AquaBioTech Group

ICT Handbook

Version 2.2

AquaBioTech Group

Headquarters, Malta

03rd December 2025

AquaBioTech Group

Central complex, Naggar Street, Targa Gap, Mosta MST 1761 - Malta G.C.

Tel: +356 2258 4100 **E-mail:** aqua@aquabt.com

Contents

1. Introduction

1.1. Purpose

This document outlines the Information and Communications Technology (ICT)-related policies and guidelines that all **AquaBioTech Group** employees are required to follow in the course of their daily work, regardless of their physical location or the specific **AquaBioTech Group's** office in which they are based. The primary aim of this ICT Handbook is to support the delivery of high-quality IT services and to uphold the integrity, security, and reliability of company data and digital infrastructure.

AquaBioTech Group will make this ICT Handbook available to all employees who are expected to use it as a key reference resource for any ICT-related issues or questions. This document itself adheres to the standards and practices it sets out, serving both as a guideline and as an example of best practice.

1.2. IT support requests

To ensure efficient handling and timely resolution of IT-related requests all queries need to be sent to the IT Helpdesk via one of the following official channels:

Email: **helpdesk@aquabt.com**

Phone Extension: **999** (internal use only)

Please note that requests submitted through unofficial channels—including Microsoft Teams™, SMS, WhatsApp, personal emails, or any email addresses other than the one listed above—will not be monitored or actioned by the ICT Department.

Should you be abroad/out of the office and unable to access email then please contact front office directly on **+356 2258 4100** and ask to be redirected to ICT.

2. Use of Company Facilities

All company facilities, including hardware, software, networks, and office infrastructure, are to be used exclusively for work-related operations only. Only tasks, and duties directly associated with an employee's role and responsibilities within **AquaBioTech Group** should be carried out.

Personal or unauthorised use of company resources are prohibited unless explicitly approved by management.

2.1. Company Access Cards

To ensure the safety and security of personnel within **AquaBioTech Group** premises, the following rules regarding company access cards are mandatory and must be strictly followed:

- The use of your personal access card is always mandatory when on company premises.
- All employees are required to register each entry and exit using the designated card readers.
- Access cards are personal and may not be shared or exchanged with other staff members under any circumstances.
- In the event of a lost or stolen access card, you must immediately notify:

The **HR Department**: hr@aquabt.com

The ICT Department: helpdesk@aquabt.com

- Temporary access cards ("**Joker cards**") are subject to the following conditions:

Must be **returned** within **24 hours** of issuance

Automatically **disabled after 24 hours**; they are not a valid long-term replacement

Cannot be shared with or transferred to another staff member

Limited to **one request per month** per employee

Repeated failure to comply may result in the employee being sent home to collect their personal access card and return to the office and their time counted as unauthorised absence.

- In the case of a **lost or damaged access card**—where the damage is deemed to be due to misuse or non-standard wear and tear—the employee will be charged a **replacement fee**.
- Access to restricted areas or specific doors is subject to prior written approval from **HR and/or the Departmental supervisor** and will only be granted after the required training has been completed and certified.

Labs Access (Dry labs or Ecology): **labsec@aquabt.com**

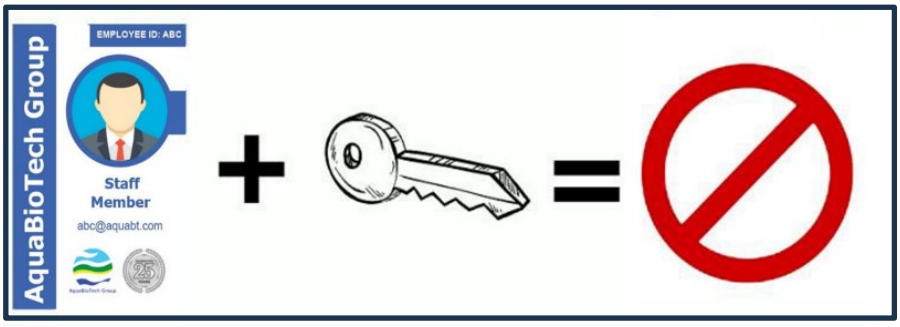
Innovia Facility Access: **innoviasec@aquabt.com**

Roof Access: **roofsec@aquabt.com**

Backdoor LVL0: **doorsec@aquabt.com**

The ICT Department will not process any access requests unless written authorisation has been received in advance from the departmental supervisor.

- Under no circumstances should you access card and keys be stored or carried together. If both items are lost and the incident is not reported immediately; you may be held financially responsible for the full cost of replacing all affected black keys for employees and interns including the door locks.



3. Company Communications Channels

Effective communication is essential to the operations of **AquaBioTech Group**. To support this, the company provides a range of communication tools — SIM cards, the 3CX™ mobile application, and WhatsApp Business™. All communication tools are mandatory for all staff.

These tools are critical for maintaining real-time contact with employees during work hours and in extraordinary circumstances such as emergencies, urgent updates, or operational disruptions.

