VANGEST

Information Technology Usage Policy

INDEX

Information Technology Usage Policy

1. Introduction

Any company that is part of "Vangest"— a group consisting of all commercial entities whose share capital and/or voting rights are, at all times, predominantly held by Vangest, S.A. (hereinafter referred to individually as the "Company")—provides access to a wide range of tools for work, which include, among others, equipment and software.

This provision is made so that the Company's employees can perform the functions entrusted to them by the Company, to the extent required by each of these functions. However, these tools operate in an integrated manner, making it essential to establish rules and procedures for their assignment, use, and cessation of use.

This policy has therefore been designed to assist the Employee in understanding the rules that must be followed by all Employees. All references in this policy to information technology should be construed as encompassing:

The Intranet and the Internet (including, in particular, social network sites) and email—"Networks";

Software that is owned by or licensed to the Company (regardless of whether it is integrated into the Company's Equipment or operates under a SaaS model—Software as a Service)—"Software";

Computers, tablets, mobile phones, and any other mobile devices, technology, or equipment that may arise from time to time and is owned or controlled by the Company, and whose access or use is granted to the Employee—"Equipment".

(together, Networks, Software, and Equipment hereinafter referred to as "IT").

2. Scope of Application

This policy applies to:

- Employees (including employees, temporary workers, and interns)—"Employees";
- Service Providers or collaborators from companies providing services to the Company who are granted access to IT—"Service Providers";
- Administrators and other managers of the Company—"Administrators". (together, Employees, Service Providers, and Administrators hereinafter referred to as "Collaborators").

The Company reserves the right to review, amend, or revoke this policy at any time, providing timely notification of such changes to all Collaborators.

It is part of the nature of information technology to undergo constant evolution. The principles of this policy shall apply to new types of technologies and devices with the necessary adaptations, regardless of whether they are specifically mentioned or provided for herein.

3. Compliance with this Policy

The Company considers that negligent or improper use of the IT made available to Collaborators is likely to cause serious harm to the Company. In this regard, any Collaborator who violates this policy, whether by action or omission, negligently or willfully, may be temporarily or permanently prohibited from accessing the Company's IT without prior notice, and, if an employee, may also be subjected to disciplinary action. In severe cases, Collaborators may, according to their applicable relationship and in compliance with the relevant legal processes, be barred from continuing to collaborate with the Company.

Additionally, any Collaborator may be held civilly or criminally liable for damages caused to the Company resulting from their failure to comply with the rules set forth in this policy.

4. General Principles

The diligent and prudent use of the Company's IT means, in general terms, that the Collaborator shall not use the IT to search, transfer, view, or store any content that contains:

- Any obscene or pornographic material;
- Any offensive or inappropriate content related to ethnicity, religion, belief, gender, gender identity, marital status, civil union, sexual orientation, disability, age, or any other personal characteristic;
- Any other content that could reasonably be considered offensive, defamatory, or in poor taste, according to the Company's exclusive criteria;
- Any content that exploits the vulnerabilities of others;
- Any content for which intellectual property rights belong to third parties, including third-party software, films, music, books, games, and others.

Collaborators should also avoid using IT in a manner that may damage, overload, or otherwise negatively impact the Company's IT and systems.

5. Equipment

The Company may assign Equipment to Collaborators, including but not limited to work electronic devices. The assignment is made according to the needs of the Collaborator in the context of their functions within the Company. Consequently, all Equipment must be used exclusively for the professional functions of the Collaborator with the Company, and under no circumstances shall its use for personal purposes or any other purposes not allowed by this policy be permitted or tolerated. If the Collaborator, at their own risk, decides to use any Equipment for personal purposes or purposes

other than those permitted by this policy, they may incur a violation of this policy. Furthermore, they should not have any expectation of privacy regarding the content stored on such Equipment, as this Equipment and the information contained therein will be subject to archiving and monitoring as provided in Chapters 8 and 11 of this policy.

The Equipment must be maintained and used diligently and prudently. In particular, the Collaborator:

- Must use protective equipment, such as appropriate bags, cases, screen protectors, etc., whenever possible;
- Must not leave the equipment in an unattended location;
- Must avoid exposing the equipment to extreme cold or heat temperatures;
- Must only use accessories provided by the Company or those whose use has been authorized by the Company;
- Must protect access to the Equipment by using pins or passwords;

In general, must be familiar with and comply with all safety standards indicated by the Company or by the manufacturer or distributor of the Equipment.

