CODE OF CONDUCT
Modalities for the correct use of company computer systems

The progressive diffusion of new information technologies exposes the Data Controller to risks of both financial and criminal involvement, while at the same time creating image and security problems. It is precisely for this last purpose that the company has already taken steps with reference, in particular, to the security measures imposed for the processing of personal data by European Regulation no. 679/2016 - General Data Protection Regulation (the so-called "GDPR") to give appropriate indications and instructions to all personnel concerned by these measures. Given that the use of the company's IT and telematic resources must always be inspired by the principles of diligence and fairness, attitudes which are intended to support any act or behaviour carried out within the scope of the employment relationship, it is deemed useful to adopt further internal rules of common conduct, aimed at avoiding unconscious and/or incorrect behaviour.

COMPANY COMPUTER SYSTEMS

The personal computer (fixed and mobile) and the related programs and/or applications entrusted to the employee are, as is well known, work tools, therefore:

- ✓ such instruments must be stored appropriately;
- ✓ such tools may only be used for professional purposes (in relation, of course, to the tasks assigned) and not for personal, let alone unlawful, purposes;
- ✓ theft of, damage to, or loss of such instruments must be reported promptly to the company.

For the purposes set out above, acts or behaviour in conflict with the aforementioned indications should therefore be avoided, such as, for example, those referred to below by way of example.

Personal computer usage

a) Access to the computer is using unique personalized credentials; do not write your password on the monitor or under the keyboard, do not divulge your password, recreate your password according to the criteria indicated when you are asked to change it (8 alphanumeric characters with at least one capital letter and one special character);
b) To avoid the danger of introducing computer viruses as well as altering the stability of the computer's applications, it is only permitted to install programs from outside if expressly authorized by the IT department;
c) The use of programs that are not officially distributed is not allowed (see, in this regard, the obligations imposed by Legislative Decree no. 518 of 29 December 1992 on the legal protection of software and by Law no. 248 of 18 August 2000, containing new regulations on the protection of copyright); all material that is not suitable for work activities will be uninstalled without notice;
d) You may not change the configurations set on your PC;
e) You may not install your means of communication (such as modems) on your PC;
f) On PCs equipped with a sound card and/or CD player, listening to programs, audio, or music files is not permitted, except for purely business purposes;
g) The printing of files is done via shared printers on the network, collect the printed data as quickly as possible.

Use of magnetic media

a) It is not permitted to download *files* contained on magnetic/optical media that are not relevant to one's job performance;
b) All *files* of uncertain or external origin, even if related to the work activity, must be checked and authorized for use by the Management or person delegated;
c) When transporting company data, files must be password-protected.

Using the corporate network

a) Network drives are strictly professional information sharing areas and cannot, in any way, be used for other purposes. Therefore, any *file* that is not work-related may not be located, even for short periods, in these units;
b) Network drives are for file exchange and are not backed up, always keep a copy on your PC in case of data loss, network drives have no "recycle bin" if you delete files they cannot be recovered;
c) Files must be copied to a specific folder, and not scattered in the main folder.
d) The company reserves the right to remove any *file* or application that it deems to be dangerous to the security of the system or acquired or installed in violation of this Code of Conduct.

Use of the Internet and related services

Internet browsing:

a) It is not permitted to browse on sites that are not relevant to the performance of assigned duties, especially those that may reveal the employee's political, religious, or trade union opinions;
b) No financial transactions of any kind, including *remote banking, on-line* purchases, and the like, may be carried out, except in cases directly authorized by management or its delegate and under normal purchasing procedures;
c) The downloading of *free software* (*freeware)* and *shareware* from internet sites is not permitted, unless expressly authorized by management or a delegated person;
d) Any form of registration on sites whose content is not work-related is prohibited;
e) Participation for non-professional reasons in *forums*, the use of *chat lines*, electronic noticeboards, and *guest book* registrations, even using *pseudonyms* (or *nicknames*), is not permitted;
f) The storage of computer documents of an insulting and/or discriminatory nature on grounds of sex, language, religion, race, ethnic origin, opinion and trade union, and/or political affiliation is not permitted.
g) You may use social networks and other tools to view educational and/or training material for purposes strictly related to the management of your work duties. You may not use the above tools for personal purposes.

Electronic mail:

While pointing out that **e-mail is** also **a working tool**, it is useful to note the following:

a) **It is not permitted to use electronic mail** (internal and external) **for reasons unrelated to the performance of assigned duties;**
b) It is not permitted to send or store messages (internal and external) of an insulting and/or discriminatory nature based on sex, language, religion, race, ethnic origin, opinion and trade union and/or political affiliation;
c) e-mail directed outside the company computer network can be intercepted by outsiders and, therefore, must not be used to send 'Strictly Confidential' work documents;
d) the use of the company e-mail address for participation in debates, forums, or mail-lists is not permitted unless explicitly authorized otherwise;
e) It should not be used to spread heavy files between internal mails (for this there are shared folders on the server);
f) **It is imperative to delete, without opening, e-mails that arrive from strangers (or unsolicited e-mails) containing unclear messages, especially if they have attachments;**
g) Never **under any circumstances open** attachments with the extension **.EXE, .PIF, .COM, .BAT, .SCR** and since recently **.ZIP that are suspicious**; first contact Information Systems, even if the e-mails come from known persons or e-mails;
h) **Do not click on ambiguous addresses or images in the text**, check in the bottom left corner, bypassing the mouse over the link without clicking, if the link is consistent with the text; in case of any doubt contact IT;

Since in the event of contractual and legal violations, both the company and the individual worker are potentially liable to sanctions, including criminal sanctions, the company will check, within the limits allowed by legal and contractual rules, compliance with the rules and the integrity of its computer system.

Failure to comply with this Code of Conduct may result in disciplinary, civil, and criminal sanctions.