3CX™ is only used by staff that has an assigned internal telephone extension

3.1. Usage of Company SIM Cards

Company SIM cards are provided by **AquaBioTech Group** as essential tools for business communication. The Company has a large non-Maltese workforce as such you are permitted to utilise the company SIM as your personal Maltese number. However, the following rules apply to the issuance, use, and management of these SIM cards regardless as to whether you utilise them solely for work or for work and personal use:

- SIM cards will be issued by **AquaBioTech Group** with the condition that the mobile phone must remain switched on during working hours and periods of operational importance.
- Each prepaid SIM card is credited with an initial top-up of ten Euros (€10.00).
- Employees must make a call or send an SMS at least once within a six (6) months period to ensure the SIM card and assigned number remains active and is not deactivated by the service provider (EPIC). (a SMS containing your company initials must be sent to ICT via +356 9921 2203)
- Any work-related top-ups made by the employee will be reimbursed upon presentation of a valid receipt.
- In the case of company mobile contracts, if the monthly usage exceeds the plan limit, any excess charges incurred for personal use must be paid by the employee.
- The company reserves the right to issue either a contract SIM or a Prepaid SIM and

may switch between these at its discretion.

- All company SIM cards remain the property of **AquaBioTech Group** and must be returned to Front Office/Reception on the last day of an employee's contract, internship, or employment. SIM cards not returned will be cancelled without prior notice.
- A replacement fee of ten Euros (€10.00) will be charged for any SIM card that is not returned, lost or damaged due to reasons other than normal wear and tear.
- Employees are not allowed to link the company SIM cards to personal Epic accounts, attempt to register the line number under their personal name, or create an account using either a company email address or any personal email address.
- Mobile phones that are **not** Dual-SIM compatible will be issued with an e-SIM where applicable. Generally, iPhone XS and later models, including iPhone 11, 12, 13, 14, and SE (2nd generation and later) are eSIM-compatible.

How to:

Balance Check - Send a blank SMS to 16290

Credit Top-up Online - https://www.epic.com.mt/SSP/online-top-up

Value bundle Top-up – SMS the word VALUE to 16200 (a minimum credit of €9.99 needs to be available on your SIM)

Support Queries: helpdesk@aquabt.com

3.2. Phone Extensions and the 3CX™ App

As part of **AquaBioTech Group's** internal communication system, certain employees will be assigned an internal telephone extension on their first working day. This extension is integrated with the 3CX™ mobile application, which must be installed and properly configured on the employee's mobile device.

- The 3CX™ app enables VoIP-based calling and ensures employees remain reachable during working hours, including during off-site activities or in emergency situations.
- It is the responsibility of each employee to ensure the 3CX™ app remains installed, active, and functional on their mobile phone.
- ICT Department will provide you with a QR Code so that your assigned telephone extension is configured correctly on your mobile phone.

Making a 3CX™ Call

Using the iOS/Android app to make a call is as straightforward as making a call from your smartphone's native call function.

Enter a number via the Dialpad and press call.

Tap on the option from the menu and search contacts by name, extension number or email address. Or tap on a contact and select **"Call"**.

You can easily perform several actions on an active call:

"Transfer" allows you to perform two types of transfers.

"Blind Transfer"- transfer the call directly without addressing the receiver.

"Att. Transfer"- first speak to the receiver and then transfer the call.

"Conference" - add more participants to the call.

3.3. WhatsApp Business™ Usage

To support seamless communication while maintaining a clear separation between personal and work-related messaging, employees are required to use WhatsApp Business™ in conjunction with their company-issued SIM card.

- WhatsApp Business™ must be configured using your company SIM card and should be used strictly for work-related communication.
- If you are currently using WhatsApp™ with your personal number, you are kindly requested to install WhatsApp Business™. This will allow you to operate both your personal and company numbers simultaneously on the same device.
- For support in setting up WhatsApp Business™, please contact the ICT Department at helpdesk@aquabt.com

3.4. Microsoft Teams™ usage

- The use of official Company-branded Microsoft TeamsTM backgrounds is mandatory during all video calls and virtual meetings. These backgrounds are available in the following directory: T:\ABTG Office Templates\Teams Backgrounds. A guide can be found here: https://abtg.info/guides/#toggle-id-23.

- If you are unsure how to apply the background or encounter any issues, please contact the ICT Department at helpdesk@aquabt.com for assistance.

3.5. Microsoft Outlook

Email Security

All employees must exercise caution when handling emails, especially those that may be suspicious or unsolicited. Phishing and spoofing emails are a serious security risk and can lead to data breaches or system compromise.

- Never click on links or open attachments unless you recognise the sender and are confident the content is safe – this is the same for personal professional social media platforms used for work purposes, such as LinkedIn.
- If you are unsure about the legitimacy of an email, do not interact with it. Instead, forward the email to the IT Department at helpdesk@aquabt.com for review and

safety scanning.

- If you have clicked a suspicious link or entered your username and password, you must **immediately** change your password and report the incident to the ICT Department at helpdesk@aquabt.com.
- Failure to report a suspected or confirmed security incident may result in the staff member being held liable for any resulting damage, including but not limited to harm to Company systems, data, infrastructure, or information.
- The ICT Department will **never** request that you reset your password or reactivate your account via email. Any such request should be considered suspicious and reported immediately.
- Always report and verify any email that asks you to enter your user account credentials or password before accessing content. This applies even if the email appears to come from someone you know. If you have any doubts, contact the sender directly through a separate, trusted channel or reach out to ICT.

Email Etiquette

- The official Company email signature must always be used. Modifying any part of the signature, including your job title or contact details, is strictly prohibited. If any changes are required, written approval must first be obtained from both HR (hr@aquabt.com) and your supervisor. The IT Department will not process any signature modification requests without prior approval.

