UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

TRP's Information Security Management and Data Protection for SaaS

creating raving fans

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

Contents

Change Control

Version	Author	Approved By	Date	Notes
10	Simon Moore		31/07/2017	Branding Update
9	Simon Moore		18/08/2015	Risks updated.
8	Simon Moore		18/08/2015	ICO Registration Updated. Address updated.
7	Simon Moore		04/10/2012	SaaS/iCloud update
6	Simon Moore		11/03/2011	
5	Simon Moore		27/01/2011	
4	Simon Moore		09/09/2010	
3	Simon Moore		04/08/2009	ASP update
2	Simon Moore		04/07/2009	
1	Simon Moore		11/07/2007	Rebranded from Fitronics

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

Objective

Provide customers with assurance that the software services and systems provided by The Retention People (TRP) will be managed effectively, securely and responsibly.

Provide assurance that the customer's informational assets will be protected against all internal, external, deliberate and accidental threats.

Where TRP installed systems necessarily interface with existing customer systems and networks this document will provide additional assurance that the TRP system will not adversely affect existing networks and systems and existing systems will not adversely affect the TRP system.

Please note this plan does not fully detail what the customer should do to implement their own Information Security Management System. This plan details only the TRP owned systems and services that deliver the Software as a Service (SaaS) offering and where those systems/people communicate with the systems at the customer site or utilize the informational assets of the customer.

Security Policy

- The Policy ensures that
    - Information will be protected against unauthorized access
    - Confidentiality of information will be assured
    - Integrity of information will be maintained
    - Availability of information for business processes will be maintained
    - Legislative and regulatory requirements will be met
    - Business continuity plans will be developed d maintained and tested
    - Informational security training will be available for all employees
    - All actual or suspected information security breaches will be reported to the informational security manager and will be thoroughly investigated.
- Procedures exist to support the policy, including virus control measures, passwords and continuity plans
- Business requirements for availability of information and systems will be met

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

- The informational Security Manager is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments
- Compliance with the information security policy is mandatory

Overview

EngageCEM, Nutrition Complete, Clubcount, Insight NPS, TRP Identify, TRP Interact, TRP Process, TRP Targets, TRP Mobile, TRP Fitness, TRP GroupX, TRP Complete, TRP Digital, TRP NPS, TRP Benchmark and future modules for TRPs SaaS product are modules of an online web application (Software as a service) containing membership information, used for tracking member risk, interactions, processes, retention, fitness and staff.

The SAAS modules can be accessed online via via a web browser.

Web Services may be used to transfer membership and attendance information from existing Membership systems. There are 3 versions in current use.

Push versions

1. TRP Integrator - The reference web service client written and maintained by TRP for a number of membership systems. The reference web service client uses TRP's standard web service.
2. Membership systems own integration, written and maintained by the membership system and communicating back to TRP's web service which may be the standard or specific for the membership system

Pull versions

3. TRP use a membership system specific client to pull data from a web service written and maintained by the Membership system.

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

Security Management Plan

1. Organisational Security
    a. Information Security Infrastructure
        i. All technical security issues are reported to the CTO. All other security issues are reported to Operations Director. These Directors will arrange emergency meetings for security issues that need resolving.
        ii. TRP act as the customer agent (a data processor) in accordance with the Data Protection Act (The Retention People's registration number is **ZA135015**).
    b. Security of External Access
        i. External access to TRP systems is not permitted at this time either on site or at remote sites.
        ii. Where third parties are used such as IBM systems integrators for installation or system repair/replacement, these third parties are not given access to TRP systems which will be accessed remotely by TRP once internet access can be established. Hardware that cannot be repaired via the remote internet access method are replaced and TRP upload the backup data.
2. Asset Classification & Control;
    a. The servers, databases, services and associated networking together with backups are the only assets of TRP that might affect TRP contractual obligations. These are classified (e.g. in the event of failure) as having:
        i. low impact on customers systems (the customer systems and business will run without them)
        ii. a medium impact on customer's staff (as the TRP service they may wish to use would be unavailable). These risks are mitigated - see documentation below.
        iii. a medium impact on customer's members (as the internet service would be unavailable). These risks are mitigated - see documentation below.

