Reactec Analytics – Technical & Security Arrangements

Introduction

Reactec Ltd has a cloud based data reporting system as part of the Reactec Analytics Platform. The Reactec Analytics allows Hand Arm Vibration exposure data, as collected while using Reactec's HAVwear and RASOR products, to be automatically transmitted to a cloud based data server which also hosts a web based reporting tool to allow customers to access and review reports of their exposure data.

Reactec Ltd is committed to managing Information Security and Data Protection issues within a formal management system framework and has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage. This is achieved through;

- Adopting an information security policy
- Measures to protect computers (firewalls, anti-virus software, back-ups)
- Controls on access to information (password protection on files and server access, encryption of laptops, and ensuring that personal data is not stored unprotected on mobile devices)
- A business continuity/disaster recovery plan (Reactec takes regular back-ups of its computer data files which are stored off-site)
- Training all staff on security systems and procedures, and only allowing staff access to the information they need to do their job
- Detecting and investigating breaches of security should they occur

Overview

- Refer to Diagram 1 for an overview of the system architecture.
- The Reactec Analytics Platform cloud servers that host customer data are managed by Microsoft Azure who are a leading provider in the UK and host a wide variety of well-known corporate and local Government sites as well as central government departments.
- Data is transmitted from the Docking station (DST) to which HAVwear are docked typically twice daily. This can be changed by customers if a different duration between transmissions is required.
- All data is encrypted during transmission and is transmitted using a secure VPN between the Docking station & Wireless Logic (the GPRS mobile phone service provider) and between Wireless Logic and Microsoft Azure. SSL encryption is supplied between Microsoft Azure and the Reactec web application (the Analytics Platform).
- Reactec allocate Docking stations to a customer account when purchased direct, or when hired from a third party. Transmitted data is automatically allocated to that customer once the Docking station has been allocated to a customer account. Only once allocation is confirmed will the Docking station function and transmit data to the confirmed customer

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com
Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

account. A deallocation process is gone through at the end of any hire, and as a failsafe, the Docking station validates that the allocated customer account matches that on the cards used to sign out HAVwear modules: if there is a mismatch, HAVwear modules will not be signed out so no data will be collected.
The deallocation process is slightly different for HAVmeter Base stations in that a deallocation card must be used to off-hire the equipment.

Access to Data

- Reactec do not have access to personal data which includes employee ID numbers and names. Reactec are only allowed access when authorised to do so by the Analytics Software Administrator of the employee's company. The system default setting is to deny Reactec access to personal data (this is Reactec's preferred option). The data owner may grant Reactec access to personal data for a limited time or permanently – typically for a limited time to assist with technical support.
- Reactec do reserve the right to use aggregated, depersonalised data for analysis purposes.
- Every customer company is responsible for data access by their own authorised users. Company employee access can be limited to viewing specific data/reports within specific groups. There are three types of company users –
    - "System Administrator" users can manage and control data and user access.
    - "Group Administrator" users can manage data, users and view reports for specific groups only.
    - "Reports" users can view reports only.
- As the Data Controller the customer remains responsible for data access requests by employees and for long term storage of employee data. Reactec maintains the database and reports can be extracted from the database at any time during the subscription term.
- Upon termination of use of the Reactec Analytics, Reactec can provide the customer with an export of raw data records from the database. However it is the customer's responsibility to store this data beyond the date of termination.
- It is advised that customer Data Controllers have a data policy covering use of and access to personal data, and that permission has been obtained from employees for the processing of personal data. It is also strongly recommended that a user access and data protection policy is created specifically for the Reactec Analytics.

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com
Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

What connects or is connected to the technical architecture?