- **Subject Line**: All project related email communication needs to include the project code [ABT]~[xx]/[YY]~Co in the subject line. Ensure that the subject line is meaningful and reflects the content of the email. If there is an upcoming deadline or urgent action required particularly requiring response/input from senior staff include the date and time you require a response/action by. For example:

ABT~01/25~Mt: Guidance on Client feedback - Deadline: 25th Dec 12noon

- Use the "To" field only for recipients who are **required to act**. Use the "Cc" field for individuals who need to be informed but are **not** required to act. **Never use the "Bcc" field, this should only be used for emailing distribution list.** *If you need to alert a colleague or manager to a communication thread forward the email*

separately.

- When sending a message to an internal distribution list such as “All Users – allusers@aquabt.com", you must place the mailing list in the **Bcc** field. The **Cc** field must be populated with the HR email address (hr@aquabt.com). Any email not following this protocol will be automatically rejected in accordance with Company policy.
- Double-check that your message is addressed **only** to the necessary recipients. Avoid including others unless they need the information.
- Respond promptly to emails. Aiming to respond within 24 hours, even if only to acknowledge receipt and provide a timeframe for a full response. Always proofread your emails before sending. Clear, professional communication reflects the standards of the Company.
- Check for spelling and grammatical errors in both your email text and any attached documents. Use the built-in professional tools available in email software such as Microsoft Outlook, including spell check and formatting aids, to enhance message clarity and presentation.
- For external emails, always double-check that the correct file is attached before sending. This simple step helps avoid follow-up corrections and maintains professionalism.

Email Use

- For internal communications, avoid sending attachments when possible. Instead, share a link to the file’s location.

Sharing Files on the Server:

Right-click and “hold” the file on the server,

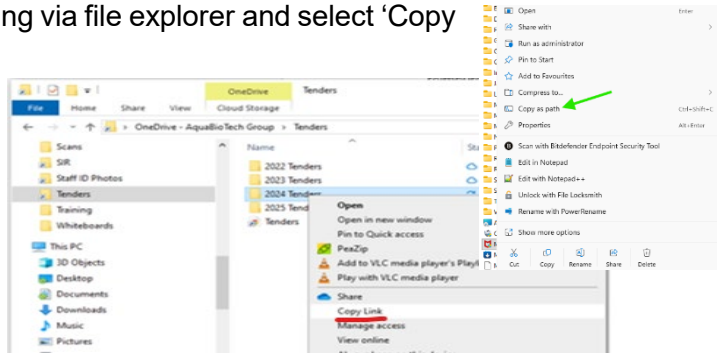
Drag it into your email body,

Select “Create Hyperlink Here” from the drop-down menu.

Sharing Files on the Cloud:

Right-click on the file name if accessing via file explorer and select ‘Copy Link’ Or click on the three dots next to the file name if accessing via teams/SharePoint and select ‘Copy Link’ or ‘Copy as path’

Paste the link into the body of the email



- Emails containing attachments such as Word documents, Excel files, PowerPoint presentations, or other editable formats will be automatically flagged by the ICT Department and will not be approved for sending, unless authorised by Management. Only PDF documents with a maximum file size of **10MB** are permitted as attachments when using Company email.
- Sharing Company confidential information or original working files outside of the organisation is strictly prohibited without prior written authorisation. Forwarding any file or confidential message to your personal email address is also strictly forbidden. Unauthorised sharing of company information will result in disciplinary action.
- The Company email account must not be used for personal matters under any circumstances.
- Using Company email or IT resources to conduct personal business or any non-work-related commercial activities is strictly forbidden.

4. Presentation and Travel Laptops

4.1. Presentation Laptops Internal usage

All staff members are reminded to follow the established procedures for borrowing and returning company presentation laptops.

Three presentation laptops are looked after by Front Office. It is essential that the laptops are returned on time to **Front Office** and used respectfully within the assigned loan period. Any incidents, issues, or damages must be reported immediately to the IT department – helpdesk@aquabt.com. Adhering to these guidelines ensures fair access for all team members, supports efficient workflow, and enables the IT department to maintain accurate inventory records. Timely returns help guarantee that laptops are available when needed by others.

How to book a Presentation laptop

Open Outlook>Calendar

Click "**New Meeting"** in the ribbon at the top

Title: Enter Meeting Details

Add **Required** staff attendees by typing names or email addresses including a Presentation Laptop if needed.

Subject: Enter a short description or title for the meeting in the Subject Line

Location: Type the meeting room name or click on the Location button: select your desired room that can host all the meeting internal attendees.

Start Time / End Time: Set the start / end times and dates for the meeting (Shortened meetings are set as default 25min / 50min).

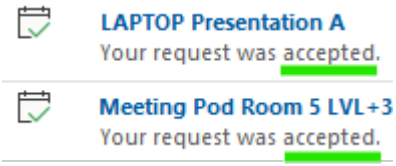
Body: Add agenda, instructions, links, or other meeting details.

If you need external attendees to join: Click on **Microsoft Teams**, click **"Teams Meeting"** from the toolbar to add the link automatically.

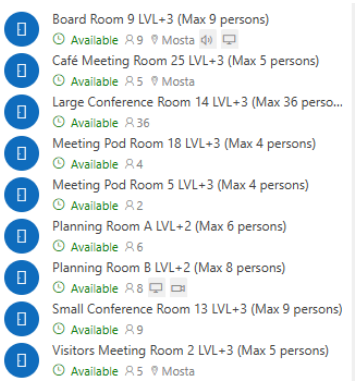
Set Recurrence (Optional): If this is a recurring meeting, click **"Recurrence"** in the ribbon, then choose frequency (daily, weekly, etc.).

Send the Invitation: Click **"Send"** in the top-left corner. This will send the invite to all attendees (including the presentation laptop and meeting room if selected) and place it in your calendar.

