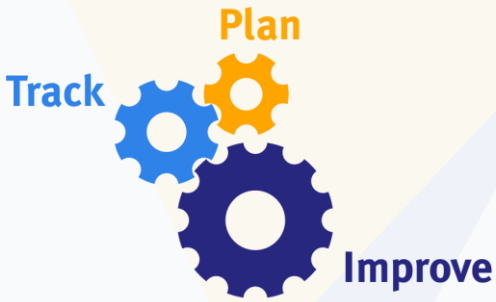
Timemaster

Standard Operating Procedures



Equisys Timemaster Ltd
Units 15B & 15C Marina Court
Castle Street
Kingston Upon Hull
East Yorkshire HU1 1TJ
United Kingdom

Tel: +44 (0)1482 588532

www.equisys.com

Contact: Support, **timemastersupport@equisys.com**

Contents

Version history

30 April 2018 - First issue (Matt Norris)

1. Introduction

This document outlines Equisys Timemaster Support's standard operating procedures in relation to the way we handle your data.

2. Support Requests

Note: Refer to Appendix 1 for a pictorial representation of this section.

2.1 Transferring Data

We will only ask for data based on a support query raised by your Timemaster administrator.

Most support queries can be dealt with without us requesting your data. However, there are occasions when we will need some, or all, of your data to be sent to us. This is needed for our support team to analyse the underlying data to resolve the support case.

Two options are available. The support team will assess the problem and then make a request to your Timemaster administrator the relevant information to be sent.

- XML files – These are produced by your Timemaster administrator and are protected by encryption on the user's PC, and in transit via email.
- Databases backup files – We will only request a backup of your data in extreme circumstances. Database backups must be compressed and encrypted with a password before being send to us. Passwords must be sent via a separate channel.

2.2 Processing of Data

On receipt of your data, we will process it as follows;-

- **XML files**
    1. Decrypt the encrypted XML file sent to us
    2. Use our custom Import program to convert the XML file into T-SQL
    3. Run the script against one of our databases
    4. Run a script to anonymise staff data
    5. Close the Import program – thus destroying on screen data
    6. Close the T-SQL script window – thus destroying the on-screen T-SQL script
    7. Destroy the decrypted XML file from disk
- **Database backup files**

    Note: Encrypted database backup files will be transferred by a protocol agreed by both Equisys Timemaster and yourselves if they are to be intermittently stored in the cloud. These files will be destroyed once we transfer them onto our secure servers.

    1. Decrypt the encrypted database backup file
    2. Restore it on one of our secure SQL Servers
    3. Run a script to anonymise staff data
    4. Destroy the decrypted database backup file on our server

3. Storing of data

3.1 On Premises customers

We will not store any decrypted data on our servers. Any data stored is either encrypted or anonymised.

3.2 SaaS customers

All data is stored on our secure hosted servers and further protected by SQL security credentials.

SQL backups are made each night and are encrypted ahead of transfer to our internal servers where they are stored as part of our disaster recovery procedures. They are then deleted from our hosted servers once this transfer is complete.

4. Connecting to customer sites remotely

4.1 Storage of connection details

Details of how to connect to client's servers are stored in a secure vault.

4.2 Visibility of your data

On Premise

When investigating a support case, we may need to log into your Timemaster application. This may expose us to personal identifiable information(PII) of your staff. We recommend your Timemaster administrator creates a separate Timemaster user account with restricted access rights for Timemaster support use. Please refer to the Timemaster - Administrator guidelines for processing personal data document for more details.

SaaS

No accounts set up by Timemaster Support have administration privileges. Nor do they have access rights assigned to them that could expose us to PII.

4.3 Support Analyst's responsibilities

We will only view data relating to the support case. No other data is obtained or viewed.

