Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

GROUP PROCEDURE FOR THE USE OF I.T. TOOLS, INTERNET AND E-MAILS

1. PURPOSE

The purpose of this Policy is to define the terms and conditions of use of I.T. Services by the users of Technoprobe S.p.A. and its Affiliates (hereinafter also called, collectively, Technoprobe or the "Group") in order to protect Technoprobe assets and avoid improper conduct that could expose Technoprobe or third parties to potential risks. Companies within the Group may issue more detailed SOPs in line with the guidelines set by this Group Policy.

2. DEFINITIONS AND ABBREVIATIONS

For the purpose of applying this Procedure, the definitions set out below shall have the following meanings:

a. **Contractor**: a third party cooperating with Technoprobe in any capacity and with any type of contract whatsoever (by way of example, but not limited to: technical consultancies, professional consultancies, etc.).

b. **Employee**: Technoprobe staff employed under any type of contract whatsoever (by way of example, but not limited to: temporary workers, project workers, trainees, interns, etc.).

c. **Policy**: this Policy concerning the use of I.T. tools, the Internet and e-mails.

d. **Device**: any computer (workstation or laptop) whatsoever, smartphone, tablet or other type of electronic device (including USB sticks, hard disks, smart cards or other data storage or data management systems).

e. **NDA**: a Non-Disclosure Agreement, i.e. a legal transaction for valuable consideration designating confidential information, whereby the parties thereto undertake to keep it secret, failing which there will be a breach of the agreement and specific penalty clauses and/or legal consequences arising from such breach.

f. **User**: Employee or Contractor specifically authorised by Technoprobe to gain access to

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

and use the I.T. Systems.

g. **I.T. Services**: Devices, networks, cloud services owned by Technoprobe and any other app that Technoprobe puts at its Users' disposal.

3. RESPONSIBILITY

The implementation of this Policy is overseen by Global I.T. department, which is assisted by the Data Protection Team or by local I.T. teams, where applicable. This procedure must be observed by all Users.

4. DESCRIPTION OF ACTIVITIES

4.1. INFORMATION AND DATA

For the purposes of this Policy, the term "**data**" is to be understood as the broadest set of information of which a User (employee, contractor, trainee, …) may become aware and must guarantee the confidentiality and secrecy, not only "personal data" as understood under the law.

As a general rule, any data (in the broadest sense of the term described above) of which Users become aware during the course of their work is to be considered confidential and must not be communicated or disclosed to anyone (even once the working relationship with Technoprobe itself has ended or if part of the information is in the public domain), unless otherwise specifically authorised by Technoprobe.

The utmost confidentiality must be observed even between colleagues, or between employees and external contractors, when disclosing known data, limiting such disclosure only to those cases in which it is necessary to do so for the purpose of carrying out the required work to the best of one's ability.

Technoprobe has adopted this Policy with a view to preventing unintentional conduct from giving rise to problems for, or threats to, the safety of Technoprobe's data and equipment.

Handling paper data, using Technoprobe Devices, as well as Internet and e-mail services, in a manner that infringes the rules set out in this Policy may expose Technoprobe and third parties to an increased threat of unauthorised access to data and/or I.T. systems, the theft or disclosure

of confidential information, as well as the theft of, or damage to, the said I.T. system and/or malfunctioning of the entire I.T. system in general.

4.1.1. Prohibition on using I.T. tools

Technoprobe assesses, at the beginning of the employment or consultancy relationship and thereafter from time to time, whether there are and continue to be the prerequisites for authorising Users to use the various Group Devices, the Internet and e-mails.

With a view to verifying the identity of all of the Users gaining access to the I.T. Systems and protecting the information to which they may have access, such Users must all be authenticated through a user account.

Unauthorised persons are explicitly prohibited from accessing Technoprobe 's I.T. tools.

4.1.2. Ownership of Devices and data

Technoprobe is the sole and exclusive owner and proprietor of the Devices that are delivered, for work-related reasons, to Employees and Contractors.

Technoprobe is the sole and exclusive owner and proprietor of all of the information, records and data contained in and/or processed by means of digital devices or stored in paper documents on the premises.

Users may not presume or believe that the information, records and data processed or stored by them in Technoprobe Devices (including e-mails and/or chat messages sent or received by them, picture files, animated image files or other types of files) are private or personal, nor may they presume that paper data in their possession may be copied, communicated or disseminated by them without Technoprobe's authorisation.

If a User becomes aware or suspects that someone has access to his or her account, he or she must inform the Global I.T. department so that his or her password is changed immediately.