Ensure you receive the confirmation for the laptop and or meeting room booking in your Inbox stating: **Accepted.** If you receive a **Declined** response from either the Meeting Room or Presentation Laptop, please edit the meeting and select an alternative option.



Meeting Room Guidelines



- **Locations:** Rooms are available on Level+2 and Level+3. Each floor has a variety of rooms designed for different types of meetings
- **Restrictions:** Only authorised staff can book the following meeting rooms: Boardroom, Café Meeting Room
- **No-Show Policy:** Repeated failure to attend booked meetings may result in booking privileges being restricted.
- **Priority Use:** Larger rooms may be reserved for cross-departmental or client meetings during peak hours.
- **Clean Desk Policy:** Leave the room tidy and ready for the next user. Remove personal items and dispose of waste properly.

4.2. Travel Laptops requests and usage

- The request must be submitted to your supervisor at least one (1) week in advance for approval. Request and approval should be forwarded to **helpdesk@aquabt.com**. The ICT department will not process any requests without prior written approval from a supervisor.
- Before traveling, the staff member must log in to their account on the company network and verify that all required software and configurations are functioning correctly.
- Failure to complete these steps will result in the laptop being blocked from logging in outside the company, rendering it unusable during travel.
- Presentation laptops that were used to travel with must be returned on the first day back in the office. The device must first be inspected by the IT department before being handed over to the Front Office.
- Any physical damages during the lease period in the possession of the Staff member could be charged for to the staff account.

4.3. Management Access to Company Computers

- **AquaBioTech Group** retains ownership of all communications transmitted through any platform—including but not limited to Email, SMS, Messenger, iMessage, WhatsApp Business™, Microsoft Teams™, when such communications are stored on company equipment. Management, along with other authorised personnel, reserves the right to access, monitor, and review any data or materials stored on company computers or systems at any time, without prior notice. This includes files, emails, chat logs, and any other digital communications or documents.

5. Internet Service

Internet usage introduces potential risks to the security and confidentiality of Company information. It also increases the risk of system contamination through viruses, malware, or spyware. Spyware can enable unauthorised individuals outside the Company to gain access to sensitive data, including passwords and other confidential information. Employees are therefore expected to exercise caution and adhere to Company guidelines when accessing the internet through Company systems

5.1. Prohibited Usage

Employees are expected to use the internet and communication platforms responsibly and strictly for work-related purposes. The following activities are strictly prohibited and may result in disciplinary action:

- Forwarding any confidential or work-related messages to unauthorised external recipients.
- Sending Company files or documents to personal email accounts.
- Attempting to bypass or disable any system security or network protections.
- Using Company systems to conduct personal business or any commercial activities not related to Company operations.
- Accessing or playing computer games.
- Engaging in non-work-related web browsing.
- Copying, distributing, or using copyrighted material in violation of copyright laws.
- Accessing or using another employee's account or login credentials.
- Viewing or accessing websites containing obscene, pornographic, or otherwise inappropriate content.
- Sending, receiving, or soliciting messages containing obscene, profane, or offensive material.
- Expressing unsolicited personal opinions on social, political, religious, or other non-work-related matters through any Company communication channels.

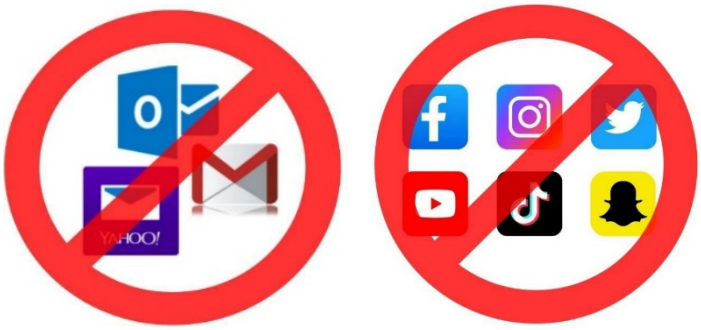
Sending or forwarding messages, jokes, or material via Microsoft Teams, Email, or any other communication platform that may be considered discriminatory, harassing, or sexually inappropriate. Such actions will be considered serious violations and addressed by Human Resources.

5.2. Bypassing firewall

- Employees are strictly prohibited from attempting to connect to the internet using any method other than the authorised and Company-approved network connections. This includes, but is not limited to, the use of external modems, personal mobile hotspots, cable connections, Virtual Private Networks (VPNs), proxy servers, or any other means intended to bypass the Company's firewall or security controls.
- Users must not attempt to conceal the origin of any data transmission or download material using a false or misleading internet address or identity.
- Any breach of this policy will be considered a serious violation and will be addressed in accordance with the Company's HR policy. Consequences may include disciplinary action, up to and including immediate termination of employment.

5.3. Personal Use Restrictions

- The use of personal email accounts—such as Gmail, Outlook.com, Yahoo, GMX, or any other free or paid email service—is strictly prohibited on all Company devices and networks.



- In accordance with Company policy, storing personal files, photos, or any other personal data on Company servers is not permitted. The Company will not back up or take responsibility for any such data. Employees found storing personal data that poses a risk to network security or Company information may be held personally liable. Any personal files discovered on Company servers—including but not limited to files stored on desktops, in the "Documents" folder, or other default storage locations—will be deleted and reported to Human Resources.
- Access to social networking applications, websites, and related services is restricted for all users. Only the Human Resources and IT departments may authorise access for work-related purposes. All other access is considered unauthorised and is strictly prohibited.

