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).