Any attempt to deceive or manipulate for the purpose of gathering information, defrauding or gaining access to Technoprobe systems must be reported immediately to the relevant head of department, internal contact person, I.T. Systems manager and the legal department. A Security Incident will then be opened.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

4.1.3. Purposes for which Devices are used

Assigned Devices are working tools put at Users' disposal solely for work-related purposes. Devices must, therefore, not be used for private and non-business purposes, save for exceptional cases and within the limits outlined in this Procedure.

Any apparent or actual tolerance on Technoprobe's part does not, however, legitimise conduct that is contrary to the instructions set out in this Procedure.

4.1.4. Handing back Devices

After the User's employment or consulting relationship with Technoprobe has been terminated or, in any event, when Technoprobe makes the discretionary decision that the prerequisites for using the Group Devices are no longer met, Users shall:

- immediately hand back the Devices used by them in their current state;
- refrain altogether from deleting or formatting or tampering with or destroying the assigned Devices or rendering the data contained therein unintelligible by any procedure whatsoever, including data encryption;
- cf. paragraph 7.6 - Device Destruction.

4.2. PASSWORDS

Access to all of Technoprobe Devices is subject to manual personal identification (log-in) procedures, with the User entering a User ID and a Password.

Technoprobe's policy also stipulates that the system still requires authentication after a period of non-use of the Group's personal computer.

Each User is responsible for the safekeeping and use of his or her authentication credentials.

Each User is responsible for all of the activities carried out through the use of his or her User ID.

4.2.1. Rules for correctly handling passwords

The following rules must be explicitly observed by Users when managing their Password:

1. The password is strictly personal and may not be disclosed or communicated to third parties;

2. Storage: the password must not be written down or recorded on any (paper, electronic, etc.) medium;

3. Length: the longer the password, the more difficult it is to discover. The minimum length thereof is eight characters;

4. Characters: the password must contain at least one lowercase letter, one uppercase letter, one number and one special character (? | ! etc.), so as to increase the number of combinations (of the same length) and prevent brute force attacks;

5. Content: it is recommended that names of persons, places, companies, animals, products, car number plates, dates, words in the dictionary and other names or symbols that can be traced back to the user are avoided;

6. Period of validity: the more frequently the password is changed, the less likely it is to be discovered. The system will automatically request the password to be changed every 90 days;

7. Change: each password assigned or chosen by a User must be new and different from the previous one.

Each User may change his or her password used for gaining access to any corporate device or cloud services account either independently - in the event that the system in question puts such feature at its Users' disposal (Change password) - or by making a request to this effect.

In order to reduce the risk of password breaches and/or intrusions, access to a User's account is gained through the "two-factor verification" procedure:

Factor 1: User Name and Password;

Factor 2: every time a User logs in on a Device that is considered unreliable, he/she will receive a security code via e-mail, telephone or an authentication app.

4.2.2. Password audit

As part of the activities conducted by it with a view to guaranteeing the safety of its technological infrastructure, Technoprobe may carry out from time to time assessments of Users' passwords for the purpose of checking their soundness and compliance with the aforementioned operating rules.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

In the event that one of the possible findings of the audit is that the password has been decrypted, such password shall be blocked and the User shall be requested to change it. This finding could give rise to the disciplinary measures envisaged under the National Collective Employment Agreement adopted by Technoprobe or to claims for damages on account, and as a result, of the breach of contract in question.

4.3. ACTIONS TO BE TAKEN TO PROTECT THE WORKSTATION

Physical devices must be used and the data contained therein must be handled with a view to safeguarding the security and integrity of Technoprobe 's wealth of data.

Users must then perform the following steps:

1. lock their Devices (by simultaneously typing WIN+L) whenever they leave their workstation;
2. close the session (Logout) at the end of the day;
3. switch off Technoprobe personal computer after Logout;
4. ensure that there are no unauthorised persons behind them who can view the Device's screens.

4.4. USE OF TECHNOPROBE PERSONAL COMPUTER

4.4.1. Correct use of the Group COMPUTER

Each User is responsible for the use and safekeeping of the Personal Computer he/she has received and is required to comply with the rules set out in the following paragraphs and, in general, with this Procedure.