5. Updating SaaS Software

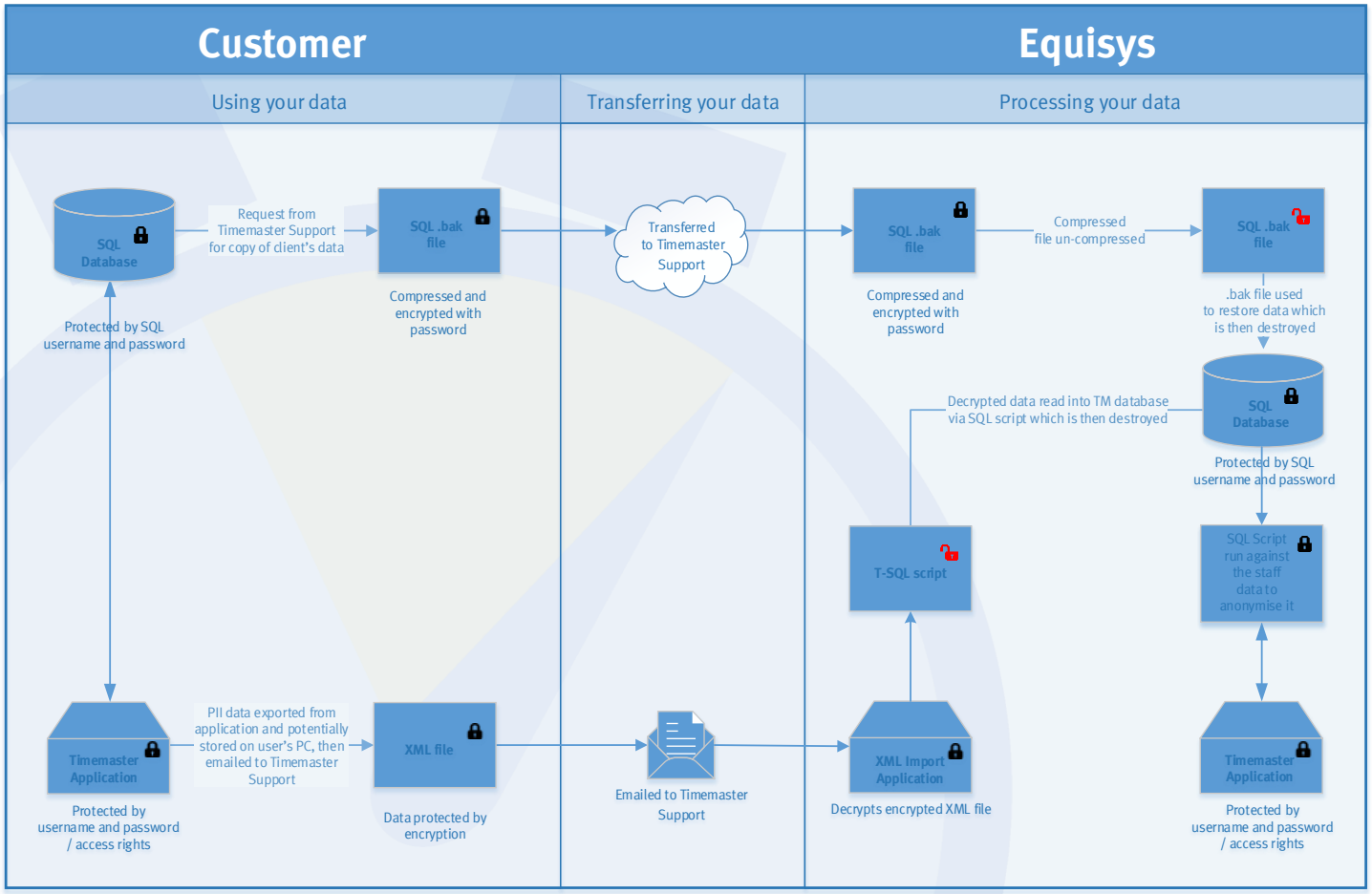
When a new version of Timemaster in made available we will;-

1) Send an email notification out to the Timemaster administrators at each of our SaaS customer sites. This email will notify recipients of the time and date when the upgrade will take place.
2) We will take a backup of client data before updating your software – this will adhere to the principles outlined in the Storing of Data section (above).

3) We will then proceed to perform the process of upgrading the software.
4) Finally, we will send a notification email out to the same recipients notifying them that the upgrade has been completed.

Note: No data is viewed during the upgrade.

Appendix 1


Customer
Equisys
Using your data
Transferring your data
Processing your data
SQL Database
Request from Timemaster Support for copy of client's data
SQL .bak file
Compressed and encrypted with password
Protected by SQL username and password
Transferred to Timemaster Support
SQL .bak file
Compressed and encrypted with password
Compressed file un-compressed
SQL .bak file
.bak file used to restore data which is then destroyed
SQL Database
Protected by SQL username and password
Decrypted data read into TM database via SQL script which is then destroyed
T-SQL script
SQL Script run against the staff data to anonymise it
Timemaster Application
Protected by username and password / access rights
PII data exported from application and potentially stored on user's PC, then emailed to Timemaster Support
XML file
Data protected by encryption
Emailed to Timemaster Support
XML Import Application
Decrypts encrypted XML file
Timemaster Application
Protected by username and password / access rights