#wearelogistics

# Policy for the use of technological resources

**January 2023**

BERGÉ
Moved by Logistics

# CONTENTS

# 1. Purpose and aim

The purpose of this Policy for the Use of Technological Resources (hereinafter the "Policy") is to ensure that all professionals of BERGÉ Infraestructuras y Servicios Logísticos, S.L. and its subsidiaries make an appropriate, responsible and lawful use of the technological resources at their disposal, and act in accordance with the principles and guidelines established in the Code of Conduct and the rest of BERGÉ's internal policies and procedures.

This Policy is compatible with and complements the other internal policies, guidelines and procedures issued by the Cybersecurity Committee and the GRC Department.

This Policy pursues the following aims:

I. Promoting the use of technological resources aimed at meeting the productive needs of BERGÉ, ensuring productivity through the use of work time.

II. Allowing BERGÉ to exercise due control in an attempt to prevent the use of technological resources to engage in the following prohibited conducts:

- Harassment or discrimination.
- Disclosure of confidential information or non-compliance with data protection regulations.
- Attempting against the company's security and its tangible and intangible assets (property, intellectual and industrial property rights, underlying business, reputation, good image, etc.).
- Putting at risk the security and stability of computer equipment, systems, or the information contained therein.
- Acts of unfair competition against the Company.
- Infringing other rights of the company or third parties.
- Breaching the contracts or relationships established between BERGÉ and its employees or third parties.
- Transmission, distribution, storage, downloading, installation, copying, viewing, sending or receiving of any kind of offensive or discriminatory content especially if its possession or use constitutes an illegal action: this includes, without limitation, all material protected by copyright, trademarks, distinctive signs, trade secrets or other intellectual or industrial property rights used without proper authorisation.
- Attempting against the honour and good image of the company, its employees or third parties.
- Any other conduct contrary to the legal system (including criminal, administrative, civil, etc.), to this standard or other regulations in force within the Company.

III. Allowing the company to exercise its right and duty to verify the correct fulfilment of the obligations of employees and allowing the company, in the event of detecting that the technological resources have been used improperly, the company may put an end to the prohibited conducts and sanction the users who have incurred them.

## 2. Scope and enforceability

This Policy is addressed to all professionals of BERGÉ Infraestructuras y Servicios Logísticos, S.L. and its subsidiaries (hereinafter "BERGÉ").

Subsidiaries shall be understood as companies in which BERGÉ Infraestructuras y Servicios Logísticos, S.L. holds a stake in the share capital that allows it to have control, pursuant to the provisions of Article 42 of the Commercial Code.

The Policy constitutes an internal rule of mandatory compliance for all BERGÉ professionals, regardless of their geographical, hierarchical or functional location, and the contractual modality that determines their relation with BERGÉ.

No general exceptions to the application of the Policy will be approved. If a specific exception is required for justified reasons, prior authorisation from the GRC Department will be required.

# 3. Definitions

For purposes of this Policy, the term "user" or "users" includes all BERGÉ professionals regardless of their geographic, hierarchical or functional location, and of the contractual modality that determines their relationship with BERGÉ, external collaborators, if any, and in general, any person authorised to use BERGÉ's Technological Resources.

For purposes of this Policy, the Technological Resources made available to users shall mean:

- computer equipment, application servers, remote access terminals, desktops or laptops, and similar or equivalent devices,
- any application or software program, networks and systems,
- internet, Intranet, email, on-premises file storage and sharing services, locally or in the cloud, and instant messaging.
- accounts that provide access to the use of *hardware, software* and information systems,
- landlines, mobile phones, smartphones, tablets, etc.
- electronic certificates,
- any other element or technological innovation that the company may acquire.

The Technological Resources available to BERGÉ are production tools at the service of the company's business, so that users can exercise their duties to develop the company's business. This, and no other, is BERGÉ's purpose to make such resources available to users. Therefore, BERGÉ must control the use of the Technological Resources insofar as they are production tools and through them the professional performance of the user is fulfilled, in order to check whether their use is adjusted to the purposes that justify them.

BERGÉ's Technological Resources are an important asset insofar as they allow it to work efficiently and productively, but an inappropriate use of them can generate damages for the company that can become extremely serious, including criminal liabilities for the company itself.

# 4. Instructions for use of Technological Resources

## 1. General instructions for use of all Technological Resources

**1.1.** BERGÉ grants users access to its Technological Resources, and the ability to view or modify the information they process and store. The different permissions for access to the media, networks, systems, and the information itself, will be granted after a formal approval process that will ensure that each user has access, only, to the resources and information required for the performance of their duties.