Users shall take the following steps:

1. keep the password through which access is gained to Technoprobe personal computer with the utmost diligence and not disclose it to third parties;
2. switch off the computer, or take care to Logout, every night before leaving the office or in case of prolonged absences, since leaving a computer unattended and connected to the network may lead to the use thereof by third parties, without there being any possibility of subsequently proving misuse thereof;

3. save, at the end of the day, the files that have been created, processed or modified in the centralised document repository system. Technoprobe does not back up data stored locally or data shared through corporate communication systems (e.g. Microsoft Teams);

4. use solely and exclusively the Group network memory areas, creating and recording files and software or data archives there, without creating, therefore, other files outside the network drives;

5. not allow third parties access to their computers, unless the latter are Users with whom they share the use of the same personal computer or unless strictly necessary and under constant control;

6. keep only those storage, communication or other devices (such as, by way of example, burners, modems, etc.) authorised by Technoprobe;

7. guard the personal computer assigned to them diligently, both while travelling and during the course of the normal use thereof.

4.4.2. Express prohibitions on the use of the Group's COMPUTER

Users are forbidden from:

1. using the Group personal computer for personal purposes or, in any event, for activities that are not work-related;

2. handling, storing (even temporarily) or processing personal or (in any event, non-work-related) files, documents and/or information in the Group network, hard disk or other mass storage device, as well as in any Group I.T. tool in general;

3. changing configurations that have already been set on the personal computer;

4. using programmes and/or encryption systems without Technoprobe's prior authorisation in writing;

5. installing software for which Technoprobe does not hold a licence, or installing any (even more recent) version other than the applications or operating system to be found on the personal computer that has been delivered to the User in question, without Technoprobe having explicitly authorised such User to do so; nor are Users allowed to make copies of the installed software for personal use;

6. uploading to the computer's hard disk or server any document, game, music or audio-visual file or image other than the ones required for performing the tasks entrusted to the User; in particular, Users cannot store electronic documents that are offensive and/or that discriminate on the basis of sex, language, religion, race, ethnic origin, political opinions and trade union and/or political affiliations;

7. adding or connecting hardware devices (e.g. hard disks, drivers, PCMCIA cards, etc.) or peripherals (cameras, smartphones, USB keys, etc.) other than those delivered to the User in question, without the latter having been explicitly authorised by Technoprobe to do so;

8. intentionally or negligently creating or disseminating, programmes likely to damage Technoprobe's or third parties' I.T. system, such as viruses, trojan horses, etc;

9. accessing, disclosing or using information that is unauthorised or otherwise not needed for the purpose of the duties performed by the User in question;

10. carrying out maintenance activities on their own;

11. allowing maintenance activities to be conducted by persons not explicitly authorised to do so by Technoprobe;

12. reproducing or duplicating computer programmes

The I.T. Systems Department staff can proceed at any time whatsoever to remove a file or app on a Users' computer or on network drives that they deem to be a Security risk.

System administrators can, for the purpose of Technoprobe needs, use their login (which grants them administrator privileges) and their administrator's password to gain access both to the local network mass storage memory (i.e. repositories and backups) and the Group's servers and they can, upon giving the employee prior notice, access the computer, even remotely.

4.5. INTERNET

4.5.1. The Internet is a work tool

Users can only connect to the Internet from the Device supplied to them for work-related reasons. In particular, the use of social networks is prohibited, unless they are explicitly authorised to do so.

4.5.2. Explicit prohibitions on using the Internet

1. Websites that may reveal the User's views on political, religious, trade union and health-related matters cannot be browsed, since this is potentially capable of revealing personal data

2. Access cannot be gained to websites whose content is unlawful, is contrary to public policy, is significant for the purpose of the commission of a criminal offence, or discriminates on the basis of race, ethnic origin, skin colour, religious belief, age, gender, citizenship, marital status, disability.

3. Users cannot download software (even free software) from websites.

4. Users are strictly forbidden from carrying out financial (including remote banking) transactions of any kind whatsoever or on-line purchases and the like, except in those situations in which they are directly authorised to do so and provided that this is done in observance of normal purchasing procedures.

5. Any form of registration on websites whose content is not work-related is prohibited.

6. Users cannot participate in non-professional forums, use chat lines or online noticeboards or take part in discussion groups or leave comments on articles or subscribe to mailing lists and use Technoprobe trademark or name, unless they have been specifically authorised to do so by the Group.

7. The storage of electronic documents that are insulting, defamatory and/or discriminate on the basis of sex, language, religion, race, ethnic origin, opinion and trade union and/or political affiliation is prohibited.

8. Promoting personal gain or profit through the use of the Group Internet or e-mails is prohibited.

9. Users cannot gain access from PCs other than Technoprobe PCs belonging to the Technoprobe internal network unless they have been specifically authorised to do so in accordance with the specific procedures laid down by the Group.

10. Finally, it is forbidden to create personal websites on Technoprobe systems or purchasing goods or services on the Internet unless the purchased item has been approved as a business expense.