6. Use of Internal Networks and Platforms

The Company provides access to the following services:

- Internet
- Intranet
- Email
- Collaborative Platforms (namely, Webex, Teams, Zoom)

6.1. Internet

Access to the Internet is provided for purposes related to professional activities, that is, to conduct research in the context of professional functions performed, access online services, communicate with clients or third parties, and, in general, for any purpose related to the interests of the Company. Therefore, the use of the Internet provided by the Company for any personal purposes or purposes other than those mentioned above is neither permitted nor tolerated.

The Collaborator should be aware that websites can “know” who has visited them. If the Collaborator visits a site, they may leave a “business card” that allows the owners of the site to know who visited. Visiting an inappropriate website may cause harm to the Company and the Collaborators themselves. Under certain circumstances, this may even constitute an illegal act, potentially resulting in legal liability for both the Company and the Collaborator. Such use would constitute a violation of this policy, and the Company may take appropriate and pertinent measures in this context.

6.2. Intranet

Includes Internal Applications, Websites, Email, Fileshare, ERP, IOT Factory.

6.3. Email

The Company provides Collaborators with email accounts with the following domains:

3dtech.pt, attlda.pt, cadflow.pt, distrim.pt, distrim2.pt, dt2rmc.pt, ehtp.pt, grandesign.pt, hpm.pt, iemc.pt, moliporex.pt, moliporex.com, mptool.pt, vangest.pt, vangest.com.

The aforementioned domains are owned by the Company and managed exclusively by the Company as its IT. Consequently, these emails must be used exclusively for the professional functions of the Collaborator with the Company, and under no circumstances is their use for personal purposes or purposes other than those above permitted or tolerated.

Email constitutes an integral part of the Company's business activity and is an essential tool for the performance of that activity. For the purposes of archiving and monitoring provided for in Chapters 8 and 11 below, the Company will assume that all emails received and sent through the Company's email account are not personal and are solely related to the Company's business activity. Collaborators should have no expectation of privacy regarding communications sent or received through that email account.

Regarding matters related to the Company and/or its activities, Collaborators must use the email account assigned by the Company and no other, including, without exclusion, in any communications with clients or suppliers. If the Collaborator receives a message at an email address belonging to the Company that is of a personal nature, they must immediately inform the sender that such an address should not be used for that purpose.

Since email is a form of written communication, the Collaborator should exercise the same care in drafting emails as they would in preparing other forms of external communication. Email messages may be read by individuals who are not necessarily the intended recipients of the message.

All emails must contain the following information in their signature:

CONFIDENTIAL. Message and any attachments exclusively intended for the individuals to whom they are addressed: if received in error, please notify the sender and delete the message and attachments. The Collaborator should also be aware that email messages are documents subject to disclosure in the context of legal proceedings. In this context, they should not include any personal information in an email and should avoid using email to share confidential information or information that may contain the Company's trade secrets.

The contents of emails sent to individuals outside the Company or its group should not contain any trade secrets of the Company, any confidential or proprietary information of the Company, or any other information that may harm the Company's business. If it is necessary to send information of this nature, the Helpdesk should be contacted to assess the need for sending the information with encryption.

The Collaborator should only disclose their Company email address for professional purposes and must keep their passwords secure.

The Collaborator must not import external files or unknown messages without prior verification through antivirus software.

If the Collaborator receives an email with an attachment and is uncertain about its origin or content, they should not open it. Collaborators should immediately contact the Helpdesk team and request advice and/or inspection of the email in question.

If the Collaborator suspects that their Equipment may have been infected by a virus, they should immediately disconnect it and contact the Helpdesk team.

6.4. Collaborative Platforms

Collaborative platforms are those that enable instant communication between Collaborators or between Collaborators and third parties. These platforms can facilitate communication via text, audio, video, or a combination of these three (e.g., Zoom, Teams, Google Meet, etc.).

Currently, the Company provides all Collaborators with the following collaborative platforms:

- Cisco Webex for internal and external communications;
- Microsoft Teams for internal and external communications.
- Cisco Jabber for internal communications.