**1.2.** Each user shall keep due care of the Technological Resources that are assigned thereto, preventing the access of other people to work tools and to the login credentials (User and password) that have been assigned thereto for their use. In accordance with the foregoing, users must not access the resources assigned to other users, unless expressly authorised by the Legal Department Manager and due to company requirements.

**1.3.** **General rule for the use of technological resources:** Technological Resources means the company's working tools. The use of the resources must therefore be intended to fulfil the duties assigned to users within their contractual relationship with BERGÉ, and must be used in appropriately in accordance to its nature and professional purposes.

**1.4.** **Prohibitions of use:** any use of the Technological Resources in violation of the employment contract and current legislation is expressly prohibited, so is any use that is contrary to the principles and provisions of this Policy, the BERGÉ Code of Conduct and other internal policies and procedures.

**1.5.** **The technological resources are those approved by BERGÉ.** The use of media or technological environments not approved by BERGÉ to store the organisation's information is discouraged. In particular, free and open source tools, since the use of this type of tools usually results in the loss of control and decision making over the information stored in them.

**1.6.** **Warning on the company's control of the use of the Technological Resources:** the Technological Resources are work tools made available to the users by BERGÉ for the performance of their professional duties and therefore may not be used to transmit, distribute, store, download, install, copy, view or send contents unrelated to the development of BERGÉ's professional activity. Although the Company is aware that corporate uses imply that occasionally a personal use of the Technological Resources may occur even if they are the company's, users are warned of the following issues of extreme relevance:

- Pursuant to Art. 20.3 of the Workers' Statute, BERGÉ has the right to monitor and control that the work tools are used without incurring in the prohibited uses described in this Policy and in the rest of BERGÉ's internal procedures and rules.
- Pursuant to Article 31 bis of the Criminal Code, BERGÉ has the duty to monitor and control that no criminal offences take place within the company.

- The aforementioned right and duty imply that BERGÉ's monitoring and control of the use of the Technological Resources is necessary and unavoidable.
- BERGÉ admits a private use, provided that it is moderate and occasional, of the Technological Resources for the needs of users other than those for the performance of their professional activity for the company. Such private use may never be for other user professional activities.
- Users are aware of the existence of company monitoring and control measures on the use of Technological Resources.
- Users are aware that, since the right and duty of surveillance and control by BERGÉ of the use of the Technological Resources is necessary and unavoidable, such use is subject to possible control and therefore there are no expectations of privacy, confidentiality and secrecy of communications even when they are making a use other than professional.
- BERGÉ may inform workers, at any time, that the personal use detected is considered excessive and it may instruct them to limit, moderate or even cease such activity. Users understand that the company may, in the event of detected use or storage of personal information, warn or even directly remove such personal information from the Technological Resources. At no time will the company be forced to give support or provide security to such information or personal use.

**1.7.** The following table details, by way of example, the uses of the company's Technological Resources for personal purposes considered reasonable and uses considered excessive and therefore prohibited:

| | WORKING HOUR | |
|---|---|---|
| | **DURING** | **OUT** |
| **Reasonable / sporadic use** | Buying cinema tickets | **Those considered reasonable during working hours, even if with more continuous use.** |
| | Checking the weather, traffic, stock exchange<br>Occasional online purchases.<br>Online Press<br>Use of National ID (DNI) or other personal certificates.<br>Instant messaging: SKYPE, WhatsApp, Hangouts, etc.<br>Watching non-leisure videos.<br>Personal Banking.<br>Social Media | + Continued Use of Social Media<br>+ Games<br>+ Viewing leisure videos (series, films, etc.) from a connection without additional charge, for example WIFI. |
| **Excessive / prohibited use** | **Those considered reasonable during working hours but making an excessive use thereof.**<br>+ Use of WhatsApp as work support (orders, response to complaints, etc.)<br>+ Watching films/series<br>+ Continued Use of Social Media<br>+ Viewing leisure videos<br>+ Games<br>+ Sending personal data to the company via WhatsApp<br>+ Redirecting from the email inbox: complete or selected sensitive content. | **Any business activity or that generates any economic benefit to the employee**<br>+ Sending personal data to the company via WhatsApp |

The examples mentioned above are conditional on the particular requirements of each job post.

Additional specific standards on the use of certain media are set out in Annex I. This Annex forms an integral part of this standard.

