Quibim

General Information. Best practices in cybersecurity.

Table of Contents

1. Object

External personnel or collaborators (hereinafter, the "**Collaborator(s)**") who use Quibim resources or information assets must comply with the security provisions required by Quibim under its Information Security Management System (hereinafter, the "**ISMS**"), according to the characteristics and nature of the activities and engagement to be carried out, the services to be provided and the use they shall make of Quibim's information and resources.

Generally, when a user has doubts about whether an activity may be acceptable or unacceptable, it must inform its superior and, in any case, act as restrictively as possible, i.e., not carry out the activity until the necessary information has been obtained.

The rules, controls and procedures included in this "**Best practices in cybersecurity**" document have been drafted to ensure compliance with the provisions of the General Data Protection Regulation (EU 2016/679) and the Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), the international standard on information security ISO 27001 and the Spanish National Security Scheme under Royal Decree 311/2022.

2. Quibim's position

Internet browsing and the use of corporate e-mail, as well as the use of corporate resources in general, is not subject to systematic review by Quibim, in order to respect the preferred way of performing the engagement of Collaborators, their right to privacy and the secrecy of communications. However, by accepting or signing, as the case may be, the document herein, Quibim Collaborators expressly consent and is warned that Quibim may make a general control of the use of systematic review tools, utterly respecting the privacy and dignity of each individual.

Specifically, such general control will be aimed at verifying the rational and fair use of all corporate resources, the detection of possible abusive behavior, the prevention of criminal behavior, security, protection of goods and persons, detection of viruses and security attacks. Therefore, if any identified misuse of the communication systems is evidenced, Quibim shall take action as deemed appropriate.

Reviews may be carried out on an individual basis only when there is reasonable suspicion of the commission of a crime, misconduct, administrative offence, breach of employment, or a breach of these rules that compromises the security of information systems or may entail risks or damage to the assets or protected interests described in Quibim's rules, controls and procedures, and in particular, the document herein.

3. Confidentiality

It is the obligation of all Collaborators who access information, whether considered personal data, or not, or whether it refers to Quibim's business, in digital format, on paper or on any other medium, to respect the applicable regulations in this area, maintain the utmost confidentiality of said information and apply the security measures established in this document, in all applicable regulations or communicated from time to time by Quibim.

The security measures established for the processing and storage of personal data, in digital or paper format, must be complied with. A summary of the same is available at Quibim's webpage, **here**.

The applicable directives included in the ISMS for the handling of confidential information and documentation related to Quibim's scope of development must be complied with.

Remember, the confidentiality obligations agreed upon in the non-disclosure agreement entered into with Quibim, or analogous confidentiality provisions agreed, establishes that Collaborators undertake to inform Quibim of any unauthorized use of confidential information by third parties of which they have become aware of by any means.

4. Specific rules on the use of e-mail

Collaborators are responsible for all actions performed with the e-mail accounts and respective mailboxes and should be aware of the risks involved in the misuse of e-mail.
For this reason, the guidelines to be followed are described below:

- If a user receives messages with inappropriate content in their e-mail, they must inform their superior of this circumstance, for the adoption of the pertinent measures.

- It is forbidden to use the e-mail for any purpose unrelated to the engagement and professional responsibilities entrusted by Quibim.

- For security reasons, e-mail may not be used to send or reply to messages or chains of messages likely to cause congestion in Quibim's systems or that may introduce viruses or involve any risk or problem in Quibim's systems, tools and platforms.

- It is also forbidden to make any other use that may negatively affect Quibim's reputation, compromising its image and name.

- Given that both the Internet and e-mail are major sources of propagation and infection of computer viruses, and although Quibim takes the utmost precautions, the Collaborator, in the event of any suspicion of virus entry, must act according to the following protocol:

    - Communicate any suspected virus attack to your contact within Quibim and to Quibim's Security Manager (securitymanager@quibim.com).
    - Never open an attachment without checking that it is not infected, regardless of its origin, especially when the origin is unknown.
    - Do not execute executables attached to an e-mail.
    - Never open unknown URLs, especially if they come from an unknown or untrusted source.
    - In the case of opening Office documents (Word, Excel, etc.), it must be done without activating the macros since it is a possible entry of viruses.

5. Specific rules on the use of the Internet

- Each Collaborator is responsible for the Internet sessions initiated from corporate computers provided by Quibim, if any.
- Internet access and use may not be used for leisure, commercial or lucrative purposes for the benefit of the Collaborator.

- Nor may the Internet be used as a means of access for the commission of illegal actions or actions contrary to current legislation, morality, good customs and public order.