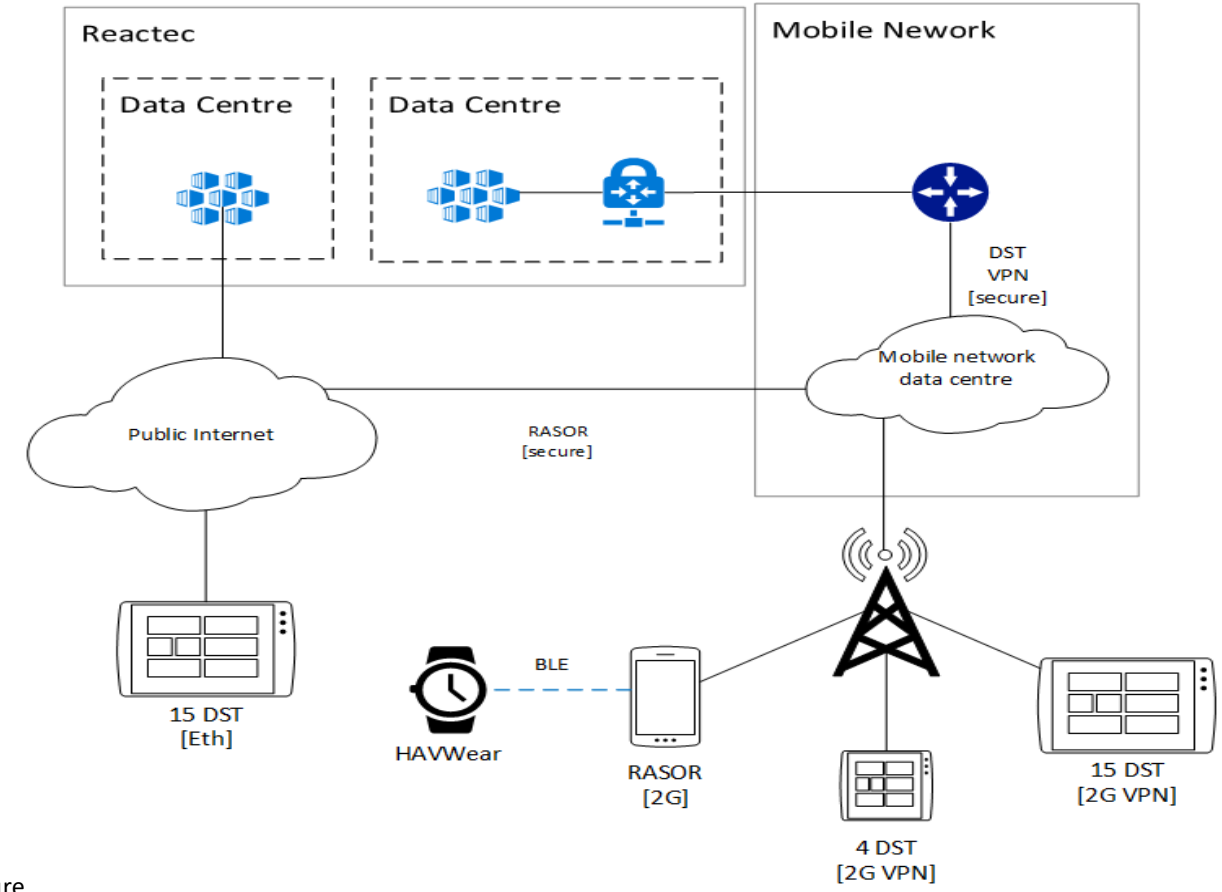


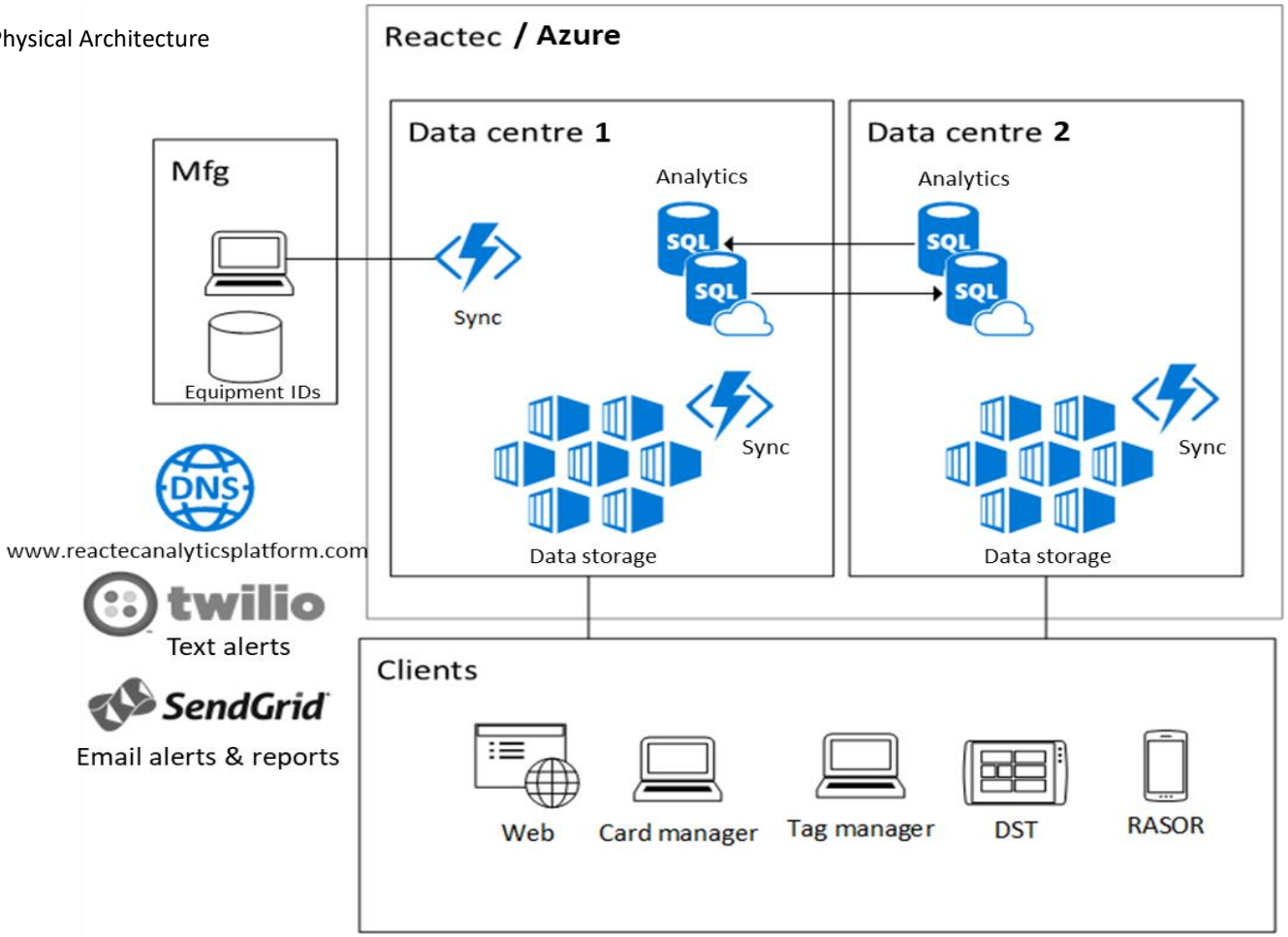
Diagram 1: Comms Architecture

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com

Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

Reactec Analytics –
Technical & Security Arrangements

Diagram 2: Physical Architecture



Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com

Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

Common FAQs regarding technical & security arrangements

1. What is the technical architecture of the system?

Refer to Diagram 2. The Reactec Analytics is cloud hosted software, located on a Windows 2016 virtual server hosted by Microsoft Azure (https://azure.microsoft.com/en-gb/support/trust-center/). The contracted Data Centres are in the UK (UK South and UK West), and backups are to sites in the UK. Azure have additional data centres but the location of Reactec's virtual servers cannot be changed to outside of the UK without prior notification to Reactec of any proposed relocation.

2. Who is being made responsible for what, where?

The Customer is the data controller, responsible for creation of data, for ensuring accuracy of input data, for sharing and using that data and for archiving of data in the form of reports. The Customer can set up three types of user within the Analytics Platform: a company administrator can upload data, create and manage users, and view reports across the entire account; a group administrator can do the same only for the group specified (enables local management at say, depot level) and a reports user can only view data reports for their assigned groups.

Reactec Ltd are data processors responsible for management of the database, database backups, and destruction of information upon the Customer leaving the platform. Reactec have system administrators who manage allocation of hardware to the Customer (ensuring data allocation to the correct customer account) and who can provide technical support. The platform has been designed such that Reactec staff cannot view personal data without the permission of a Customer user, and such permission is revocable.

Microsoft Azure host the cloud server and have no data processing ability. Their responsibility is solely to manage the server architecture. Microsoft Azure do not have knowledge of the quantity, value or use of the data Reactec store within the Azure Cloud system.

3. What legal and regulatory requirements have been taken into account?

Refer to Reactec standard T&Cs and the software license for the Analytics.

Reactec Ltd is registered for Data Protection with the ICO as a data controller, reg: Z9674723. The registration includes provision of an internet service to Reactec's clients.

Microsoft Ltd is registered with the ICO, reg: Z6296785. Although the general registration includes the Trading and Sharing of Personal Information, Microsoft makes a specific undertaking in relation to its Azure services that it will not use customer data, or derive information from it for advertising or data mining purposes. Microsoft Azure have adopted the world's first code of practice for cloud privacy, ISO/IEC 27018.