    b. Sensitivity analysis of information held by server.
    Classification:

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

CLASS A
Highly sensitive information which, if its confidentiality, integrity or availability was compromised, would be likely to result in critical damage such as the loss of life, serious financial loss or significant breakdown of confidence in the government or judiciary.
CLASS B
Sensitive information which, if its confidentiality, integrity or availability was compromised, would be likely to result in serious damage such as the loss of civil liberties, significant financial loss, or serious breakdown of confidence in a Committee or Department.
CLASS C
Information which, if its confidentiality, integrity or availability was compromised, would be likely to result in minor damage such as small financial loss, or embarrassment to a Committee or Department.
CLASS D
Non-sensitive information which, if its confidentiality, integrity or availability was compromised, would not be likely to result in any real damage occurring.

IMPACT & CLASSIFICATION RISK	Critical Damage A	Serious Damage B	Minor Damage C	Little / No Damage D
Loss of Confidentiality			X	
Loss of Integrity				X
Loss of Availability				X

c. Risk Management

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

Server

Risk	Probability of occurring	Result	Probability of result	Mitigation	Result probability	Time affected
Power Failure	0.01%	Loss of service	0.001%	N+1 Redundant Power UPS and Generator mitigates likelihood of result. System maintainable on backup power for more than a week.	0.00001%	Duration of power failure
	0.01%	HD corruption	0.001%	UPS prevents. Secondary Backup SAN mitigates Hourly Backups, Daily offsite Backups allow rebuild.	0.00001%	Time to rebuild from backup 1hr-1day
Network failure outside of TRP control	0.01%	Loss of service	25%	Notify relevant network providers of fault. Multiple redundant links with different providers mitigate.	0.0025%	Duration of network failure
Server security compromised	0.01%	Loss of service, data loss etc	50%	Deny remote access on server and firewall. Erase and reload from backup.	0%	1hr-1day
System Failure	0.01%	Loss of service, data loss etc	100%	Typically the virtual server will be transfer automatically to an alternate node within a few seconds. Provision replacement server and recover from hourly snapshot backups.	1%	5sec (alternate node) 1hr (re-provision from hourly snapshot) 1day (full rebuild)
Loss of connectivity to customer site	0.01%	Stale data, i.e. shows data from last sync	100%	Determine fault and fix	1%	Depends on fault

Risk	Probability of occurring	Result	Probability of result	Mitigation	Result probability	Time affected
Power Failure (server running integration client)	0.01%	Loss of service	100%	UPS (if present) will retain service for a short time and protect against surges and brown outs. TRP service will resume on reboot with no loss of data as integration "state" is maintained (assuming database integrity is ok)	1%	Duration of power failure
	0.01%	Database corruption	10%	UPS (if present) prevents. Normal recovery tools should be used to recover the database(s) into a working state.	0.001%	Duration of power failure + recovery time
Network failure outside of TRP control	0.01%	Loss of service	100%	Notify relevant network providers of fault. Integration client will detect failure of network and provides diagnostic tools. Data flow will resume once network restored. (Retry time 15 minutes)	1%	Duration of network failure
Client PC security compromised (when logged in)	0.01%	Unrestricted access to data covered by data protection Act	50%	It would be time consuming to extract significant amounts of data. The data is of limited interest or value. Data deleted or modified maliciously can be recovered from backups.	0.5%	Duration of access to Client PC. Max 24 hours before automatic logout
PC Failure	0.01%	Loss of service	100%	Replacement PC and recover from backup	1%	Less than 48hrs
Membership database server security compromised	0.01%	Unrestricted access to data covered by data protection Act. (This is outside TRPs control)	50%	Possible unrestricted access to the membership system database which may include financial information.	0.5%	Duration of access to Client PC.
Membership database server security compromised	0.01%	Unrestricted access to the web service software allowing the sending of invalid/malicious data to TRP web service.	50%	TRP can block access. WS is designed to survive sending of incorrect/malicious data. Backups allow roll back and recovery of data prioir to change	0.5%	Duration of access to Client PC. Or lock out by TRP which ever comes sooner. Max data loss/corruption 1 hours worth to previous backup.