**1.8.** In line with the risk assessment conducted in the project to adapt to the European Personal Data Protection Regulation (GDPR), the company's Technological Resources should not store files containing the following types of information:

- Data on ideology, union membership, religion, beliefs, racial origin, health or sex life.
- Data collected for law enforcement purposes without the consent of the persons concerned.
- Data derived from acts of gender violence.

## 2. Intellectual and Industrial Property

**2.1.** The information or contents disseminated or disclosed on the Internet or in other media are protected by intellectual and industrial property laws, both national and international.

**2.2.** The company complies with these laws, so to avoid liability to the detriment of the company, users should check, before using such information or content, if they can effectively make use of such information in accordance with the laws and licenses and authorisations obtained by the company. In case of doubt, the user will avoid its use or will contact the BERGÉ systems department manager to confirm whether or not the use of such information or content complies with current legislation.

**2.3.** Sending emails or communications over the Internet may cause the information to become known to the general public. This dissemination could preclude or prejudice the protection of the company's intellectual or industrial property. Therefore, when sending emails or accessing the Internet, users should not reveal any information about the intellectual or industrial property of the company, unless it is public or qualified as public use by the company, except for users who have among their duties the management and advice of industrial and intellectual property matters.

## 3. Power to monitor the proper use of Technological Resources:

**3.1.** A user's infringement of any standard in these regulations can cause very significant damage to the company and even lead to incur in criminal wrongdoing and constitutes a breach by the user of their contractual obligations. In such a situation, BERGÉ shall be entitled both to demand that users immediately cease their actions and to adopt disciplinary and other actions in accordance with the applicable regulations, in particular those provided for in the labour regulations, including suspension from duties without pay, and dismissal in cases where the seriousness of the conduct makes it advisable.

**3.2.** BERGÉ may access and control all the Technological Resources and their use, always in accordance with the Law applicable at all times, for the following purposes:

- Being able to prove that due control has been exercised.
- Checking the application by the users of the measures and procedures of use and security established by the Policy.
- Imposing penalties or requesting workers and other users to engage in prohibited conducts.
- Accrediting such behaviours before the judicial bodies or other authorities.

## 4. Control measures and methods practised by BERGÉ:

**4.1.** Orderly storage and search systems of the behaviours prohibited in this Policy on corporate email systems, applications and file storage and sharing both locally and in the "cloud".

**4.2.** Such storage will be maintained for the duration of the professional relationship between the user and BERGÉ and up to a maximum of 10 years after the end of the relationship, or for the legally established period, given that the content may be essential for the company's activity, maintaining the relationship with customers and other operators in the market, meeting the company's responsibilities and conducting the controls described.

**4.3.** In the event that BERGÉ has indications that lead it to reasonably suspect that a user or users have disregarded the provisions of the Policy or have engaged in conduct that is prohibited by current legislation or BERGÉ's internal regulations, the GRC Department, shall conduct, with technical support, specific accesses to the Technological Resources used by the user or users in question in a specific manner with respect to said user or users.

**4.4.** The control measures will be adapted to the characteristics of each Technological Resource as detailed below.

**4.5.** Access to the information contained in the computer equipment:

- Access shall consist in detecting through an automatic search whether illegal software or software that has not been authorised by BERGÉ is stored on the computer equipment.
- Access will also consist in conducting automatic searches for free terms that could reveal misconduct such as harassment, discrimination, unfair competition, disclosure of secrets, etc.
- Should the automatic searches result in improper material being used or stored in the computer equipment, the GRC Department will inform the Company Management and the HR Department, who will decide on the actions to take.

**4.6.** Access to email boxes and to the information contained in the emails:

Access will consist in conducting automatic searches for free terms that could reveal misconduct such as harassment, discrimination, unfair competition, disclosure of secrets, etc.

- Should the automatic searches result in improper material being used or stored in the computer equipment, the GRC Department will inform the Company Management and the HR Department, who will decide on the actions to take.

- In relation to the emails sent or received via the company's email server and other channels likely to contain information, a full backup copy of all elements will be stored to prevent the loss of the information contained therein. This backup copy will be used both for the due attention of relations with the clients, suppliers, public authorities, administration and employees of the company, and for controlling compliance by users of the instructions established in this Policy.

**4.7.** Access to the use of Internet and the Intranet by users:

- Automatic access to web page data opened by the user in order to detect contents unrelated to the Company's activity and the time spent by the user to browse through this type of pages.
- Access will consist in seeking free terms that could reveal misconduct such as harassment, discrimination, unfair competition, disclosure of secrets, etc.
- Should the automatic searches result in improper material being used or stored in the computer equipment, the GRC Department will inform the Company Management and the HR Department, who will decide on the actions to take.