- Reasonable personal use of Company computing and telecommunications resources is permitted only during non-working hours—such as lunch breaks, before or after regular working hours—and only if it does not interfere with business operations or result in any additional cost to the Company.
- Permitted personal use does not include activities related to personal businesses, political campaigning, union matters, or any other similar non-work-related initiatives. Such use is strictly prohibited.

5.4. Responsible Internet Usage

All internet activity conducted through Company systems is traceable to its origin and may be subject to monitoring. Therefore, all internet usage must be appropriate, responsible, and capable of withstanding public scrutiny or disclosure.

- Users must not knowingly access websites or online content that could bring the Company into disrepute. This includes, but is not limited to, material that violates Company usage policies, contains pornography, hate speech or literature, promotes violence, or contravenes any applicable laws, including the Human Rights Act, Criminal Code, or other national or international legislation.
- Accessing online newsgroups, engaging in online chat, or using social networking sites such as Facebook, Instagram, or similar platforms for non-business purposes is strictly prohibited during work hours or on Company systems.
- Playing online games, engaging in online gambling, or accessing online entertainment sites (e.g., video streaming, music streaming, or gaming platforms) is strictly prohibited on Company equipment and networks.

5.5. Staff Wi-Fi Access

Before a staff member's mobile device can be approved for access to the Company's free Wi-Fi network, the following conditions must be met:

- The staff member must use a Company-issued SIM/eSIM in the device.
- The device must have **WhatsApp Business™** App properly installed and configured and **3CX™** App where applicable.
- A secure device lock code (PIN, password, or biometric security) must be set on all smartphones.
- When using a personal mobile device within Company premises, you are still expected to fully comply with all Company policies, including those related to

security, confidentiality, and acceptable use.

- If a mobile device (personal or Company-owned) that was used to access any Company information—such as email, OneDrive™, or SharePoint™—is lost or stolen, this must be reported immediately to both HR (hr@aquabt.com) and the ICT Department (helpdesk@aquabt.com).
- The use of personal laptops, tablets, or any other personal devices on the AquaBioTech Group Wi-Fi or LAN network is strictly prohibited under all circumstances.

5.6. Guest Wi-Fi Access

To maintain the security and integrity of the Company's network, access to the Guest Wi-Fi is strictly controlled and only granted through a secure token system.

- Staff members who are expecting visitors and require Guest Wi-Fi access must request tokens in advance through the Front Office.
- Upon receiving a token, the staff member must clearly write the following information on the back of each used token:

Your initials
The event name
The date of use

- It is the responsibility of the requesting staff member to return both used and unused tokens to the Front Office promptly after the event.
- Any attempt to use unauthorised tokens, reuse expired tokens, or bypass the limitations of any Company Wi-Fi network is a serious breach of policy and may result in disciplinary action.
- The MCA (Malta Communication Authority) in general, monitors the use of internet networks and may monitor Internet traffic and/or block access to Internet sites without notice.
- The internal ICT Department of the company may access a given user's Internet records at any time without notice to the user upon receiving a request / approval from the applicable Department Head and the Human Resources Manager.

5.7. Privacy

While individuals may reasonably expect a degree of privacy when using Company computers and electronic services provided for the performance of their duties, it is important to understand that all user mailboxes, files, and system activity may be accessed by IT administrators at any time—without prior notice.

Such access may be carried out to:

Remove malicious files or emails that could compromise network security,

Investigate potential policy violations or technical issues, or

Address any other concerns deemed necessary by Management.

By using Company systems, employees acknowledge and consent to this level of monitoring in accordance with Company policy.

6. Security

AquaBioTech Group prioritises the security of its systems and data. All employees are required to follow the Company's established information security protocols, which include but are not limited to:

Using strong and secure passwords,

Performing regular system updates where applicable,

Complying with data classification and handling guidelines,

Ensuring that critical data is regularly backed up to maintain integrity and availability.

Employees are expected to fully comply with all information security policies and procedures. This includes:

Always safeguarding sensitive and confidential information,

Promptly reporting any suspected or actual security incidents to the ICT Department and Paying close attention to regular security awareness emails and updates issued by the ICT Department.

Security is a shared responsibility. Failure to comply with these policies may result in disciplinary action in accordance with the HR policy framework.

6.1. Data Protection

To ensure data security and continuity, all employees are responsible for saving their work in the designated network drives or approved cloud storage SharePoint locations. This enables regular and reliable backups in line with Company protocols. These systems are in place to maintain the integrity, availability, and recoverability of critical business data.

- Only files saved within the 'Desktop' and 'Documents' folders on Company computers are included in the automated backup process. Employees must regularly verify that these folders are properly synchronised with the local server.
- Personal data or non-work-related files stored on the Company server or within backup-included folders (including Desktop and Documents) are strictly prohibited. Any such personal data found will be deleted immediately and reported to HR.
- In the event of data loss, corruption, or other incidents, **AquaBioTech Group's** ICT infrastructure provides two levels of backup protection to safeguard Company data:

Daily Shadow copies (7am and 12pm Daily) (FILESRV) for instant file restore

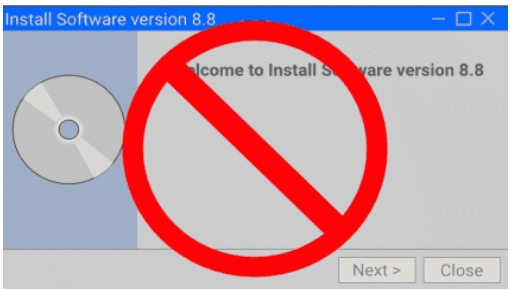
Daily Incremental Image backups of all Servers using licensed 3rd party Software (VEAAM) to a local NAS backup storage device.