Both Reactec and Microsoft Azure process data in accordance with the provisions of the Data Protection Act 2018 and the EU General Data Protection Regulation 2016/679 (GDPR), and Reactec's

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com
Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

contractual terms with customers incorporate a data processing agreement setting out the permitted data processing.

The contracted server locations for live data are within Azure's data centres in London and Cardiff. Backups are also stored with Azure in London. Reactec has entered into a contractual Geo restriction with Azure to restrict data storage to the UK.

If the customer uses the automated reports emailing service (see section 12), then data may be transferred outside of the EEA. This is because the third party mail relay service, operated by SendGrid Inc (part of Twilio Inc) uses servers in the USA, Japan and India as well as the UK to relay emails. However, personal data transfers via the SendGrid Services to outside the EEA/UK, either directly or via onward transfer, are protected under US Privacy Shield and the Standard Contractual Clauses.

4. Are suitable people overseeing the system?

Microsoft Azure are ISO/IEC 27001:2013 certified and are certified ISO/IEC27017:2015 compliant for IT Security controls (based on ISO27002 for cloud services).

Reactec are Cyber Essentials Plus certified and ISO9001:2015 certified (Cert. No. FS597197) and the company's information security and data protection policy and procedures are incorporated into the Quality Management System (QMS), which is subject to internal audits and external audits by BSI annually. Reactec staff training processes are also part of the QMS.

Reactec performs Identity checks (passport and visa status), employment history checks (references) and Basic Disclosure criminal record checks on all new recruits.

5. What evidence is there that the people are aware of their responsibilities and are carrying them out?

System configuration and system operations procedures are incorporated into the Reactec Quality Management System, including a procedure that sets out staff responsibilities relating to the Analytics Platform. Information security procedures are audited internally annually as part of maintaining Reactec's ISO 9001 certification.

As part of their induction to Reactec, new staff are made aware of the Information Security suite of documents in our QMS. Staff must be trained on administration of the Analytics Platform and the arrangements set out in the Analytics Software Data Handling Procedure, prior to being given administrator rights within the Analytics Platform (the CEO signs off any new user authorisations).

7. What are the known threats and vulnerabilities to the system?

Penetration Testing on the web application and network infrastructure is conducted annually by Context IS, who are CREST approved and highly accredited information security specialists. The penetration tests include:

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com

Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

- Reconnaissance
- Authentication, authorisation and session related testing
- Encryption analysis
- Information leakage tests
- Input validation analysis
- Application logic testing
- Network mapping
- Automated vulnerability assessment

A redacted copy of the latest report is available on request.

Microsoft Azure also conducts Penetration Testing on the Azure service offering, this is conducted using FedRAMP methodology by independent contractor Kratos Technology & Training Solutions Inc.

Reactec maintains and manages the development cycle of the software in-house, but the testing environment is also hosted by Microsoft Azure. Penetration Testing will be performed after any development of the software that is likely to significantly affect the security of the Analytics.

8. What personal data fields are held within the system?

RFID Card Mandatory Fields: Employee ID*; Operator First Initial; Operator Last Name; ELV limit; EAV limit.
*The Employee ID must be unique to the customer but the nature of the ID reference used is up to the customer: it could be a payroll reference for example.
RFID Card additional optional fields: CSCS ID; Operator First Name; Date of Birth; National Insurance Number;
If CSCS cards are used then ELV & EAV is stored for up to 3 employers (each employer can only read their ELV and EAV for the individual).
Online Portal data fields: all of the above fields, plus vibration exposure points data.

9. What uses will you make of our personal data?

Reactec Ltd will not access operators' personal data without authorisation from the customer, and will do so only to assist with technical support issues. Reactec will not use or sell on personally identifiable data. Reactec reserves the right to make use of Aggregated Data, which means data, including Operator Vibration Exposure Data, which has been anonymised such that it is highly unlikely to identify a living individual or individual customer, that is tracked across time and which is not confined to one Customer or Authorised User. Such data can provide important improvements to the management of HAVS.

10.Who and what determines who has access to what, where?

Refer to the Reactec Analytics Platform Software Administration manual for information on what the company administrator, group administrator and reports user roles entail (available to download from http://www.reactec.com/support). It is the responsibility of the Customer to decide which staff members have access and at what level of role. Reactec policy is to direct any requests for changes in users to a customer administrator and, by exception, any request to set up a new user on

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com
Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

behalf of the customer will not be actioned by Reactec unless written authorization from the customer is obtained.