- Any software or file with the aforementioned contents found on any computer equipment owned by Quibim will be deleted without prior notice, regardless of any possible action that may be taken.

- The installation of any P2P type of software for file exchange, chat services, instant messaging, etc., is expressly prohibited.

- Should a Collaborator receive pages with inappropriate content through the technological means made available to them by Quibim, they must inform their

contact within Quibim of this circumstance, so that the appropriate measures may be taken.

- The Collaborator must not connect to any online service or utility without the prior and express authorization of the Security Manager, nor may the Collaborator connect to "anonymous browsing" pages.

- The traffic data generated by the established communications may be retained if the pertinent authorities request it.

6. Specific rules on the use of passwords

Passwords are for the personal and exclusive use of the Quibim Collaborator, and each individual is responsible for any use. For this reason, deliberately providing a personal password to any other person is considered a very serious offense.

Furthermore, it is also forbidden to write passwords clearly on any type of support (paper / electronic), as well as to use passwords in Quibim in private areas and vice versa. If necessary, you can consult the Security Manager about the possibility of using a corporate password manager.

It is the obligation of all Quibim Collaborators to strictly comply with the rules for the use of passwords indicated below:

- They must be at least eight characters long (twelve characters in environments without two-factor authentication). We generally *recommend twelve characters*.

- They must include upper-case and lower-case alphabetic characters, numbers (at least one) and special characters (at least one). Dictionary words in any language or variations on them, including the user identifier or part of the user's name or surname, and passwords based on the name of the organization are expressly forbidden.

- At the time of the first access to a system or platform with a previously generated password, the user must proceed to change it. From that moment on, it is the sole responsibility of each user to keep the chosen password secret.

- Reuse of the previous ten (10) passwords is not allowed.

- Password changes are forced annually (in environments without two-factor authentication, passwords shall be changed every six (6) months or less).

- After five (5) consecutive unsuccessful access attempts, the user's account is automatically blocked, requiring Quibim IT Department's intervention to unblock it.

- It is forbidden to store ("remember") passwords in web browsers. We recommend the use of password managers.

In case of suspicion, for whatever reason, that a password has been compromised, it must be communicated to the Security Manager (securitymanager@quibim.com) to change it immediately.

7. Mobile device policy

7.1 Introduction

Despite being essential for performing daily work activities, mobile devices introduce significant risks that must be properly managed to ensure the security of Quibim's information and information systems.

7.2 Responsibilities

It is the sole responsibility of the Collaborator to ensure the security of both the device itself and the information it processes and contains, complying with these regulations and all those relating to the security of Quibim's information systems.

7.3 Laptops:

- We recommend having the option to automatically update applications and the operating system.
- Laptops must be automatically locked after five (5) minutes of inactivity. However, users have the responsibility to lock their computers every time they leave or are absent from their workstations.

7.4 Smartphones

In the case of corporate devices, make sure and contact the IT Department to have the correct security configuration. Our recommendations are as follows. :

- The automatic application and operating system update option is enabled by default.

- Protection of smartphones by at least a four-digit PIN. Alternatively, a biometric control (fingerprint or facial recognition) can be configured, with patterns being prohibited.

- Automatic lockout after thirty seconds of inactivity.

- It is the sole responsibility of the mobile device user to ensure the security of both the device itself and the information it processes and contains.

- The storage of relevant Quibim information on the device is not permitted. It is the responsibility of the mobile device user to keep all the business information in the Quibim information repositories updated at all times. All relevant information must be worked on directly or stored daily in the organization's file servers so that a possible loss of support or equipment never means a loss of information.

- If there is a suspicion of infection that a device has been infected by any type of malware, the Collaborator must disconnect the device from the network and notify Quibim's Security Manager as soon as possible.

7.5 Transportation of equipment and computer media

About electronic media, the following guidelines are included:

- We do not recommend using external media (external hard disks, pen drives, memory adapters, etc.) on corporate equipment. Only corporate devices, which must be previously encrypted with a strong algorithm and password, should be used in case of need (for justified operational or business reasons). We recommend contacting your IT Department to follow security guidelines in this regard.

On the other hand, the guidelines regarding portable equipment are:

- The equipment cannot be left unattended at any time.

- The computer must remain locked as long as it is not being used.

- Be aware of possible foreign glances (shoulder surfing).

- If the computer is transported in a car, it must not be visible or easily accessible. Under no circumstances may the computer be left in the car.

- The computer must not be subjected to inappropriate environmental conditions of temperature and humidity. For example, equipment should not be left inside a vehicle in the sun or outdoors.

- In case of theft or loss of the equipment, Quibim's Security Manager must be notified as soon as possible, indicating any data that may be relevant for its recovery (place, date, time, etc.).