Monthly Full Image backups of all Servers using licensed 3rd party Software (VEEAM) to a local NAS backup storage device.

6.2. Software Access and Installation Policy

To ensure system stability, security, and compliance with licensing regulations, **AquaBioTech Group** enforces strict controls on the acquisition and installation of software.

- Any software required in addition to the standard Microsoft Office suite must be authorised by the staff member's departmental supervisor and downloaded, installed exclusively by the ICT Department.
- If access to software not currently available on the Company network is needed, employees must contact the ICT Department at helpdesk@aquabt.com for guidance and support.
- Access to Company software and applications is granted based on job roles and responsibilities. Requests for additional software must be justified by work requirements and approved accordingly.
- All software installations must be pre-approved by the ICT Department. No software will be installed without a written request from the employee's supervisor.
- The ICT Department must be informed well in advance of any software requirements for specific projects to allow adequate time for evaluation, licensing, and installation.
- Staff members are strictly prohibited from installing any software themselves. Any such attempt will be automatically blocked and flagged by the IT system and may result in disciplinary action.

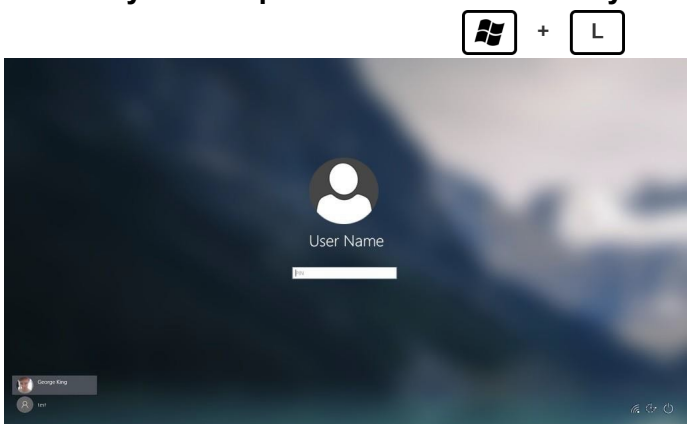


6.3. System Updates and Maintenance

To ensure the security, stability, and integrity of Company computers, the ICT Department regularly applies Windows security updates and maintenance tasks. To support these preventive measures, the following guidelines must be followed:

- From Monday to Thursday, all computers must be left powered on with the Windows user account locked, not signed out or shut down. This allows scheduled system updates and enables remote maintenance when required. Users should ensure that all open files are saved and closed before locking the computer. (Open files **cannot** be backed up)

To lock your computer: Press Windows key + L.



- On Fridays, before leaving the premises, all staff must shut down their computers properly. This reduces energy consumption and supports the safe operation of equipment over the weekend. It is essential to save and close any open files when not in use. Leaving files open may result in unsaved changes, data loss, or version conflicts - especially during overnight updates or system restarts.
- Updates are typically scheduled to be installed during the night. To ensure these are applied successfully, computers must remain connected to the Company network throughout the evening (Monday–Thursday).

6.4. External File Sharing Policy

To maintain the security of Company data and ensure compliance with internal protocols, the use of any third-party file sharing platforms—including but not limited to Dropbox, Google Drive, Box, WeTransfer, or similar services—is strictly prohibited.

If files need to be shared with external individuals, the following procedure must be followed:

First, obtain written permission from your supervisor.

Contact the ICT Department at helpdesk@aquabt.com to request the setup of a designated and secure OneDrive folder for external sharing.

The ICT Department will only process file-sharing requests that have prior written approval from the staff member's supervisor. This procedure ensures all external file sharing is conducted in a secure, monitored, and compliant manner.

6.5. Use of Personal Storage and Mobile Devices

To protect **AquaBioTech Group's** network and data integrity, the use of personal storage devices - such as external hard drives and USB flash drives—is strictly prohibited for transferring or storing Company data. These measures are in place to prevent the introduction of malware, unauthorised data transfer, and breaches of confidential information.

To further mitigate security risks, USB access is disabled by default for all employees.

The term mobile and storage devices include, but is not limited to:

Notebooks and netbooks

Smartphones and tablets

USB devices and external hard drives

USB flash drives and SD cards

Any other device capable of connecting—either wirelessly or via cable—to any part of the **AquaBioTech Group** network.

- Any mobile or storage device intended to store, retrieve, or access Company files, information, or emails must first be approved by the IT Department. Devices may not be connected to the network or any Company system without prior written authorisation.

6.6. Computer and Password Security

- To maintain the confidentiality, integrity, and availability of Company data, all staff must follow strict guidelines related to computer and password security.
- Company computers must never be left unlocked when unattended. Before stepping away from your desk, you must either:

  Lock your computer (Windows key + L),

  Log out of your session entirely.
- Password security is critical. The following rules must be always observed:

Never write down passwords in plain text or store them in unprotected formats.

Do not share your password with any other staff member under any circumstances.

Follow recommended IT password guidelines.

Minimum of 10 characters

A mix of uppercase and lowercase letters

At least one number and one special character

Avoid using:

Simple or common passwords (e.g., password123, 123456)

Variants of Company names (e.g., ABTG, aquabt)

Staff member initials or easily guessable personal information

By adhering to these practices, you help protect both your account and the wider Company network from unauthorised access and data breaches.

