary Packages

To reduce the attack surface, it is recommended to remove all software packages that are not strictly necessary for the operating system, services, or tools in use.

Password Constraint

Group Policies **MUST** be configured to ensure that administrative account credentials comply with the password policy defined by the Institute.

Blocking of Special Accounts

Where possible, the **Administrator** account **MUST** remain disabled, and a separate administrative account should be created, to be used only in exceptional cases, with a non-significant username (e.g. not “**root**”, “**administrator**”, “**superuser**”).

Access to Services by Specific Users

Access to services and resources by specific users can be controlled (prevented, limited, and monitored) through Group Policy.

Access to Specific Ports or Services via Network

Access to specific ports and services can be controlled by appropriately configuring the firewall.

It is prohibited to activate email or messaging services. Any other services, such as web servers, **MUST** be agreed with the relevant IT resources responsible team.

File Sharing

Where it is necessary to share files or folders, sharing must be properly configured by applying at least the following restrictions:

- prevent sharing with **everyone**;
- allow *sharing* only to a restricted group of users by assigning appropriate permissions (read/write, read-only, etc.)

Remote Access to the System

Remote access to the system **MUST** take place exclusively via RDP (Remote Desktop Connection) with Network Level Authentication enabled, and with explicit specification of the accounts authorized to use it.

Maintenance

System Update

The operating system **MUST** be kept continuously up to date. All security patches **MUST** be applied as soon as they become available. Automatic updates should be enabled for both the operating system and installed software.

Where critical services are present that may be disrupted by automatic updates, an alerting system **MUST** be in place to ensure updates are applied through interactive procedures as soon as possible. In such cases, remediation actions **MUST** be prioritized based on the associated risk, and the most critical vulnerabilities **MUST** be addressed first.

Where vulnerabilities cannot be resolved, the accepted risk **MUST** be documented and communicated to the relevant IT resources responsible team.

Following significant system changes (e.g. the addition of new services), **IT IS MANDATORY** to agree with the team on the execution of a security scan. Once completed, all necessary actions **MUST** be taken to remediate identified vulnerabilities or to document accepted risks.

Verification of Accounts and Credentials

To verify the robustness of administrative credentials, it is recommended to configure appropriate Group Policies (minimum length, complexity) and to periodically perform checks using dedicated tools on user account password files.

User Management

All accounts created on a device **MUST** be authorized in accordance with the *INFN Regulation on the Use of IT Resources*.

Administrative privileges **MUST** be restricted to users with appropriate competencies and operational necessity.

An inventory of all administrative accounts **MUST** be maintained, ensuring that each account is formally authorized.

Administrative accounts **MUST** be used exclusively for operations requiring elevated privileges, and all access **MUST** be logged.

A clear separation between privileged and non-privileged accounts **MUST** be ensured, with distinct credentials. If a user also holds an administrative role, they must have two separate accounts, only one of which belongs to the Administrators group. All accounts, especially administrative ones, MUST be nominative and attributable to a single individual.

Management of Files Containing Critical or “Institute-Relevant” Data

Access to files containing data subject to specific confidentiality requirements or critical information (e.g. personal certificates, server certificates, **SSH** private keys, **GPG** keys) **MUST** be restricted to the owner only.

Malware protection

The endpoint protection agent provided by the Institute **MUST** be installed, with automatic updates enabled and automatic scanning of removable media upon connection.
The use of a personal firewall **IS MANDATORY**, and the IPS features of the endpoint protection agent **MUST** be enabled.
The use of external devices **MUST** be strictly limited to situations strictly necessary for work activities.
Autoplay of removable media **MUST** be disabled.
Automatic execution of dynamic content (e.g. macros) **MUST** be disabled.
Automatic opening of email messages and file previews **MUST** be disabled

Backup

IT IS MANDATORY to perform at least weekly backups of the information strictly necessary for full system recovery, especially on systems containing user data.

Where backups are stored in the cloud, or where confidentiality cannot be ensured through physical protection, **IT IS MANDATORY** to encrypt backups before transmission and ensure that backup systems are not permanently accessible over the network, in order to prevent attacks from affecting backup copies as well[1].

Data Encryption

For laptops, the use of an encrypted filesystem (e.g. **BitLocker**) is recommended to ensure that data cannot be accessed in case of loss or theft.
The use of encrypted filesystems is also recommended for desktop systems hosting data requiring specific confidentiality requirements.

The Institute's guidelines regarding the types of files that **MUST** be protected through encryption shall be complied with, ensuring that private keys are adequately protected.

System Compromise

In the event of a system compromise, the relevant IT resources responsible team **MUST** be informed immediately, and the recovery procedure must be agreed with the team.

System restoration **MUST** be carried out using images saved at the conclusion of the installation and configuration phase, or by performing a new installation[2].

1. The aim of this rule is to improve the protection against ransomware (Reveton, CryptoLocker, WannaCry, …).
2. See "Installation".

Log Files

The maintenance and periodic analysis of log files help identify and resolve security issues as well as system misconfigurations.

Where possible, it is recommended to store copies of log messages on another system.