11. Using the Internet for file sharing activities through unauthorised file sharing tools is prohibited.

4.5.3. Sabotage prohibitions

Users are forbidden from gaining access to certain websites by inhibiting filters, sabotaging or otherwise overcoming or attempting to overcome or disabling the systems adopted by Technoprobe for the purpose of blocking non-compliant access. In any case, Users are forbidden from using websites or other tools that achieve this end.

4.5.4. Copyright

Users are forbidden from gaining access to the Internet for the purpose of infringing current applicable copyright legislation. In particular, the downloading of material protected by copyright (texts, images, music, films, files in general) is prohibited unless explicitly authorised.

4.6. EMAILS

4.6.1. Emails are a work tool

Technoprobe e-mails must be used solely for work-related reasons. The use thereof for personal reasons is not permitted.

Users can use e-mail accounts belonging to the Technoprobe domains. The persons to whom individual accounts have been assigned are responsible for the proper use thereof.

Contractors must use their own e-mail account and not one belonging to Technoprobe domains, unless explicitly authorised in writing by Technoprobe to do so. In such case, authorised Contractors must comply with the rules of this Procedure.

Addresses containing names must, in any event, be considered as fully-fledged business addresses.

The choice of the e-mail account to be assigned to the User is made by Technoprobe.

4.6.2. Explicit prohibitions

1. Users are forbidden from using e-mail addresses containing Technoprobe's domain for the purpose of subscribing to any website for non-work-related reasons without having been explicitly authorised in writing to do so by Technoprobe, or to use Technoprobe's domain for personal reasons.

2. Users are forbidden from creating, filing or sending, even within the Group's corporate network, advertisements or promotional messages or in any case non-work-related attachments (films, images, music or other content), as well as participating in requests, petitions, mass mailings having contents of any kind whatsoever, "chain letters" or in general in public debates, and using the Group address therefor.

3. Users are forbidden from soliciting charitable donations, or sending election propaganda or other non-work-related items.

4. Users are forbidden from using the e-mail service to forward confidential information or in any case Technoprobe documents to persons outside the Group, unless this is done on account of the duties performed by them.

5. The use of a shared repository is recommended for emails to which large attachments are annexed. The use of a shared repository (if available) should always be preferred to e-mails.

6. In the case of unknown senders or unusual messages, Users should forward the communication/information to Technoprobe's Internal I.T. Systems, so as not to run the risk of being infected by viruses.

7. In the case of emails coming from known senders that contain suspicious attachments (i.e. files with the extension .exe .scr .pif .bat .cmd), such email should be forwarded to the Technoprobe internal I.T. Systems department/the Company's internal I.T. Systems Department must be informed thereof by e-mail and such emails should not be opened.

4.6.3. Termination of relationship

In the event of the relationship between Technoprobe and the User being terminated, the latter is forbidden from deleting e-mails sent and/or received through the account assigned to him/her, since such emails are Technoprobe assets.

In the event of the relationship between Technoprobe and the User being terminated, the account assigned to him/her may be kept active for a period of up to 12 months or terminated, even before the said 12-month term, depending on business needs.

4.6.4. Illegal use of Emails

1. Users are forbidden from sending, even within the Group network, e-mails containing

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

material whose contents are of a violent or sexual nature or in any case offend the principles of personal dignity, religious freedom, sexual freedom or freedom of thought, including political thought.

2. Users are forbidden from sending e-mails, even within the Group network, containing material whose contents are contrary to the law and to public policy, concern the commission of a criminal offence or discriminate in any way whatsoever on the basis of race, ethnic origin, skin colour, religious faith, age, sex, citizenship, marital status or disability.

3. If the User receives emails with such content, he/she shall delete them immediately and notify Technoprobe.

4.7. USE OF OTHER DEVICES (LAPTOPS, TABLETS, MOBILE PHONES, CELL PHONES AND OTHER ELECTRONIC DEVICES)

4.7.1. The use of laptops, tablets or smartphones

Technoprobe can grant the right to use laptops, tablets and cell phones (hereinafter called "Mobile Devices") to Users.

The User shall be responsible for the Mobile Devices assigned to him/her by Technoprobe and shall look after them diligently both when travelling and while using them in the workplace.

The rules of use for networked computers apply to Mobile Devices, with particular attention being paid not to remove any files processed on the Device before being handed back.

