Guidelines for Windows devices

v 1.3

Attuazione della Circolare AgID 18/04/2017, n. 2/2017
“Misure minime di sicurezza ICT per le pubbliche amministrazioni.
(Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)”
GU Serie Generale n.103 del 05-05-2017

Livello Minimo

Intro

This guide reports procedures, actions and configurations aiming to implement the requirements of AGID (*Agenzia per l'Italia Digitale*) guideline 18/04/2017, n. 2/2017 ("Minimum ICT security requirements for public administrations" (Prime Minister's directive August 1st 2015)", published in Italian–"*Gazzetta Ufficiale*" – General Series no 103 – 2017-05-05, for devices using Microsoft Windows operating system. We limit the analysis to minimum level of security required by the guideline, i.e. the minimal set of security measures that MUST be adopted by any public administration office.

Indications below reported aim to fulfil requirements expressed by AGID directive, not replacing, but rather integrating what is already indicated by *Commissione Calcolo e Reti (CCR)*:

Disciplinare per l'uso delle risorse informatiche–Regulation for the Use of INFN Information Technology Resources (CD 23/02/2007);

Carta della Sicurezza Informatica - Charter of IT security (CD 23/02/2007);

Windows base (20/12/2005)

Windows advanced (20/12/2005)

Servizi Centralizzati - Centralized services (20/12/2005)

Gestione Incidenti - Incident management (20/12/2005)

Sicurezza della LAN - LAN security (19/12/2005)

available here (some of them in Italian only):

- https://web.infn.it/CCR/index.php/it/sito-utenti-del-calcolo/sicurezza-informatica,
- https://web.infn.it/CCR/index.php/it/sito-utenti-del-calcolo/sicurezza-informatica/56-progetti-dei-gruppi-di-lavoro/documentazione-progetti/81-documenti-progetto-harmony

In particular this guide is an update and an extension of "Windows base (20/12/2005)" "Windows advanced (20/12/2005)" documents and, according with the guideline requirements, is addressed mainly to users having system administrator access level.

Guideline requirements related to minimum security level is reported in **Appendice A**.

Every single security measure will be referred with the related identifying number ABSC ID (Agid Basic Security Control(s) Id Number).

Systems administrator's duties

Procedures, actions and configurations targeted for implementation of AgID guideline, minimum level of security, will be indicated with the following keywords and included in a box (with a gray background in case of measures required by multiuser systems).

IT'S MANDATORY [IT] MUST/ [THEY] MUST, [IT] MUST NOT / [THEY] MUST NOT.

Fulfillment of these measures is a system administrators' duty. Duties listed in the paragraph **Users management** applies to multiuser systems only.

Measures not marked with above indicated keywords are suggestions to increase the security level, although not explicitly recommended by the minimum level of security of the Guideline.

Operating system installation and configuration

In order to protect operating systems with standard and secure configurations [ABSC ID 3.1.1, 3.2.1] the installation and configuration of Microsoft Windows operating system MUST be done in agreement with the "Computing Services" (CS) staff, following the methods and procedures they promote, beside those reported in this guide.

Preinstalled systems, and in general those whose configuration is not well known, should not be connected to the network.

When using virtual images or preconfigured, administrator credentials MUST be modified before network activation[ABSC ID 5.3.1].

If students, or other people not subject to INFN IT security policies, have free access to the area where the system is going to operate, it is suggested to

- Protect BIOS access with a password
- Disable from BIOS the boot choices from usb, floppy and CD .

Installation

When it's not possible to use a semi-automated installation procedure provided by CS, only images downloaded from *official* repositories, or images provided by the CS **MUST** be used. In both cases, image authenticity MUST be validated comparing image checksum with the one reported in the repository.

When the installation image is not provided by CS, it **MUST** be stored *offline* [ABSC ID 3.3.1].

Only stable and maintained versions have to be installed, avoiding test versions or versions no longer supported.

In case of a server running centralized services, **IT'S MANDATORY** to compile and keep updated a list of software used and related versions. [ABSC ID 2.1.1].

According with statements of "Disciplinare per l'uso delle risorse informatiche" - "Regulation for the Use of INFN Information Technology Resources" concerning network configurations, IP addresses MUST be assigned by CS, either statically or via dhcp.

Configuration and first boot

In order to enhance operating system security, it is suggested to perform these steps at first boot, possibly offline

Setup package signature check

Make sure that the OS package management system checks package signatures, such to reduce possibilities to install suspicious packages.

Uninstallation of unnecessary programs

In order to reduce the risks deriving from potentially vulnerable software, it is suggested to uninstall all the software programs that are not strictly needed by the operating system, services and tools used.

Password policy

Group Policies MUST be set, such that administrative credentials:

- Have adequate strength[ABSC ID 5.7.1],
- Are replaced with reasonable frequency [ABSC ID 5.7.3],
- Are not reused within a short period of time [ABSC ID 5.7.4].

Disable special accounts

When possible, **Administrator** account MUST be disabled. Another account without a meaningful username MUST be created for administrative purposes, to be used only if strictly needed (i.e, do NOT use: **root**, **amministratore, superuser**).

For Windows hosts managed via Active Directory Domain, it is suggested to assign a random password to the local administrative account; the host will be accessed with administrative rights via the privileged domain account created for each administrator.

Users access to services

Group policy allows to control (forbid, limit, log) access to services and resources

Network access to port and services

A proper firewall configuration allows to control (forbid, limit, log) access to specific network ports and services

File sharing

If own files or folders MUST be shared with other users, it is recommended at least to:

- Do **not** share **to everyone**
- Share rights MUST be granted strictly to the users it's meant to and only with the needed permission (i.e. read/write, read)

Remote access to the system

RDP (Remote Desktop Protocol) MUST be the only mean to access remotely the system. Users with RDP access right MUST be listed explicitly; it should be avoided to extend RDP access to everyone [ABSC ID 3.4.1].

