

## ANNEX 2 TO THE CODE OF CONDUCT

### Requirements for the correct use of company computers and 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. And 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 COMPUTERS AND SYSTEMS

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

- ✓ IT hardware must be stored appropriately;
- ✓ Company IT 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 be avoided. The information below further details proper and improper usage of certain IT tools, which should be used as a guide rather than an exhaustive list.

#### Using a *personal computer*

- a) Access to the computer is by means of unique personalised credentials, which you need to protect from use by others at all times (i.e. do not write your password on the monitor, under the keyboard or on a readily findable piece of paper, do not divulge your password, use passwords in compliance with the criteria indicated when changing your password, etc.);
- b) To avoid the serious danger of introducing computer viruses as well as altering the stability of the computer's applications, it is only permitted to

- install programmes from outside if expressly authorised by the IT department and then only under the supervision of the IT outsourcer;
- 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);
  - d) All material that is not suitable for work activities will be uninstalled without notice;
  - e) You may not change the configurations set on your PC;
  - f) You may not install your own means of communication (such as modems) on your PC;
  - g) The printing of files is done via shared printers on the network, so 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 authorised for use by the Management or a delegated person;
- 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) Files must be copied to a specific folder and not scattered in the main folder;
- c) 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

- authorised by Management or its delegate and in accordance with normal purchasing procedures;
- c) The downloading of *free software (freeware)* and *shareware* from Internet sites is not permitted, unless expressly authorised 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 a work tool**, it is useful to note the following:

- a) **It is not permitted to use Company electronic mail 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 authorised otherwise;
- e) E-mail should not be used to send heavy files between internal users (for this, there is Teams and / or shared folders on the server);
- f) **It is imperative to delete, report and flag as potential phishing, spam or junk e-mails, without opening them, that arrive unsolicited from strangers, strange e-mail addresses, appear suspicious or 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-mail addresses;

- h) **Do not click on ambiguous addresses or images in the text**, check in the bottom left corner, by passing the mouse over the link without clicking, if the link is consistent with the text; in case of any doubt contact the IT outsourcer (support@alternitone.com).

### **Use of Artificial Intelligence (“AI”) tools**

The Plenisfer recognises the strategic importance of generative AI systems and is committed to ensuring their ethical, responsible, fair and transparent use, in line with its core values and current legislation (e.g. EU Regulation 2024/1689, Law no. 132 dated 23<sup>rd</sup> September 2025, EU Regulation 2016/679, provisions on copyright and intellectual property). In particular, the use of such systems must be carried out in compliance with the principles of confidentiality and personal data protection. The use of AI systems must generate tangible business benefits, avoid harm related to inclusivity and sustainable growth.

Therefore, your use of AI applications, agents, tools or the like (“AI Tools”) must be in line with the following:

- a) You are responsible for your use of AI Tools and you must expressly validate any output generated by AI Tools as AI Tools are not authoritative sources;
- b) It is not permitted to use AI Tools for regulatory filings, legal documentation output, sensitive financial calculations or other formal or strategic output without thorough review and validation by the user;
- c) It is not permitted to use company provided AI Tools for non-business purposes including but not limited to generating any insulting and/or discriminatory nature based on sex, language, religion, race, ethnic origin, opinion and trade union and/or political affiliation;
- d) It is not permitted to expose Confidential or Sensitive Company documents or data to non-secure AI Tools;
- e) It is required to disclose the use of AI Tools in any output;
- f) You must validate and take personal responsibility for any output where you used AI Tools in the output generation.

\*\*\*

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 / or criminal sanctions.***