Within the "cloud" server assigned to Reactec by Microsoft Azure each user population is logically separated by the customer login. Each customer login is associated with a username and email address that must be unique within the database.

Regarding attacks, a user is locked out for 30 minutes upon three unsuccessful login attempts, making brute-force attacks on passwords very slow (access can be reinstated by an administrator). The Analytics password specification is supplied in Appendix 1.

Reactec has an internal procedure as part of its QMS setting out separation of duties relating to the Reactec Analytics Platform and application of least privilege to the least number of staff. Reactec System Administrators and support staff cannot view operator personal data within a customer account unless the customer gives permission via the User Permissions page visible to customer administrators. Such permission can be given temporarily and can be revoked. An audit log records what is accessed during periods where permission has been given.
For Reactec developers, RDP Access to the live Azure server is restricted to two IP addresses, is configured to only allow clients using NLA, and a valid username / password is then required to log onto the server. Those two addresses are static IP addresses at Reactec's office in Edinburgh and the home address of our lead software developer, as he is entitled to home-working using his work laptop.

There are no privileges granted to suppliers and sub-contractors, other than temporary access from time to time to enable Context IS to conduct penetration testing. Microsoft Azure have adopted the world's first code of practice for cloud privacy, ISO/IEC 27018, and restrict virtual access to customer data for its employees based on business need by role-based access control, multifactor authentication, minimizing standing access to production data, and other controls. Access to customer data is also strictly logged, and both Microsoft and third parties perform regular audits (as well as sample audits) to attest that any access is appropriate.

11.What protects data at rest from unauthorised access?

All server data backups are stored in an encrypted state. All databases are encrypted at all times, both when in use and in backups.
Access to backups, databases and server data is restricted both by IP address and credential authentication methods.

12.What protects data in transit from unauthorised access?

Data is stored within the Docking Station (or Base station) until it is transmitted. All data is encrypted during transmission using AES 128 CBC. The static key is within the Docking Station software, and a unique key is generated using the serial number of the Docking Station that is transmitting the data. At present, there is no known practical attack that would allow someone without knowledge of the key to read data encrypted by AES when correctly implemented, and the

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com

Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

U.S. Government considers the design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level.

An IPSec VPN is used between the Docking Station & Wireless Logic (the GPRS mobile phone service provider), and between Wireless Logic and Microsoft Azure.

SSL encryption is supplied between the end user and the Reactec web applications.

Email alerts and automated emailing of reports can be set up by customer administrators. The Reactec Analytics Platform uses a third party mail relay service (SendGrid Inc) to send emails to registered users of the Analytics Platform. SendGrid relays the email without saving a copy, and will by default try outbound TLS v1.1 or higher when attempting to deliver email. This means that if the recipient's email server accepts an inbound TLS v1.1 or higher connection, the email is delivered over a TLS encrypted connection. If the receiving server does not support TLS, the email will be delivered over the default unencrypted connection. The Customer should check their email settings to determine whether emailing of reports containing PII meets their data security requirements.

Reactec engage a sub-contracted IT consultant to manage and control the server in Reactec's office, but they have no access to the live Reactec Analytics or to the Microsoft Azure servers.

13.What contains any data leakage?

Customer administrators have the ability to export data from the Analytics (at which point it becomes unprotected), and can give and revoke access to the system for additional users.
The most likely source of data leakage is via poor management and control of user access. Reactec therefore recommend best practice is to keep the number of full administrators within the system to a minimum and ensure user access is reviewed regularly and revoked when staff leave.

The system will allow a user to set up a report to be emailed to users automatically on a daily, weekly or monthly basis. This option is pre-populated with the email addresses of customer users authorised to view that group's data. It is not possible for Reactec to restrict the user email addresses to exclude, for example, non-company addresses, but only a customer administrator can add new users to the system; a user cannot amend his own email address; and an email address can only be used once within the entire system.

14.What would be your recommendations for

a) how long we keep HAVs data collected electronically for?

All data collected by the system is automatically uploaded into the database. The hardware will keep a temporary file of data in the Docking station until such time as the next successful upload takes place, at which point it automatically deletes the data file from the hardware.

b) how long we keep data available in the Analytics Platform software for?