Examples of log files to be copied to another system include:

- **%SystemRoot%\System32\Winevt\Logs\Application.evtx**
- **%SystemRoot%\System32\Winevt\Logs\Security.evtx**
- **%SystemRoot%\System32\Winevt\Logs\Setup.evtx**
- **%SystemRoot%\System32\Winevt\Logs\System.evtx**

Rules for the Use of Apple macOS Operating Systems

V 2.1 – 27/10/2025

Table of Contents

1. Introduction

This guide sets out procedures, actions, and configurations aimed at implementing the requirements laid down by AgID Circular No. 2/2017 of 18 April 2017, "**Minimum ICT Security Measures for Public Administrations** (Directive of the President of the Council of Ministers of 1 August 2015)" (Official Gazette, General Series No. 103 of 5 May 2017), by the General Data Protection Regulation (GDPR), as implemented in Italy by Legislative Decree No. 101/2018, by the recent **NIS2 Directive**, as transposed in Italy by Legislative Decree No. 138/2024, and, finally, by the **INFN Regulation on the Use of IT Resources.**

2. Recommendations for the use of Personal Devices

Holders of an administrative account on one or more personal devices may limit themselves to following the recommendations set out in this section. Individuals who have been formally appointed as “system administrators” shall implement all the measures established in this document.
For the purposes of this document, “personal devices” shall mean desktop or laptop computers assigned to users in the context of their work activities, on which no accounts of other users are present and on which confidential data are not stored on a continuous basis.
For such devices, the appointment of a system administrator by the Reference Director is not required.

Users of personal devices shall:

1. use operating systems that are currently supported and authorized by the relevant IT resources responsible team (see Section 4);
2. regularly apply operating system security updates (see Section 6.a);
3. ensure that operating system protection software (firewall, antimalware, etc.) is enabled and kept up to date (see Sections 9);
4. ensure that access to the operating system is protected by a strong password and is in any case compliant with the password policies adopted by INFN;
5. do not install software obtained from unofficial sources or repositories, for which an appropriate license is not held, or that is expressly prohibited by the relevant IT resources responsible team;
6. lock access to the system and/or configure automatic screen locking when leaving the workstation unattended;
7. do not click on links or attachments contained in suspicious emails and apply appropriate measures for malware protection (see Section 9);
8. connect only to mobile storage devices (USB drives, external hard disks, etc.) whose origin is known (new devices, previously used devices, or devices provided by the relevant IT resources responsible team);
9. configure disk encryption on laptops and desktops (see Section 11).

3. Responsibilities of the System Administrator

Procedures, actions and configurations aimed at implementing the requirements, limited to the minimum security level, shall be identified by the following keywords and enclosed within a box (in the case of measures required only for multi-user systems, the text background shall be grey):

IT IS MANDATORY,
MUST,
IT MUST BE.

It shall be the duty and responsibility of the system administrator to implement the measures so identified.
All indications not marked by the above-mentioned keywords are recommendations not explicitly required under the minimum security level set out in the Circular, but are nevertheless advised to improve system security.

4. Installation and Configuration of the Operating System

In order to use standard secure configurations for the protection of operating systems, it is recommended to coordinate the installation and configuration of MacOS operating systems with the relevant IT resources responsible team, in accordance with the procedures established by the team itself.

Systems that are preinstalled or whose configuration is not fully known, should not be connected to the network

Where physical access to the machine is not controlled, it is recommended to set up a password[1] to access the *Firmware* to forbid the boot from external devices and the access to the Recovery Console.

[1] Recovering a lost Firmware password requires the intervention of an Apple support centre (https://support.apple.com/it-it/HT204455)

a. Installation

If it is not possible to use a semi-automated installation system provided by the relevant IT resources responsible team, only installation images obtained from official Apple repositories via standard Recovery procedures, or directly provided by the relevant IT resources responsible team, **MUST** be used.

If preconfigured virtual images, containers, or Docker images are used, administrative credentials **MUST** be changed before connecting the system to the network.

Only supported and stable versions must be installed, avoiding the use of obsolete versions no longer supported by Apple.

Where it is necessary to keep non-upgradable systems in production, risk mitigation measures **MUST** be applied, such as isolating the device from the rest of the network.

It is recommended to periodically verify the operating system end-of-life (EOL) date through authoritative sources, such as the vendor's official website or online aggregators (e.g. https://endoflife.date/).

In the case of servers, it is recommended to perform a minimal operating system installation, avoiding the installation of software that is not strictly necessary for the operation of the services provided.

For servers providing centralized services, **IT IS MANDATORY** to compile and keep up to date an inventory of the required software and their respective versions.

In accordance with the provisions set out in the *INFN Regulation on the Use of IT Resources*, IP addresses **MUST** be assigned by the relevant IT resources responsible team, either directly or through DHCP servers

b. Configuration and first boot

The password of all administrative accounts

- MUST comply with the password policy adopted by INFN.

Any form of **root** login, including access via **SSH**, **MUST** be disabled.

To access the system remotely, only software that uses secure protocols **MUST** be used (e.g. SSH, SCP, screen sharing with encryption enabled).