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

Membership Server Failure	0.01%	Loss of service	100%	Replacement PC and recover from backup of membership system	1%	Less than 48hrs
Data interception	0.01%	Obtaining passwords and membership data	1%	SSL encryption protects from data interception.	0%	0
Cross Site Scripting /CSRF, Click Jacking, Host Header Validation	0.01%	Compromise other users by inserting malicious content into information viewable by others	1%	System has built in protection for Cross Site Scripting, Click Jacking, Host Header Validation and CSRF for example to strip tags/code that could be used maliciously.	0%	0

Customer site (note: these are not assets of TRP).
Membership database server where Web Services provide push/pull access to member data for TRP SAAS

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

3. Personnel Security;
    a. All TRP employees are required to keep all confidential information (customer or otherwise) confidential under their contract of employment and job description.
    b. Employees sign a personal security declaration committing them to
        i. Comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant.
        ii. Only use data belonging to client for the purpose for which it has been authorised;
        iii. Deposit all data sets within specified and access-restricted folders inside the secure Fitronics network;
        iv. Keep data for no longer than necessary and destroy the data set, or return it to the client by registered mail to a named contact, once the purpose for which it was retrieved has been completed;
        v. Only share access to any data sets with other employees of Fitronics Ltd who have completed the personal security declaration or Partners/Suppliers who may have cause to process such data sets in the cause of carrying out relevant work on behalf of Fitronics Ltd and that have been bound in writing by the terms of this declaration.
        vi. familiarise themselves with the security policies, procedures and any special instructions that relate to use of the Government Connect when delivering services to clients; and
        vii. Acknowledge that use of any such Government Connect network facilities may be monitored and/or recorded for lawful purposes; and
        viii. Acknowledge that communications sent or received by means of Government Connect may be intercepted or monitored.
    c. Potential employees are assessed to ensure they will meet the security obligations of their position.
    d. In the event of an employee leaving passwords, security keys etc are changed and systems checked to ensure no security issues.
    e. All TRP staff are bound by any confidentiality agreements of TRP and will be required to additionally sign any such confidentiality agreement a customer presents for that purpose.

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

i. For avoidance of doubt this includes Personal Commitment Statement for GSi and related documents of customers.

f. Staff are trained in security aspects relevant to their position, including legal responsibilities regarding information covered by the data protection act.
g. Staff have a duty to report and document security and other technical incidents.
h. Incidents are logged in a database together with fixes and mitigation and other pertinent information for the avoidance of future issues.
i. Security and technical incidents can be reported to the customer automatically at their request via email (their email will be linked into the reporting database and emailed whenever a relevant customer event/incident/fix occurs) or notified in person only when significant events occur.
j. All TRP employees are contractually required to adhere to the acceptable use policy.

4. Physical and Environmental Security;
    a. Physical and Environmental Security
        i. Server
            1. Our secure data centre environment gives TRP's dedicated servers access to a high-speed internet connection through multiple providers, 24/7 security, plus a fully redundant power system.
            2. Access control requiring swipe-card, multiple digit PIN, finger-print plus accurate weight matching, ensuring absolutely no access to unauthorised personnel.
            3. Denoco climate controlled environment
            4. Air Conditioning
            5. FM-200 gas fire suppression system
            6. APC X UPS, with Backup Generators (30day run time)
            7. Redundant Tier 1 connectivity
            8. Full CCTV coverage
            9. 24*7*365 Security guards
        ii. TRP equipment at Customer site
            1. Responsibility of customer to restrict access to equipment, cabling and utility supplies. TRP can advise.