It is the exclusive discretion of the Company to choose the communication platform(s) it deems suitable for its interests. The Company may opt to install a single collaborative platform or several, and may internally define the rules for the use of each or leave their selection to the discretion of the Collaborators.

The collaborative platforms mentioned above are licensed to the Company and managed exclusively by the Company as its IT. Consequently, these platforms must be used exclusively for the professional functions of the Collaborator with the Company, and under no circumstances is their use for personal purposes or purposes other than those above permitted or tolerated. Collaborators should have no expectation of privacy regarding the content they share on these platforms, whether through audio, video, text, or document sharing.

Written Communications:

The internal chat serves as a communication tool exclusively between Collaborators. Collaborators should use the chat for quick communications with other Collaborators, such as, but not limited to, requesting or sending documents, scheduling meetings, or clarifying quick questions. The chat should not be used for sharing large documents or complex information that, in the Company's interest, should be archived for future reference. In such cases, the Collaborator should opt for email.

Collaborators should exercise caution when creating chat groups: to avoid excessive "noise" during working hours, the chat should be used as necessary and in accordance with the functions performed by the Collaborator.

Virtual Meetings:

The Collaborator should, whenever possible, opt to use the platforms authorized by the Helpdesk for conducting virtual meetings. If invited to use other platforms, they must (i) seek prior authorization from the Helpdesk and (ii) whenever possible, use those external platforms via a browser, i.e., without downloading the application of that external platform.

The Collaborator should bear in mind that the virtual meeting should proceed in a manner similar to an in-person meeting, and therefore it is requested that the Collaborator present themselves appropriately and conduct themselves similarly to how they would in a face-to-face meeting.

The Collaborator should take special care when sharing their screen: they should close all windows that are not relevant to the presentation in question before starting any screen sharing to avoid sharing unwanted content.

7. Definition and Safeguarding of Access Data

The Company has a centralized system for assigning and managing access to its systems. The identification of Collaborators and their passwords are an essential part of the Company's strategy to prevent unauthorized access to its systems.

In this regard, all access data assigned by the Company are personal and non-transferable. The Collaborator may not share this data with anyone, not even with other Collaborators of the Company. To prevent unauthorized access, the Collaborator must keep their access data in secure locations known only to themselves.

The Collaborator should be aware that they will be responsible for any unauthorized actions in the Company's systems where their User ID and corresponding password are used. The use of their password by third parties may lead to serious commercial damage to the Company. Thus, the deliberate disclosure of the password to others, particularly to individuals outside the

Company may constitute a serious disciplinary violation.

If the Collaborator suspects that their password has been discovered or used by a third party, they must change it immediately to prevent unauthorized use.

8. Information Archiving

The Company uses internal servers to archive all information created, received, or extracted through its IT systems. The use of centralized information archiving and management systems ensures the security, integrity, and availability of all information generated in the context of the Company's business.

In this context, the Collaborator may not, under any circumstances, choose to use fixed (e.g., computer) or portable (e.g., USB drive) local storage systems, except in exceptional situations where it is not possible or timely to process that information in the Company's centralized systems.

Similarly, no Collaborator may delete any data (including, but not limited to, documents and emails) from the Company's servers or export it to personal or unauthorized storage folders.

The processing or archiving of information on client platforms may only be done in circumstances where it is not possible or convenient to process it using the Company's centralized systems and with prior express written authorization from the Helpdesk.

In accordance with the hierarchy of access that may be established, the Company may access any information stored in files controlled by the Company (including, but not limited to, documents and emails) at any time, as set forth in Chapter 11 of this policy.

9. Downloading and Use of Software

The downloading of any software by the Collaborator (if registered in the internal system as a user) onto the Equipment is not permitted, except with prior express written approval from the Helpdesk team. The Collaborator can refer to Chapter 13 of this policy below for instructions on how to request such installation.

Any software whose download is authorized must (i) be verified to rule out the possibility of malware that could jeopardize the Company's IT infrastructure, and (ii) may only be used in accordance with the respective licenses or intellectual property rights and this policy.