7. Document Control

7.1. Electronic File Naming Convention

File names need to be kept as short and concise as possible and without any spaces. Do not add any characters after the date

<ABTGroup/Company name>~<ProjectCode>~<DocumentName>.<VersionNumber> (If any) ~<dd-Mon-yy>

Example: ABTG~XYZ01~TechOfferBoQ~01-Jan-25

7.1.1 Please never modify a shared or read only file until previous user finish working on it or save a file as a copy of the original.

7.2. Group, Company and Department Name Abbreviations

ABTG = **AquaBioTech Group**

ABTL = **AquaBioTech Limited**

AqCi = **AquaCirc Limited**

7.3. Project Code Format

<Letter Client Code><Sequential Project ID Number> / Year project started ~ ISO 3166 Country Code

Example: **XYZ 01 / 22 ~ Mt**

7.4. File Name Length

The length of filenames should never exceed 50 characters. Filenames exceeding 50 characters might cause problems to backup software and might be shortened automatically.

7.5. Document Name Format

<Filename Part 1><Filename Part 2>.<Version number (if any)>

File names should be in Title Case without any spacing in between the words.

Example: **TechOfferBoQ~**

7.6. Version Numbering

- Vs1.0: Until the document is approved will be designated as the first version
- Vs1.1: When the author makes any major change to the document
- Vs1.2 When colleague1 receives the file and makes changes to the document

Example: ~Vs1.0

7.7. Date Format

- _ _-_ _ _-_ _ (DD-MMM-YY)
- Date 2x Numbers
- Month 3x Letters
- Year 2x Numbers

Example: 01-Dec-25

7.8. File Path Lengths

The maximum file path length for Windows is 260 characters including spaces, special characters, and the file name.

The file structures must be simple and clear to make it easier to find old data and for the network backups to execute correctly.

Below are examples of a long file path and a shorter simplified version.

Examples:

299 characters, Too Long

W:\ABTGClientResearchProjects\2015Projects\EuropeanUnionProjects\MonitorControlandSurveillanceProjects2020\DataReportsDocumentationResearchPapers\Reports\VesselMonitoringSystem\Thisisversion1ontheReportontheHoursLoggedontheVesselMonitoringSystemPerVesselType.docx

94 characters

W:\Projects\2020\EU\MCS2020\Data\VMS\ReportOnHrsLoggedOnVMSPerVesselType~01-Jan-20.docx

7.9. Saving Location

Please save all work-related documents, files and folders under their own Project folder on the local shared directories, as the backup server is configured to grab files from these folders only. In case of any accidental damage or corruption to any of your files or documents, please contact ICT department helpdesk@aquabt.com to recover the latest available backup version of your file.

7.10. General Examples

ABTG~CFF01~FarmEquipmentRequirements~21-May-08.doc (50 characters)

Should be abbreviated to

ABTG~CFF01~FarmEquipReq~21-May-08.doc (37 characters)
ABTT~AKK01~VegetationCoverageMap~03-Jan-07.jpg (46 characters)

Should be abbreviated to

ABTT~AKK01~VegCoverMap~03-Jan-07.jpg (36 characters)
ABTL~ANC03~SiteSurveyReport~02-Jun-07.doc (41 characters)
ABTI~EVS01~TrialData~23-Oct-07.xls
ABTL~CFF02~ReCircTankLayouts-Vs1~Feb-08.dwg
ABTL~CFF01~OxygenTanks-TopView~Nov-07.dwg

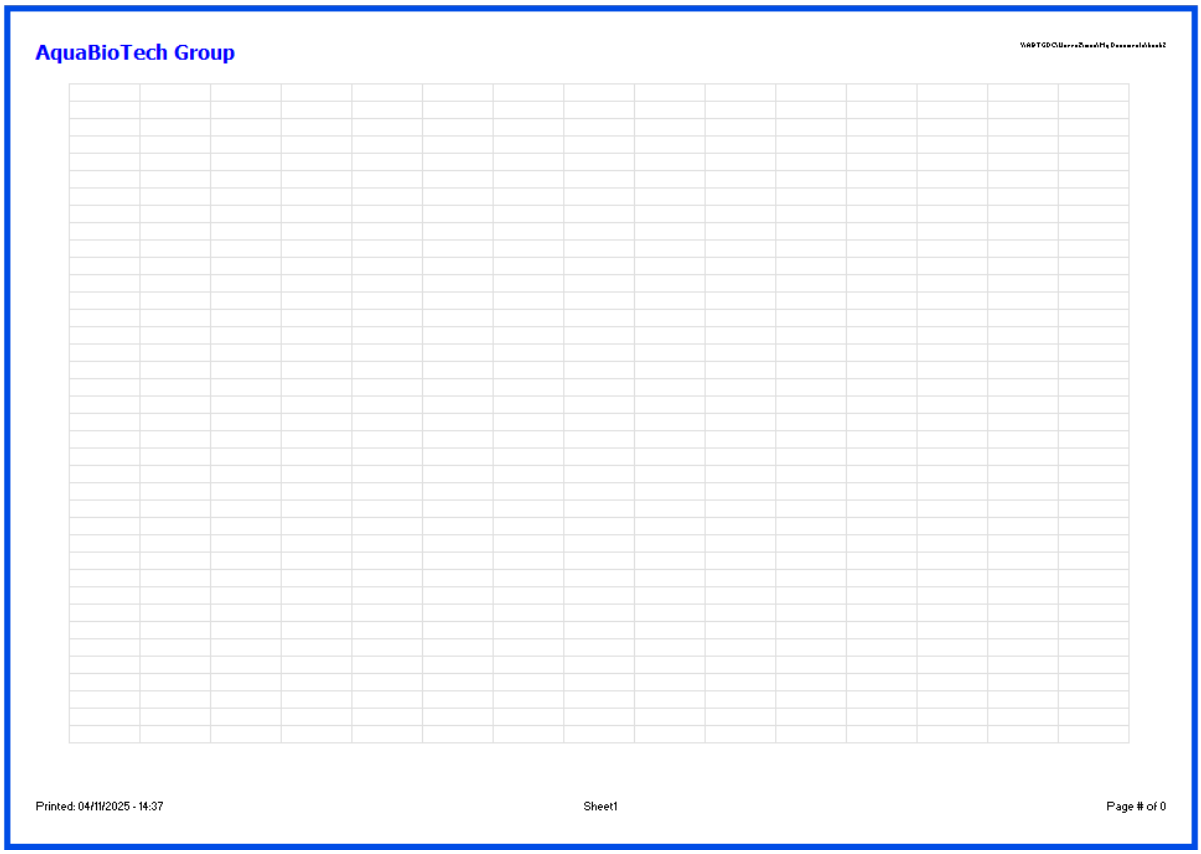
7.11. Document Formatting / Template Guidelines