First backup

When the installation and configuration is done, a full backup of the system MUST be performed, so that system can be recovered if compromised [ABSC ID 3.2.2]. This backup MUST be stored *offline* [ABSC ID 3.3.1], for instance on CD or DVD.

Specific software, as *clonezilla*, can be used on this purpose. For more info: https://www.pg.infn.it/servizio-di-calcolo-e-reti/misure-minime-di-sicurezza-agid/

For Active Directory Domain users, it's suggested to enable **roaming** profile.

Maintenance

System update

The Operating System MUST be kept constantly updated. In particular, Security patches MUST be applied as soon as they are released. [ABSC ID 4.8.2]. It's recommended to enable automatic updates both for operating system and installed software [ABSC ID 4.5.1].

If the system has critical services that could be potentially broken by automatic updates, those MUST be notified and performed interactively at the earliest opportunity. In this case priority MUST be assigned to the actions for vulnerability fixing according with the associated risk. In particular top priority MUST be given to patches fixing severe vulnerabilities. [ABSC ID 4.8.2].

If a known vulnerability cannot be fixed, the accepted risk MUST be documented [ABSC ID 4.7.1] and communicated to the CS.

If the system is subject to significant variations (i.e. new services added) IT'S MANDATORY to agree with the CS a security scan to highlight potential new vulnerabilities introduced [ABSC ID 4.1.1]. If the scan finds new vulnerabilities, actions MUST be taken to fix the vulnerabilities, or if not possible, the accepted risk MUST be documented [ABSC ID 4.7.1] and communicated to CS.

Accounts and credentials audit

Proper group policies MUST be set, in order to verify the adequate strength of administrative credentials (minimum length and complexity). Specific programs MUST be used to periodically check users account and passwords [ABSC ID 3.1.1, 3.2.1, 5.7.1].

Users management

Administration privileges MUST be granted only to users having adequate skills and that need, for operational purposes, to change systems' configuration [ABSC ID 5.5.1].

A registry of all administrative accounts must be maintained, ensuring that each of them is formally authorized [ABSC ID 5.2.1].

Administrative accounts **MUST** be used only for administrative, not-ordinary tasks. Any administrative access MUST be recorded. [ABSC ID 5.1.2].

Administrators' privileged credentials MUST be clearly distinguished from non-privileged ones, which MUST correspond to different credentials [ABSC ID 5.10.1]. In other words, if a user is also an administrator, he/she MUST have two accounts, but only one of them will be member of administrators group and will be enabled for administrative tasks.

All accounts, and administrative ones in particular, MUST be nominal and clearly associated to one physical person (no shared accounts)[ABSC ID 5.10.2].

Management of files with critical or relevant data

Access to files with particular requirement for privacy or confidentiality (data relevant for INFN) or containing critical information as personal certificates, server certificates, gpg keys…. MUST be limited to the owner only.

Malware prevention

Users **MUST** install an antivirus software [ABSC ID 8.1.1]. Automatic update of AV must be set, as well as automatic execution of anti-malware scan when a removable device is plugged in[ABSC ID 8.8.1].

IT'S MANDATORY to use a personal firewall, while antivirus IPS capabilities MUST be enabled

IT'S MANDATORY to limit usage of external devices, limiting their usage only when strictly required from operational needs [ABSC ID 8.3.1].

IT'S MANDATORY to disable automatic execution of contents from external devices in the moment they are connected [ABSC ID 8.7.1].

IT'S MANDATORY to disable automatic execution of dynamic content (macro) included in file [ABSC ID 8.7.2].

IT'S MANDATORY to disable automatic opening of e-mail messages [ABSC ID 8.7.3].

IT'S MANDATORY to disable automatic preview of file contents [ABSC ID 8.7.4].

Safety copies

IT'S MANDATORY to make, at least weekly, a backup of the "information strictly needed for a full restore of the system" [ABSC ID 10.1.1].

In case of backup on cloud, or when it's not possible to ensure the complete confidentiality of the information contained in the backup by proper physical protection of supports, **IT'S MANDATORY** to encrypt the backup before its transmission [ABSC ID 10.3.1], making sure also that it's not permanently accessible through the network, avoiding that attacks to the system will involve also its safety copies [ABSC ID 10.4.1][1].

Enhance data protection with cryptography

For laptops, it's suggested usage of encrypted filesystems, to prevent access to data in case of loss.

Encrypted filesystems are suggested also for those workstations with special privacy requirements.

Follow INFN indications on the kind of files that **MUST** be protected with encryption, making sure that encrypting keys are protected as well [ABSC ID: 13.1.1].

System compromission

If a system is compromised, CS MUST be contacted immediately, and recovery procedures MUST be agreed upon.

In any case, system recovery **MUST** be performed either from safety copies created when the system was installed and configured[2], or as a new installation[3] [ABSC ID 3.2.2].

1 La richiesta è volta a migliorare la protezione contro ransomware (Reveton, CryptoLocker, WannaCry, …).
2 See "First backup".
3 See Installation".

Log files

It can be useful to maintain and periodically analyze log files in order to spot security issues and wrong system configurations.

It is suggested to keep a copy of log messages, when possible, on a different machine.

Example of log files to be copied on a different machine:

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

APPENDICES

Please refer to the AgID web page https://www.agid.gov.it/en/security/Minimum-ICT-security-measures-for-public-administrations for the minimum ICT security policies for public administrations.