Rules for the Use of Apple macOS Operating Systems

V 2.1 – 27/10/2025

Table of Contents

1. *Introduction* 2
2. *Recommendations for the use of Personal Devices* 3
3. *Responsibilities of the System Administrator* 4
4. *Installation and Configuration of the Operating System* 4
   a. Installation 5
   b. Configuration and first boot 5
   c. Filesystem sharing 6
5. *Remote access to the system* 6
6. *Maintenance* 7
   a. System Update 7
7. *User management* 7
8. *Management of Files Containing Critical or Institute-Relevant Data* 8
9. *Malware Protection* 8
10. *Backup* 9
11. *Data Encryption* 9
12. *System compromise* 9
13. *Log Files* 9
14. *Additional recommendation* 10

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.