The database is designed to be a complete record of employees' HAV exposure over time, and provides useful trend analysis, both to evidence actions by employers to reduce overall employee

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com

Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

exposure over time, and to assist with monitoring equipment vibration levels for maintenance purposes. The data would be at risk of being unrepresentative if selected data sets were deleted. Therefore the entire data set will remain available in the software for as long as subscription to the Analytics is maintained.

c) how long we keep data outside of the software for?

Arrangements should be made for the long term storage of reports outside of the software, as these form an employer's permanent record of information. Reports can be stored as pdfs or in paper form. The length of time that these reports are kept depends on your own record storage policy.

15. What enables an initial secure system configuration and on-going accurate data processing?

Reactec software engineers manage patching, patches are tested on an internal test server (based in Reactec's office) and then on a staging server (Microsoft Azure) before going live. Potential vulnerabilities are regularly alerted to Reactec by Microsoft Azure.

Live data is not used on the test servers, fake test data is generated internally using test equipment. Exceptionally if a customer issue can't be determined or replicated using the test data, the live data may temporarily be copied to an encrypted drive on the developer's computer for debugging purposes and will be immediately removed once the issue has been identified.

16. What is the System Development Lifecycle (SDLC)?

Reactec's software development life cycle is controlled through its ISO9001-compliant design procedures (the same process is used for all products, leading to greater synchronization of product development). The Analytics software and firmware is currently subject to at least quarterly releases of updates. The Docking station has been designed such that firmware updates can be pushed down via the Analytics Platform connection, ensuring that all hardware can be updated remotely. Most of the updates are for maintenance purposes, but will occasionally include new features which will be communicated to customers via alerts and newsletters.

Reactec tests software upgrades on a test server that imitates the database prior to live release, and that enables integration with the hardware to be fully tested.

17. What configuration review and change management processes are in place?

The Reactec QMS includes a Design Development procedure and a universal change management process that is controlled through the use of Issue Reports and Change Orders.

18. What are the arrangements for periodic backup and system resilience?

Reactec use the Microsoft Azure managed back-up service. Backups are encrypted.
A full system snapshot is taken daily on a 7-day rotation. A file level backup of data files, website files and sequel database files is taken every hour.

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com

Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

19.What are the incident response and business continuity arrangements?

Reactec have a Business Continuity Plan that is audited annually.
A Support Services Policy setting out Reactec's incident response arrangements is available on request.

Azure Cloud Servers reside in world-class data centres, with a 99.9% Network Uptime Guarantee (excluding planned or emergency maintenance) and Incident Response Management processes.

20.What instrumentation to detect, monitor and audit events is used?

Microsoft employs intrusion detection, denial-of-service (DDoS) attack prevention, regular penetration testing and data analytics and machine learning tools to help mitigate threats to the Azure platform.
Reactec system and event logs are managed manually at present, but an automated SIEM solution, EventLog Analyzer, is currently under test and will be implemented once fully approved.

Reactec Ltd
T: +44 (0) 131 221 0920
F: +44 (0) 131 229 9051
E: info@reactec.com
W: www.reactec.com

Company Number: SC221428 Registered Office: Vantage Point, 3 Cultins Road, Edinburgh EH11 4DF, United Kingdom VAT Registration Number: 804 120 877

Appendix 1:

Reactec Analytics Website

PASSWORD SPECIFICATION

CONTENTS

SUMMARY

This document details the constraints and rules for User passwords on the Reactec Analytics Platform Website.

CREATED BY	VERSION
William McAinsh	1.0

Reactec Analytics – Technical & Security Arrangements

PASSWORDS

COMPLEXITY

The password must be a minimum of 8 characters with a least 1 character from each of the categories below:

- Upper case letters
- Lower case letters
- Numbers

FREQUENCY

The password must be changed at least once per year.

LOCKOUT

After 3 unsuccessful logon attempts, a User account will be locked for 60 minutes, this can be reset by an Administrator with relevant privileges.

RESET

A User can request a password reset link to be emailed to them if they have forgotten their password.

From the website, an Administrator can send a reset password link or resend the welcome email if the User account hasn't been used yet.

CHANGE

A User can change their password at any time once logged on.

PASSWORD SECURITY

STORAGE

All passwords are secured using a one way hash before being stored in the database. Passwords are never stored in clear text and cannot be recovered by the system.

TRANSPORT

When passwords are reset or changed, the website always uses a secure HTTPS connection.

Passwords are never sent via email or any other method.

INACTIVITY

If a User has not been active for 30 minutes, they will automatically be logged out of the website and will have to re-enter their credentials.