WORK@HOME AND BYOD

Issued by:

Security and Privacy

(Marco Azzarini) (Daniela Granata)

.....

Verified by:

Head of the Issuer

(Antonio Napoli)

.....

Approved by:

Security & Facility

(Antonio Napoli)

.....

RECORD OF VERSIONS		
Version	Date	Description of the changes introduced
01	09/11/2009	First Edition
02	14/06/2010	Added more precise references to mobile computing Inserted Chapter 4.2 Mobile Computing: Mobile Phones and Chapter 4.3 Mobile Computing: Digital Cameras More clearly described telework and how to do it
03	2017, 5th Sept	Renamed (former BPM-PS-0023) and internationalization Specified (Cap 4.4) using VPN. Specified (Chapter 4.2) using Bluetooth.
04	05 May 2020	Document critical review, following the introduction of regulation on Work@Home (Chapt. 4, 6, 7 and 8 - Par. 5.1)
05	22 April 2021	Document review following the introduction of BYOD

CONTENTS

1. AIM

The purpose of this document is to define:

- the rules that the employees of the Comdata Group (hereinafter the Company) must follow, in the workplace or elsewhere, to access via **corporate or personal devices** to the tools (applications, e-mail, network, documents, etc.) made available by the Company for professional purposes and
- the security requirements to protect the company data and information accessed through the aforementioned Devices.

2. DEFINITIONS

Comdata Group	Comdata S.p.A. and the Companies controlled directly and indirectly
Personal Devices	Smartphone, Tablet, PC, Laptop and any other employee-owned object through which it is possible to access Company tools, documents and applications
Remote PC	Personal or Company P C used outside the Company offices
Sharing Devices	Various software tools used to carry out communication and exchange of data and office documents and / or production support (e.g. shared areas, tools for video and tele-conferencing, tools for exchanging messages, etc.).
MFA	Multiple factor authentication, strong authentication, twe eyse authentication
MDM	Mobile Device Management
VAPT	Vulnerability Assessment e Penetration Test – vulnerabilities detection techniques
IDS/IPS	Intrusion prevention and detection systems

3. WORK@HOME AND BYOD

The **Work@Home** is a type of work that does not require the physical presence of the worker in the office or company and is facilitated by the use of ICT and telematic tools.

Bring Your Own Device - use your own device, refers to the use of personal devices, owned by the worker, to access the services and tools made available by the Company. The Work@Home can be carried out in the following ways:

- Use of devices owned by the worker (in which case we also speak of BYOD);
- Use of Company-owned devices.

The use of telecommuting tools and BYOD Devices is previously authorized by the Company.

Using the Work @ Home Devices, the Worker @ Home can connect (where necessary) to internal access channels to the Company's network or even to external access channels (via the Internet) in order to carry out its activity.

Workers@Home are assigned a company mailbox to exchange information with their colleagues.

3.1 PREREQUISITES FOR USING THE BYOD

It is a necessary condition for the use of BYOD, and it is the responsibility of the worker:

- Check that your Device is in the operating conditions provided by the manufacturer, in particular that it has not undergone any type of modification to the system software and hardware with respect to the configuration with which it was supplied by the vendor, with the exception of the updates provided by the manufacturer or provider and by the suppliers of the installed software and that it does not have any type of illegal software on board;
- Install and configure on your device, if required, the software indicated by the Company. This software must never be removed, modified or altered by the User, as long as the device is used in BYOD mode (eg install the "Google Device Policy" application on the phone according to the instructions received from the Information Systems Department);

- Install Antimalware software, if it is not already present on your device. This software must never be removed, modified or altered by the User, as long as the device is used in BYOD mode;
- If using a PC or Laptop, install/activate a Personal Firewall, if it is not already running on the Device;
- Always enable the native security features of the Personal Device, in particular the SIM PIN, the password to access the device, the data and peripheral encryption features.

The Devices are authenticated and access to Company services is allowed only for authorized Devices (by the Information Systems Management).

The Company guarantees that the data of the owner of the Device are never accessed in any way by the Company staff or by the software used by the Company.

4. BEHAVIORAL RULES

In order to raise awareness and train workers and Workers@Home not to compromise or expose information and data, they are given by the Company operational and behavioral instructions through information, training and documents on the topics of Information Security, Privacy and the correct use of equipment and data. .

In the case of Work@Home, workers and Workers@Home are also required to:

- Access the Company services and tools only with the methods and software provided (eg applications indicated by the Company), using their own credentials.
- To access Company services (even if carried out via browser) it is strictly forbidden to use non-proprietary Devices (eg smartphones of friends / acquaintances, workstations at Internet cafes, ...);
- In case of remote PC use, always turn off the Device connectivity kit (preferably also the whole PC) at the end of processing;
- In case of remote PC use, do not use and/or store the Device in common and/or condominium rooms, also to place the Device in a room in your home where the movement of people is minimal;
- If Company equipment is used, this is used only and exclusively for the performance of the assigned duties;
- In case of failure or malfunction of the instruments used, immediately notify the Company, so that the problem can be resolved promptly and without prejudice to the Company organization;
- Store with particular and relevant diligence the instruments eventually made available by the Company.
- Do everything possible to prevent unauthorized persons present in the place of work from accessing the personal data processed in carrying out the activities (for example, keeping the system screens that contain personal data out of the reach of their family members and guests) ;
- Do not record the data processed and / or conversations that took place by means of the electronic tools used in carrying out the work activities;
- Block the work session in the event of leaving the chosen working position, even for very short time intervals;
- Where not technically inhibited, limit the local saving of data to exceptional and very limited cases, taking care, once the need has ceased, to delete such data from local memory;
- In case of loss or theft of the Company or BYOD Devices used, promptly inform the Information Systems Management;
- Unless specifically authorized, do not connect to the company or personal instrument used to work removable media (eg USB keys);
- Do not install unauthorized and unnecessary software on the Company instrument for the provision of the service;
- Use of browsers considered adequate in case of access to the Company e-mail directly via the Internet;
- Do not use public connections (hot spots, hotels, etc) or private connections of strangers or strangers, even if protected, on Company Devices;
- The user is obliged to refuse consent to the installation of additional unauthorized software;
- When using public connections (eg Wi-Fi Hotspot) it is recommended to use the encrypted protocols;