Passwords that are trivial or based on dictionary words in any language must not be used.

To further improve operating system security, it is recommended to perform the following actions at first boot:

- disable Bluetooth and enable it only when necessary;
- control (prevent, restrict, and monitor) access to services and resources through firewall rules.

c. Filesystem sharing

Where it is necessary to share a filesystem, the following guidelines **shall** be followed:

- prevent **root** access (where possible) [2];
- mount the filesystem in read-only mode (where possible);
- always limit filesystem exposure to the strictly necessary clients;
- periodically review access status;
- where possible, filter access ports by allowing access only from authorized devices, using a firewall.

5. Remote access to the system

To access the system remotely, only software that uses secure protocols **MUST** be used (e.g. **SSH**, **SCP**, **RDP**, **VNC over TLS**).

MacOS allows remote management features to be enabled. Where required, these must be appropriately configured to prevent unauthorized access.

[2] This requirement is very stringent and generally impractical to implement; however, its feasibility should still be evaluated to enhance protection against ransomware (Reveton, CryptoLocker, WannaCry, …).

6. Maintenance

a. System Update

The system **MUST** be kept continuously up to date. All security patches **MUST** be applied as soon as they become available.
Automatic updates may be enabled through Apple's Automatic Updates service for software distributed through official channels. For additional software installed outside the App Store, manual mechanisms or centralized MDM-based systems must be used.

Where the use of automatic updates is deemed inappropriate, an alerting mechanism **MUST** nevertheless be in place. In such cases, **IT IS MANDATORY** to assign a priority level to vulnerability remediation actions based on the associated risk.

Following significant system changes (e.g. the addition of new services), **IT IS MANDATORY** to agree with the relevant IT resources responsible team on the execution of a security scan. Once the scan has been completed, all necessary actions **MUST** be taken to remediate identified vulnerabilities or to document accepted risks.

7. User management

Administrative privileges **MUST** be restricted to users who possess the appropriate competencies and an operational need to modify system configurations.

IT IS MANDATORY to maintain an inventory of all administrative accounts and ensure that each of them is formally authorized.

Administrative accounts **MUST** be used exclusively for operations requiring elevated privileges, and every access **MUST** be logged. For this purpose, **IT IS MANDATORY** to always use sudo.

A clear separation between privileged and non-privileged accounts **MUST** be ensured.

All accounts, particularly administrative ones, **MUST** be nominative and attributable to a single individual.

All accounts **MUST** be authorized in accordance with the *INFN Regulation on the Use of IT Resources.*

Starting from macOS El Capitan, all users with administrative privileges belong to the *sudoers* group and the *root* user account is disabled. In addition, a protection mechanism is enabled that prevents even users with root privileges from performing changes considered potentially harmful (*System Integrity Protection*).

It is nevertheless recommended, where possible, to distinguish administrative accounts from regular user accounts and to rely on the use of the sudo command in order to reduce the risk of executing operations that may be harmful to the system.

8. Management of Files Containing Critical or Institute-Relevant Data

Files containing data subject to specific confidentiality requirements or critical information (e.g. personal certificates, server certificates, SSH private keys, GPG keys) **MUST** be stored with permissions set to 600 (rw-------) or 400 (r--------).

9. Malware Protection

IT IS MANDATORY to install and properly configure integrated anti-malware systems (e.g. Microsoft EDR/XDR, Wazuh XDR).

IT IS MANDATORY to enable and configure the integrated firewall or an equivalent system.

IT IS MANDATORY to restrict the use of external devices exclusively to situations strictly necessary for work activities.

It is recommended to disable the automatic opening of email messages and the automatic preview of file contents.

10. Backup

IT IS MANDATORY to perform at least weekly backups of the information strictly necessary for full system recovery, for example by using Time Machine on **encrypted** external disks or network filesystems.

Where backups are stored on cloud services or where confidentiality cannot be ensured through physical protection, **IT IS MANDATORY** to encrypt backups before transmission and ensure that backup sites are not permanently accessible over the network.

11. Data Encryption

For laptops, the use of an encrypted filesystem (e.g. FileVault) is recommended and advisable also for desktop systems hosting confidential data.

The Institute's guidelines regarding the types of files that **MUST** be protected through encryption shall be complied with, ensuring that private keys are adequately protected.

12. System compromise

In the event of a system compromise, the relevant IT resources responsible team **MUST** be informed immediately.

System restoration **MUST** be carried out using images saved at the conclusion of the installation and configuration phase, or by performing a new installation.

13. Log Files

Periodic analysis of log files helps resolve security issues and system misconfigurations.
It is recommended to adjust logging levels and retention periods according to system criticality, within the limits defined by the Regulation.
Where possible, remote logging should be implemented.

14. Additional recommendation

- It is recommended to install software for monitoring the integrity of system files, in addition to the checks provided by the operating system.
- It is recommended to systematically assess compliance with the security policies and guidelines proposed by certification and standardization bodies (e.g. CIS, NIST, SANS, etc.).

It is prohibited to activate email systems.

The activation of web services **MUST** be authorized by the relevant IT resources responsible team.