**4.8.** Access to other Technological Resources: the criteria and rules set forth above shall apply analogously to the rest of the Technological Resources made available to users.

**4.9.** In order to secure digital evidence that might otherwise be destroyed or to protect the confidentiality of the company's proprietary information, BERGÉ may remove the user from the technological resources assigned thereto at any time and without prior notice, and the user must immediately make them available to the company. These control measures will be conducted by the GRC Department, in collaboration with the Legal Department and the Information Systems Department.

## 5. Ending the relationship with the user

**5.1.** The transfer of the use of the Technological Resources to the users for the performance of their professional service will only be maintained for the duration of the relationship with the Company.

**5.2.** Access to the Technological Resources shall be denied from the time the relationship established between the user and BERGÉ comes to an end whatever the reason.

**5.3.** The foregoing provision may be applied in the event of opening contradictory proceedings due to the commission of a fault by a user who is an employee of BERGÉ, when so advised given the nature of the fault.

**5.4.** Should the relationship come to an end, the user must hand over the Technological Resources in its possession in accordance with the internal procedures established for this purpose.

# 5. Communication and dissemination

The full text of the Policy shall be made available to all BERGÉ professionals, all of whom shall be obliged to its strict compliance, and shall be the subject of communication, training and awareness-raising actions for its timely understanding and application.

The Policy will be available through the corporate Intranet.

# 7. Approval and review

The Policy approved by the BERGÉ Board of Directors on 25 January 2023, is incorporated into the internal regulations and may be reviewed and/or modified to adapt to the needs resulting from applicable regulations, technological progress, and other relevant changes in the organisation.

The updating of successive versions of the Policy and/or other documents required to comply with the policy's provisions shall be the responsibility of the GRC Department.

# Annex I Specific instructions regarding technological resources

## 1. Specific instructions for computer equipment and software:

**1.1.** Computer equipment (or *hardware*) means the set of physical or material elements that make up an information system, such as computers, printers, screens, etc., while the software is the set of logical elements of an information system, such as applications, programs, operating system, databases, etc.

**1.2.** Acquisition of computer equipment and software: computer equipment, applications and programs that BERGÉ owns or holds the right to use, will be contracted according to the procedures in force in the company.

**1.3.** Installation and maintenance of computer equipment: Users may not make any changes, handling or modifications without the express authorisation of the BERGÉ Information Systems Department. All new computer equipment must be installed through the resources, companies or computer equipment determined by the BERGÉ systems department manager, and installing any additional hardware without their authorisation is prohibited. Any type of maintenance other than that set out in the Recommendations Annex must be consulted and approved by the BERGÉ Information Systems Department Manager.

**1.4.** Use of passwords to access computer equipment and, in general, Technological Resources that require access passwords: compliance with the provisions of the password policy issued by the BERGÉ Cybersecurity Committee is required.

**1.5.** Software installation: each computer will have installed the applications and programs required to enable the proper performance of the duties of the users for whom they are intended. Users must justify their requests for installation of new software, which must be approved by BERGÉ's Information Systems Department. In addition to the generally prohibited behaviours in this Policy, it is prohibited to:

- -install, without authorisation from BERGÉ's Information Systems Department, any software or computer application on the user's own initiative.
- -access or use unlicensed or "pirate" software (unlawful conduct that entails serious criminal and civil liability, as well as obviously putting at risk both computer equipment and the information they contain).
- -install digital certificates in the computer equipment that can be used to represent the company, without following the internal procedure defined for this purpose.

## 2. Specific instructions for portable devices:

**2.1.** Portable devices means laptops, PDAs, mobile phones, CDs, DVDs, Blue Ray, USB sticks, memory cards, and so on. Users shall use the security mechanisms provided by the company to prevent the theft or loss of the devices and/or the information they house, and shall comply with the manufacturer's instructions and with the policies and guidelines issued by the BERGÉ Cybersecurity committee.

**2.2.** At BERGÉ facilities one must work with the resources owned by BERGÉ. When external resources are introduced in its facilities, it should be taken into account that, in order to protect these assets, such computer equipment may be registered, although in this case respecting the provisions of Article 18 of the Workers' Statute concerning the registers on workers' particular belongings and other applicable regulations.