In summary, the Collaborator may not:

- Use the Equipment to commit any type of legal violations;
- Attempt, directly or indirectly, through third parties, to disable, infringe, or circumvent any security devices of the Company designed to protect privacy or the security of the IT infrastructure;
- Add, alter, update, or remove software from any Equipment except when authorized by the Helpdesk team.

10. Social Media

The Company acknowledges the popularity of social media, both for personal use and within the scope of the Company's commercial activities. However, there may be serious repercussions for the business if these sites are misused. The Company's position regarding social media is outlined below.

The use of any personal social media through IT is not permitted unless analyzed and authorized on a case-by-case basis. The Company only allows the use of social media for professional purposes.

When using social media for any reason, the Collaborator may not make or publish any comments that could harm or negatively affect the reputation of the Company, its products and services, as well as its representatives, employees, clients, and competitors. The Collaborator must also not disclose any content protected by trade secrets or that belongs to the Company.

The Collaborator must ensure that the Company is not cited or otherwise identified in a detrimental manner. Whenever the Collaborator identifies any content on social media that may harm the interests, image, or reputation of the Company, they must immediately notify the Helpdesk in that regard.

Only Employees and Administrators are authorized to disclose their collaboration with the Company on social media (professional or personal). Service providers must not publicly or privately reference their collaboration with the Company in any social media context, except if previously and explicitly authorized to do so by the Helpdesk.

If an Employee ceases to collaborate with the Company, for any reason, they must update the information on their social media where they identified themselves as a collaborator of the Company, clearly indicating the termination of their collaboration with the Company. This update should ideally occur within a maximum period of 15 (fifteen) days after the last day of collaboration with the Company. The Company reserves the right to take appropriate measures if the Collaborator does not proceed with the aforementioned update of their profile.

11. Monitoring and Access by the Company

The Collaborator should be aware that the Company may monitor the use of IT to verify compliance with this policy or whenever necessary to safeguard the interests of the Company. Monitoring will always prioritize, whenever possible, the least intrusive and most individualized measures (but not discriminatory).

However, when less intrusive measures are insufficient to protect the IT and the Company's assets, the Company may temporarily block access, conduct penetration tests, or inspect the Equipment assigned to the Collaborator. The inspection of the Equipment will, whenever possible and provided it does not jeopardize any potential defense position of the Company, be communicated to the Collaborator in advance. However, if such communication could jeopardize the Company's ability to obtain evidence, the inspection of the Equipment may be carried out remotely and without any prior notification to the Collaborator.

In particular, the Company reserves the right to monitor and audit professional emails (i.e., emails with any domain listed in 6.3 above), internet access (including information about visited websites), and any other data stored on the Equipment. Reasons that may lead the Company to carry out this monitoring include, but are not limited to:

- An imperative need to safeguard the interests of the Company, especially when access by the Collaborator is not possible or such access may jeopardize the Company's interests;
- Preventing, investigating, or detecting the unauthorized use of the email system, the internet, and the Company's computer equipment or mobile phones as mentioned in this policy;
- Preventing or detecting the commission or possible commission of a punishable act;
- Ensuring that the system operates effectively (for example, by detecting and preventing the presence of viruses); or
- For quality control or training purposes.

12. Incidents

Despite all technical and organizational security measures that can be implemented, whether due to human error or system failure, incidents may always occur that affect the availability, integrity, and/or security of IT. Therefore, it is important that the Company and its Collaborators are prepared to respond to these incidents.

Thus, if the Collaborator becomes aware of any incident related to the IT assigned to them, they must immediately contact the Helpdesk. The Collaborator should not delete any suspicious information, as this may impede the investigation being conducted by the Helpdesk team. They should only disconnect the Equipment and await further instructions.

13. Helpdesk

Any doubts, questions, requests for assistance, or notifications of incidents related to this policy should be communicated through the following contacts:

Email: https://helpdesk.vangest.pt/readydesk/customer/rdlogin.aspx

Phone:

+351 911 160 824 (David Domingues)
+351 913 048 621 (Hugo Rosa)
+351 914 258 474 (João Sousa)

(only for incidents and assistance requests that seriously and irreparably limit the Collaborator's ability to work).

VANGEST

Information Technology Usage Policy

V1 - 2023

Complexo Industrial VANGEST
Rua de Leiria, 210
2430-091 Marinha Grande

+351 244 575 700
vangest@vangest.com