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**