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

5. Communications & Operations Management;
    a. System operating practice
        i. Most maintenance jobs (e.g. backup) are tested automated procedures.
        ii. Where human intervention occurs the procedures are documented.
    b. Security (and other) Incident Management
        i. Incidents, work assignments and fixes are recorded in a database, relevant and interested parties are emailed.
    c. Segregation of Duties
        i. Management of and execution of certain activities are segregated to prevent accidental or deliberate misuse of systems. Typically all work is managed by someone in higher authority to the executor
    d. Separation of Development, Test and Production Environments
        i. Development, Test and Production systems are all separate systems at TRP.
        ii. All Production systems are fully tested with a burn in test and by TRP test staff prior to installation
        iii. On request a server can be configured with a second Test system for testing updates and changes to connected third party systems (e.g. Torex) prior to installation. Changes are then implemented on the test system before being put on to the production system. This is in addition to the testing at TRP.
    e. Systems Planning, Acceptance and Implementation
        i. Capacity planning. TRP assess the requirements when specifying a server for a customer. These are monitored throughout the life of the server. If additional capacity is required in the future the server will be replaced or upgraded under the maintenance contract. In the case of our SaaS cloud systems capacity can be upgraded on demand.
        ii. Contingency plans. The TRP system is not usually regarded as a critical system for business operation. Consequently the contingency plan essentially consists of a replacement server/virtual server being installed using the backup on the server. The time period for this is in the contract (typically 48 hours). In the case of our SaaS cloud systems, spare physical nodes are available across two data centres to seamlessly take over. Failing that backups can be restored to a new instance or physical server.

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

iii. Configuration Management: All changes to the systems are logged and reversible. Changes to production systems require the Technical Manager's agreement and where they may affect the customer, the relevant project manager who will contact the customer as appropriate.

f. Protection Against Malicious Software
   i. The systems used do not use operating systems with a significant history of "in the wild" viruses or Trojans and minimal security issues of which few have ever been exploited "in the wild".
   ii. Protection against Viruses and Trojans. Despite its inherent security the system is configured to negate the affect of any such infection. It is protected by stringent security controls, encryption, passwords and firewalls from infection. Additionally regular security audits and intrusion detection is run to identify anything suspicious. The systems do not currently have web browsers and so are immune to threats delivered via infected websites and emails.
   iii. Protection against security exploits. While these are a rarity on the systems used, the systems are patched against any such known exploits that may affect the system. Firewalls are used to mitigate the risk of an unknown exploit. Unused services on a system are disabled or removed as appropriate to additionally reduce the threats.
   iv. Where a system stores any documents or files that might be transferred to the customer's computer systems from our software and could potentially contain viruses/trojans harmful to a windows system (e.g. Word, Excel) these are checked for viruses.
   v. Additional protection of the customer network from the TRP system can be provided by a firewall under the customer's control. This would prevent the spread of any infection to the customers systems.
   vi. TRP recommend both firewall software (in addition to any hardware firewalls) and virus software be installed on all customer computer systems (and will be supplied on systems provided by TRP).
   vii. TRP can advise on the relevant security risks introduced by customer computer systems with direct or indirect access to the internet. Particularly where they may not have had such access prior to the installation of TRP.

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

g. Environment Maintenance
    i. Security Copies Of Data are held on the TRP Server for recovery purposes, this includes current and some historic copies. Allowing for complete or partial data recovery
    ii. Logs of all operations are maintained
    iii. All faults are logged
    iv. Environment guidelines are the same for any computer equipment.
        1. The equipment should be sited in a place where it will not be knocked, kicked or suffer undue vibration e.g. not under a desk
        2. The temperature should be around room temperature, excessive heat or cold should be avoided and equipment to maintain a safe working temperature installed if excessive heat or cold might occur.
        3. Air moisture content should not be excessive. The system should not be sited near running water.
        4. Adequate ventilation. If a cupboard is used it must be ventilated to prevent heat build up.
        5. In the case of TRP physical servers they are located in dedicated data centres with controls in place to far exceed all of the above.

h. Network Management
    i. TRP controlled networks are regularly checked for unauthorised connections.
    ii. If wireless is used at a customer site the latest and strongest encryption standards are used to protect that network's traffic and prevent unauthorised use.
    iii. Networks under the control of the customer should be checked by the customer.