In particular, files created or modified on Mobile Devices must be transferred to Technoprobe 's mass storage devices when they are handed back to the office for the first time, or when the project is completed or the purpose for which the files are used is achieved, and they are deleted. Apps (even free ones) cannot be installed on Mobile Devices unless they are explicitly authorised by the Technoprobe I.T. Department. Mobile Devices used outside Technoprobe premises (i.e. in conferences, company visits, etc.) must be kept in a protected place in the event of removal. In the event of loss or theft of Mobile Devices, a report must be made to the competent authorities. For this purpose, Technoprobe must be notified immediately. Even during daytime and during working hours, the Users are not permitted to leave Mobile Devices unattended.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

Users are prohibited from leaving Mobile Devices unattended and in plain view inside their car or in a hotel room or hotel lobby or waiting rooms at railway stations and airports, under penalty of disciplinary sanctions or claims for damages.

Mobile Devices that allow a protection procedure (PIN) to be activated must always only be enabled by entering the PIN itself and cannot be left without a PIN.

In the event that the Mobile Device is accompanied by a user account, the Appointee is required to be informed in advance of the restrictions associated therewith (e.g. maximum number of minutes, total data gigabytes, ...) and to comply therewith.

4.7.2. External storage media (usb storage, hard disks, memory cards, cd-roms, dvds ...)

The use of external media is prohibited, unless explicitly authorised by the I.T. department, which will carry out the appropriate security assessments for Technoprobe.

In such explicitly authorised situations, the User may be assigned an external memory disk (such as a USB key, an external hard disk, a memory card, ...) on which to temporarily copy data for the purpose of easily moving it, or putting it to other uses (e.g. cameras with memory cards, video cameras with DVDs, ...).

These devices must be handled with the same level of care as the one described in the previous Article and must only be used by the persons to whom they have been entrusted and, under no circumstances, must they be handed over to third parties.

4.7.3. Personal Devices

The use of personal Devices (desktop PCs, laptops, ...) for business use is prohibited. Contractors are prohibited from using personal external memory disks (such as USB sticks, memory cards, CD-ROMs, DVDs, cameras, video cameras, tablets, ...).

The use of personal smartphones is only permitted under the conditions laid down in the Group and local internal rules, to which reference is explicitly made.

4.7.4. Use of personal mobile phone/smartphones.

During working hours, Employees are permitted to use their personal cell phones, but only for emergency communications or during times explicitly authorised by Technoprobe.

4.8. CLOUD SYSTEMS

Only cloud services that have been assessed and approved by Technoprobe may be used to store, transfer or otherwise process Technoprobe data.

Technoprobe provides useful platforms that allow its employees and third parties to cooperate with each other. Technoprobe also provides solutions to securely forward and/or share files occasionally with internal and external entities.

4.9. CHECKS AND CONTROLS

The Group and each of the companies of the Group, in order to properly protect their rights, reserve the right to carry out

checks and controls, even occasionally and appointing external service providers if needed, with the aim to:

- Prevent the commission of misconducts;
- Comply with any Authority order or provision of law;
- Pursue organizational or productive purposes, labor safety and protection of the Group's assets and rights;
- Protect IT resources security, keep integrity of the Group's data;
- Carry out control activities with regard to compliance with law or regulation provisions, including but not limited to, antitrust provisions, anti-corruption provisions, etc.;
- Carry out internal investgations aimed at enforcing or protecting Group's rights in Court, including pre-litigation reviews, and carry out the appropriate checks with regard to objections, claims, whistleblowing reports or orders received from Authorities or internal and external individuals or bodies.

The way in which such checks will be carried out will make sure that no unnecessary access to personal information will be made. The basis for processing personal data collected during such checks is the protection of legitimate rights or interests of the companies of the Group. For this reason, no consent will be needed from the relevant individuals.

Technoprobe S.p.A.
Via Cavalieri di Vittorio Veneto, 2
23870, Cernusco Lombardone (LC) - Italy
www.technoprobe.com

Controls will be carried out through con adequate technical instruments in line with national or international standards and best practices (e.g. keywords research); in particularly significant cases the Group reserves the right to carry out computer forensic activities.

The result of the mentioned checks and controls will be processed exclusively for pursuing the purposes listed above. Such data will be processed for the time necessary for carrying out the checks and controls and to check compliance with the law and with internal policies and procedures, and for protectiong the Group's rights, then will be safely kept for a time in line with applicable statute of limitations and then safely cancelled.

It should be noted that, in any event, Technoprobe does not adopt equipment designed, to control workers' activities at a distance (which certainly includes hardware and software aimed at controlling the Users).

DOCUMENT HISTORY

Revision 1.0 – Released on December 06, 2022

Approved by the BoD of Technoprobe SpA on December 06, 2022