- In order to avoid entry and violation of your Device by unauthorized persons, it is recommended to disable the network Wi-Fi communication channels (bluetooth and similar) and, if necessary, their use is made for the minimum time needed as possible;
- The Call or Video Conference Devices are used in the best possible way in order to prevent the shared conversations and documents from being exported, copied, disclosed or recorded in an unauthorized manner and it is forbidden to record the audit session, to copy and / or capture images (both video and audio); the ban is communicated and accepted by all participants.

5. SECURITY REQUIREMENTS

The Work@Home and the use of personal Devices:

- Exposes data and IT infrastructures to additional risk;
- The Company activates specific security measures to protect itself from this risk and from any attacks or malicious activities.

The following are the security requirements implemented by the Company's Information Systems Departments.

5.1 COMPANY AND PERSONAL (BYOD) MOBILE DEVICES

In cases in which Company or personal Mobile Devices (so-called BYOD) are used to access Company services and data (e.g. e-Mail, Work Space), compatibly with costs, the logical protection of the Device is realized by Information Systems Departments, also through the '' use of MDM tools, in the following ways:

- MDM software agent can be installed, if necessary, on the Devices;
- The Devices are registered in order to authenticate their use and verify access which is allowed and possible only for authenticated Devices;
- A logical space (Company user) is organized in the Device where only Company data are stored, so that it is ensured that the data of the owner of the Device are never accessed in any way by Company personnel or by the software used by it;
- Access to the network (and data) from the Devices takes place by typing the user credentials in such a way as to allow control of the network on the basis of data access privileges;
- An antimalware system is available on the Devices;
- Periodic updates of the Device software are performed;
- PIN access is activated, preferably by differentiating personal users from those used for professional purposes through different profiles, which must have adequately secure rights;
- It is possible to remotely manage company users and devices, including blocking in the event that they are considered dangerous (eg infected or compromised);
- It is possible to install and uninstall applications, even massively, remotely;
- It is possible to delete (excluding personal data in case of use of proprietary Devices) the data remotely (eg when the Device is lost, stolen or lost) to avoid data leakage;
- It is possible to remotely lock, activate or deactivate the Device systems such as the camera, the microphone and access the Device configuration;
- Applications can be selected, blocked, activated or deactivated remotely;
- It is possible to apply lock passwords to Devices remotely;
- The Devices make it possible to optionally identify the position (localization) of the Device following an evident authorization procedure.

5.2 COMPANY AND PERSONAL (BYOD) REMOTE PC

In cases where remote personal or Company PC are used (ie used outside the Company offices), they are equipped with only the software strictly necessary for the work activity (principle of "less is more" and "need to work") and are configured, by Information Systems, with the following controls (also guaranteed locally or by access channels):

- Access allowed only through the use of personal credentials (user-id, password) with activation of password policy;
- Market Antivirus active and correctly configured to secure versions;

- Activation of the Personal Firewall;
- Activation of the lockout policy in case of inactivity;
- Periodic software updates (operating systems and antivirus) through end-point-protection solutions;
- Impossibility of saving company data locally to the PC;
- Inability to access the internet in case of antivirus and patching disabled;
- Inability to modify proxies in browsers;
- In the case of a company PC, the inability of operators to install software;
- Use of storage encryption where possible.

5.3 SHARING DEVICES

The Device is requested / authorized by the direction of the user and validated (verified the sustainability) by Information Systems, possibly having consulted the Security function.
The Device can be made available both on the Intranet and on the Internet and is used in such a way as to constitute a closed circuit between the participants only, so as to avoid the disclosure of information and data outside the circuit.

The session owner (the one who convenes or holds the meeting) allocates the virtual meeting and authorizes access to the conference system - in order to verify and ensure only the presence of authorized participants.

5.4 TECHNICAL CONFIGURATION OF THE COMPANY NETWORK ACCESS CHANNELS

The access channels for Work@Home are designed, configured and managed by the Information Systems Department and allow remote workstations to have all the resources to carry out their work activities.

The services that allow access to the network and Company resources for Work@Home are organized in such a way as to allow access only to those who have the right and to minimize the possibility of data transfer to remote locations (including blocking the copy / paste).

Therefore, the encapsulation of sessions inside waterproof virtual machines (VDI) and the remote control of local networks (VLAN) are suitable solutions.

The access services are configured with the following functions:

- Access allowed to the entrance Device with individual credentials (user-id and password) of the Company domain in MFA;
- Management of access privileges to services and data in order to allow access to only the services and data necessary for the activity - Need to Know;
- Internet access filtered by proxy and controlled by whitelist;
- Access protocol with one-to-one connection, authenticated and encrypted;
- Time control to block access outside working hours;
- Geographical access control and related alarm.

In addition, security event monitoring (IDS/IPS) and vulnerability detection (VAPT) controls are implemented on these accesses.