6. Access Control;
    a. Access control to the TRP systems
        i. Direct access (i.e. login) to the server is only permitted by TRP designated personnel. The TRP system is a black box product with no end user serviceable parts or software beyond that provided by the management and kiosk interfaces.
        ii. Access to the Management System is restricted by a login and password. The login is a 5+ digit (randomly generated) number and

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

the password is any string of more than 4 characters. It is strongly recommended that the customer site impose a password creation policy to protect their members. TRP have checks to confirm the password meets such a policy. This includes minimum password length, password reuse restrictions, complexity restrictions and strength of password restrictions.

iii. Privileges are assigned to users of TRP software can only be equal or lower than the assignor's privilege level.
iv. Additional authentication information will be required on occasion.
v. An incorrect password 3 times will lock that account for 60 mins (Configurable in duration and number of times).
vi. Persistent abuse from an individual IP address will lock that IP out of the system (Configurable in duration and number of times).
vii. All logins, failed logins, and lockouts along with IP addresses and other information are logged.
viii. Passwords for instructors to access the system are chosen/set/reset by the customer and consequently can be set to meet their requirements. If you wish to enforce password construction rules please let us know. This includes minimum password length, password reuse restrictions, complexity restrictions and strength of password restrictions.
ix. All login sessions are cancelled after 24 hours and on logout.
x. Temporary Cookies (browsers do not write these to disk) are used to store the system session ID.
xi. The session ID is generated by an algorithm based on the RSA algorithm
    1. protecting against someone creating a fake 'authenticated' cookie
xii. User terminal security is managed by the customer
    1. TRP would recommend using windows security features to lock the screen after a period of time for any PCs in public areas.
xiii. The system is protected against SQL injection attacks at several levels.
xiv. Access to the server other than via the web interface is only via SSH (RSA 128 bit encrypted, key locked)
xv. The server system is additionally protected at various levels against hackers and audit trails are kept.
xvi. User sessions can be SSL encrypted
    1. SSL protects against Man in the middle attacks

UK & Rest-of-World
18 Monmouth Place
Bath, BA1 2AY

Email: admin@trpcem.com
Tel: +44 (0) 845 621 2001

North America
67 Froehlich Farm Blvd
Woodbury, NY 11797
USA

Email: northamerica@trpcem.com
US Tollfree: +1-800-951-8048

2. And cookie interception attacks.

b. Web Service access control (push methods)
   i. Web Services is accessed via SOAP over HTTPS
      1. SSL protects against Man in the middle attacks by encrypting data in transit
   ii. Dedicated commercial SSL certificates and IP address are available as chargeable add ons
   iii. TRP generated SSL certificates are used as standard.
   iv. Web Service client is locked to the fingerprint of the SSL certificate (which is specific to the server)
      1. Prevents sending of any data to a server not matching the certificate, further protecting against Man in the middle attacks and DNS attacks.
   v. Web Service client uses a customer specific login and password to send data to the TRP server
      1. Identifies and authenticates valid live customer sites
      2. Allows TRP to block individual customers
   vi. The Web service has application protection to prevent corrupt/malicious data entering the live database.
   vii. The database receiving the web service information is additionally protected at various levels from bad data and malicious attack.

c. Web Service access control (pull methods)
   i. TRP only recommend membership systems implementing web services over SSL or other encrypted connection
      1. SSL protects against Man in the middle attacks by encrypting data
   ii. TRP recommend membership systems implementing web services restrict access via passwords specific to their customers.
   iii. TRP will provide advice on any security issues they are aware of.