7.6 Installation and use of programs. Intellectual and industrial property

We advise against installing commercial software without the required license. Therefore, if you become aware of unsupported software, it is mandatory to inform Quibim's IT Manager or Security Manager, to proceed with the uninstallation of such software and find an alternative to it.

7.7 Network connection

Although computers must be equipped with an up-to-date antivirus system capable of detecting and blocking most malware, it is impossible to guarantee this in its entirety. Connecting to untrusted networks can lead to laptop infection.

Connection to public and open WiFi networks is not advised. Furthermore, the Collaborator must avoid or, in any case, minimize as much as possible connections to unknown networks (for example, networks of suppliers, hotels or airports) to those cases strictly necessary to perform urgent professional tasks. Connection to untrusted networks, including the Internet, endangers the security of the equipment and, by extension, that of Quibim as a whole.

In the event your device is infected by a virus or other malicious software is suspected, it is necessary to disconnect the equipment from the network immediately and inform Quibim's Security Manager as soon as possible.

7.8 Rules on antivirus protection

With regard to the antivirus protection mechanisms, the following policies of use, prohibitions and obligations are detailed:

- It is not recommended to deactivate the antivirus protections installed in computer equipment or to cancel the updating of antivirus programs.
- Any anomaly detected in the updating of antivirus programs will be reported as a security incident.
- You must verify that all versions of antivirus products are correctly updated.

8. Remote access to infrastructure and systems

The following is the remote access policy that Quibim has defined:

- Remote access to Quibim's technological infrastructure and information systems must be made compulsory and exclusively from authorized computers.
- Quibim's general security policies (strong passwords, encryption, secure printing, screen locking, clear desks, etc.) apply to both working from Quibim's premises and remotely, either at home or from a hotel or temporary residence.
- Access to any type of internal information and corporate equipment by persons other than the expressly authorized Collaborator is prohibited.

9. Classification of information

Quibim has established criteria for the classification and processing of information, considering its importance and sensitivity, as well as the impact that its loss or disclosure could have.

All information is classified into one of the following levels:

- **Public**: information that is not subject to any restrictions and that is shared by the company, for example, in newspapers, on the Internet or in commercial media. The public use of company information requires the approval of the corresponding bodies. Examples: press releases, product catalogues for clients, a general presentation of the company, and the content of the Quibim websites.

- **Internal use**: information intended for internal use by Quibim personnel (and duly authorized external personnel). This is the default classification level in Quibim. The loss of confidentiality or unauthorized disclosure may have a moderate negative impact on the organization, its customers or suppliers.

- **Confidential**: information whose knowledge or disclosure to unauthorized persons could seriously jeopardize the achievement of Quibim's objectives or business and should therefore only be accessible to a very limited group of duly authorized persons.

The following are mandatory guidelines for handling and manipulating "*Internal use*" or "*Confidential*" information:

- "*Confidential*" information must only be printed when there is a justified need and is not allowed outside Quibim's facilities. It must be securely destroyed at the same time that the need that originated its printing disappears.

- Information in electronic format must be stored on corporate servers, and it may not be stored in spaces other than corporate ones (e.g., Dropbox, etc.).

- The exchange of information with third parties is not allowed unless previously authorized by virtue of an agreement that regulates the conditions of such exchange as well as the necessary confidentiality and non-disclosure requirements.

- For the exchange of "*Internal use*" or "*Confidential*" information, the infrastructure and means made available by Quibim, corporate e-mail, instant messaging and communication tools must be used. The use of other types of

resources (personal e-mails, public clouds, non-secure applications such as WeTransfer, WhatsApp, Signal, Hangouts, etc.) is prohibited.

- The information on paper must be sent using a certified postal service and with traceability of the shipment.
- Information on paper must be destroyed using paper shredders or, alternatively, using secure containers.

10. Specific rules for work in offices, rooms and facilities

The general security policy for offices, rooms and facilities is as follows:

- Quibim's offices, rooms and facilities can only be accessed by duly authorized personnel of the organization; Collaborators who need access to Quibim's offices must be properly identified and must always be accompanied by personnel of the organization.
- It is imperative that offices be securely locked in the absence of their proprietors from the premises.

11. Information security incident management

Any anomaly that affects or could affect the security of Quibim's information or information systems will be considered an incident.

All Collaborators are required to report any incident, possible incident or weakness they observe or suspect in information security that could compromise the availability, integrity and/or confidentiality of Quibim systems, services or information.

Notification of an incident, possible incident or weakness is made by the following means:

- Communication to your Quibim's PoC (Point of Contact).
- Communication to the Security Manager. securitymanager@quibim.com