7.11.1. File Templates

Word, Excel and PowerPoint have their own templates pre-installed, and they must be used all the time. If you need support, please consult IT Department or refer to the ABTG~MSWordHelpGuide~15~FEB~24 and ABTG~FormattingStyles2024~15~Feb~24

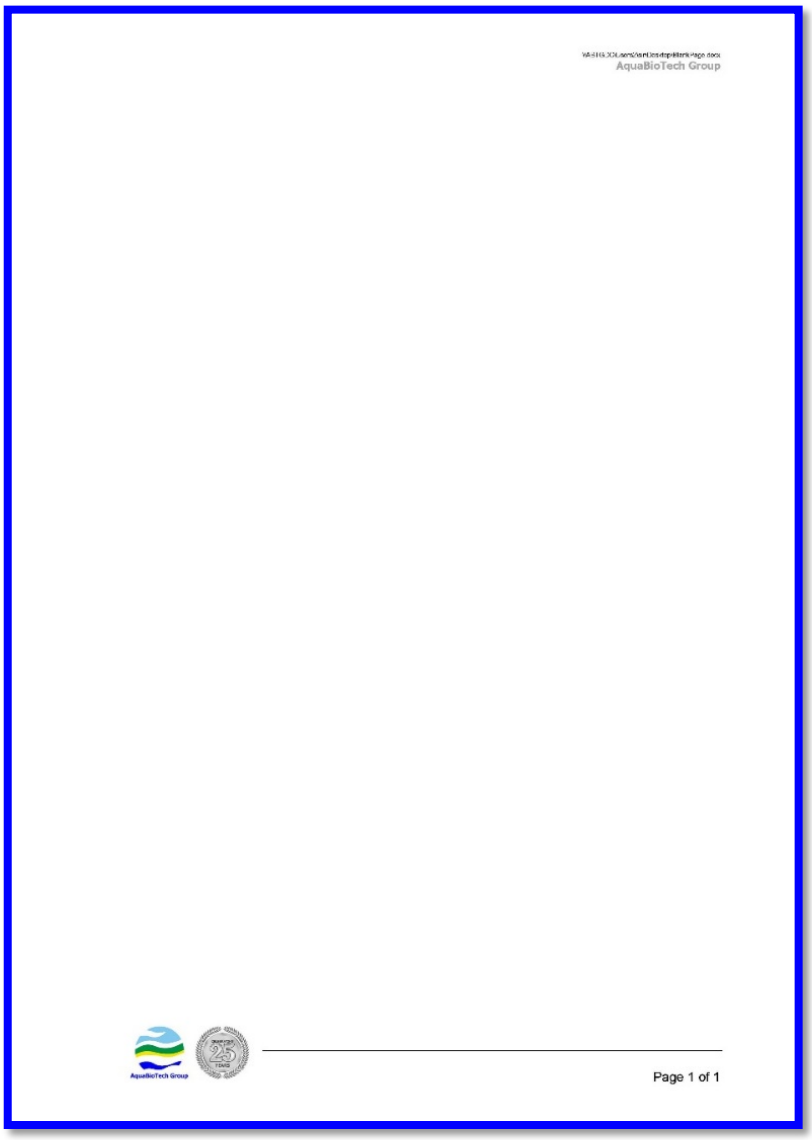
All files **must contain** the **updated** tracing code in the upper right corner of the header.

Excel Template (Landscape version) *(Open at startup)*



Word Template

(Blank Document)



PowerPoint Template (Default Theme)

8. Logo Use

8.1 Incorrect Uses of the Logo

Avoid the unacceptable applications of the ABTG Logo illustrated below:

DO NOT add any shadows to the logo

DO NOT place any objects behind the logo

DO NOT add any elements to the logo

DO NOT rotate the logo

DO NOT change the specified colours of the logo with the modification of brightness and contrast

DO NOT distort / revise/ alter the logo or separate elements within logo

Please note: Customised logo could be used only when there is necessity based on specific requirements and approved by corporate communications and marketing.

9. Exemptions and Violations of Policy

Exemptions from Policy

The Board of Directors may, from time to time, grant exemptions to a user or department from compliance with this policy, provided that a valid business justification exists.

Violations of Policy

Any violation of this policy may result in disciplinary action, up to and including termination of employment.