## 3. Instructions applicable to Email users:

**3.1.** The correct use of the email service implies that the user must not use it for actions that are prohibited in this Policy and in the legal system, including, for example, the following:

- Infringing the company's Data Protection Security Policies laid down in the Data Governance Policies issued by the BERGÉ Cybersecurity Committee.
- Simulating belonging to a company other than BERGÉ or another related company.
- Initiating or participating in the propagation of chain letters or similar actions.
- Using private mailboxes offered by any Internet supplier for professional purposes related to the company.
- Use email as a communication tool for sales or other commercial purposes alien to the company.
- Sending or requesting messages, files or materials with content of an explicitly sexual nature, of a discriminatory nature, which may be offensive, defamatory, threatening or insulting to any person.

**3.2.** Only BERGÉ's Legal Department may authorise redirecting emails for company needs. In general, other users are not allowed to automatically redirect complete mailboxes or selected sensitive content received in corporate email accounts to non-corporate email accounts and vice versa. Users who need to redirect must request authorisation from the BERGÉ legal department manager. Once the redirection is authorised, the Information Systems department will execute the redirection through its suppliers and specialists.

**3.3.** System administrators must request prior authorisation from the Legal Department if they need to access personal data or execute automated procedures (e.g. E-discovery) that also result in accessing or processing the personal data of users.

**3.4.** In the specific case of an employee deregistering from BERGÉ's information systems, his/her mailbox and information files will remain blocked and without access. Exceptionally, and provided that the employee gives his or her written consent with the authorisation of

BERGÉ's Legal Department Manager, another employee may be requested to redirect or access such information.

**3.5.** In order to prevent the degradation of the mail service and the involuntary saturation of user Mailboxes, the volume of documents, files, etc., that are attached to an email must never exceed the maximum size authorised by the BERGÉ systems department manager. If for business reasons it is necessary to annex a volume greater than that allowed, users must request authorisation from the BERGÉ systems department manager.

## 4. Specific instructions for use relating to the Internet:

**4.1.** BERGÉ shall provide users with access to the Internet according to the responsibilities or tasks assigned to them.

**4.2.** Users are responsible for the material viewed and download from the Internet. Therefore, you must make responsible and lawful use of Internet access and the websites you access from your post.

**4.3.** It is strictly prohibited to use the Internet for the prohibited conducts described in this Policy and in the rest of the legal system. This includes among others, by way of example:

- Accessing, speaking or writing in social media, forums, chats or similar applications, unless there is a direct and provable relationship with the performance of the duties.
- Downloading and / or installing on computers software, executable files or databases from the Internet. Users who need this to perform their duties must request authorisation from BERGÉ's Information Systems Department.
- Using software to download or exchange files or Peer to Peer files or any other software to download music, films, videos and / or games or multimedia playback services for leisure purposes.
- Sending emails of a professional nature or related to BERGÉ's business activity from the user's private email addresses (Hotmail, Gmail or other accounts).

**4.4.** Access to the Internet or any other computer network must be made through the connections permitted, enabled and configured by the technical specialist companies chosen by the BEERGÉ Information Systems Department Manager. Any other different connection will jeopardise the security of the company's information systems and is therefore strictly prohibited.

## 5. Specific instructions for use relating to access to the systems through the network:

**5.1.** The use of the company's data networks must be governed by the correct use of the resources that compose them, the following activities being expressly prohibited, in addition to those generally prohibited in this Policy:

- Attempt to access, read, delete, copy or modify the files of other users without the knowledge and consent of its author, or as the case may be, of the Company.
- Attempt to access restricted areas of the company's computer systems, its other users or third parties.
- Destroy, alter, disable or damage the data, programs or electronic documents of the company, its other users, or third parties.
- Attempt to increase the level of privileges of a user in the system.
- Attempt to decrypt passwords, systems, encryption algorithms or any other security element involved in the company's telematic processes.
- Voluntarily obstruct other users' access to the company's computer equipment and systems, due to the massive consumption of computer and telematic resources, and conduct actions that damage, interrupt or generate errors in said computer equipment and systems.
- Introduce programs, viruses, macros, applets, ActiveX controls or any other logical device or sequence of characters that cause or are likely to cause any alteration in computer resources.
- Introduce, reproduce or distribute computer programs not expressly authorised by the company, or any other type of work or material whose intellectual or industrial property rights belong to third parties.
- Make the computer equipment and software supplied by the company available to unauthorised third parties.

**5.2.** Users must use corporate antivirus programs and updates thereof on their computer in order to prevent material downloaded from the Internet or provided by a third party from destroying or corrupting computer data.