Information Governance Policy

Issue 5.1

Tim Kendall 21st May 2018

Version Control

Version	Date Issued	Brief Summary of Change	Owner's Name
V0.1	18/08/14	New document	Tim Kendall
V1.0	20/08/14	First issue	Tim Kendall
V2	17/03/16	Second issue	Tim Kendall
V3	30/03/17	Third issue	Tim Kendall
V4.1	15/03/18	The GDPR	Tim Kendall
V4.2	29/03/18	The GDPR +	Tim Kendall
V5	01/05/18	The GDPR++	Tim Kendall

Sign-Off

Issue	Date	Signature	Role
V1.0	20/08/14		Martin Woolley, Technical Director
V2	17/03/16		Martin Woolley, Technical Director
V3	30/03/17		Martin Woolley, Technical Director
V4.2	29/03/18		Martin Woolley, Technical Director
V5	01/05/18		Martin Woolley, Technical Director
V5.1	21/05/18		Martin Woolley, Technical Director

Contents

1. Introduction

This document describes tmwk's policy for information governance:

- In the context of contracts for the use of the spa Software as a Service, for the support of vulnerable people with accommodation-related needs,
- Particularly in relation to providers of services related to the National Health Service (NHS),

As an organisation providing Software as a Service with confidential personal data, tmwk are fully aware of the need to safeguard the personal identifiable data in the organisation using spa. tmwk currently has two employees who are also the organisation's directors, Tim Kendall and Martin Woolley. The employees, and individuals contracted to work for tmwk on spa in relation to NHS-related, and other, contracts, are aware of the Caldicott principles for personal confidential data that underpins information governance across the health and social care services:

1.1 Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

1.2 Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

1.3 Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

1.4 Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

1.5 Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

1.6 Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

1.7 The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

2. Information Governance Management

2.1 Responsibility

Tim Kendall, managing director at tmwk, is Information Governance Lead (IG Lead), and as such, takes responsibility for co-ordinating, publicising and monitoring standards of information handling within the organisation and for developing and implementing an IG improvement plan (also known as implementation or work plan). He also ensures that IG Toolkit (NHS Information Governance Toolkit) assessments are submitted as required.

Tim has overall and in-depth knowledge of tmwk and spa, as well as detailed understanding of the principles of information governance. He is also tmwk's contact with the Information Commissioner's Office. He is a Caldicott Guardian and sits on the UK Caldicott Guardian Council (UKCGC).

All staff are be made aware of their IG responsibilities. Specific new guidelines are:

- Awareness of importance of engaging in IG training, both formal and self-guided.
- Do not hold personal confidential information outside of spa (see more detail under Transfers below).
- Remove any existing confidential information as soon as possible and make contacts aware of policy (for example, use "Notice and Disclaimer") on email.

2.2 About the Policy

Everyone working for, or on behalf of, tmwk is aware of the policy stated in this document. Their signatures are captured on the form in Appendix I.

The IG Lead is responsible for the currency of this document, its review, annually or more frequently if required, and that it continues to reflect national NHS information governance guidance.

This policy is based on

- Information governance good practice as publicised by the NHS Digital.
- Data Protection legislation and good practice: tmwk are registered data controllers with the Information Commissioner's Office, reference Z1719113.
- Previous good practice applied at tmwk.

2.3 Contracts

All contracts with staff, contractor and third parties, in relation to spa's use as a service, contain clauses that clearly identify information governance responsibilities and compliance with this policy, or, in the case in particular of companies providing server hosting, those organisations are ISO 27001 certified (see Appendix V).

All organisations have a common law duty as well as a specific requirement under the Data Protection Act 1998 to ensure that confidential information is processed lawfully and protected from inappropriate disclosure. Breach of confidence, inappropriate use of patient/service user records or abuse of computer systems may lead to disciplinary measures including for loss of their tmwk contract.

tmwk apply the Confidentiality and Non-Disclosure Policy (see Appendix V) to all relevant working relationships, where not already covered by ISO 27001 certification to the satisfaction of commissioners.

tmwk have conducted a risk assessment of the technical infrastructure (see Appendix III), and have the following action plan to review existing contracts:

- Check existing contracts against all who have access to spa and spa infrastructure,
- Contact all organisations and individuals concerned regards agreeing to terms of policy, and
- Remove access and terminate relationship where Policy not agreed.

Any information governance breach is recorded by tmwk staff.

2.4 Training

All staff members are provided with appropriate training on information governance requirements: this is carried out using material from the NHS Digital and the Information Commissioner's Office (ICO). Evidence of the completion of this training is recorded (see Appendix VI). All new staff members, contractors or third parties are provided with training within the shortest feasible time of taking their post.

It is assessed that all tmwk staff require a full understanding of information governance principles and practices. The need for refreshing this training is assessed annually.

Resources recommended by the NHS Digital have been used for training, including "Data Security Awareness Level 1" and "The Role of the Caldicott Guardian" available on the Information Governance Toolkit website , as well as Data Security Awareness at the NHS Digital e-learning site.

3. Confidentiality and Data Protection Assurance

3.1 Personal Information

Personal information related to NHS and/or local authority contracts held by tmwk in spa is not shared, unless approved by the organisation using the spa service, directly contracted to the NHS and/or local authority. tmwk do not share the personal information in spa, other than with the organisation contracted with tmwk for use of spa where information relates to the fulfilment of that contact. tmwk are fully aware of the requirements of the Data Protection Act 1998 and of Common Law, as well as the forthcoming GDPR and Data Protection Bill 2018 (see section 5). Any disclosures in the public interest, or where a Court Order or statutory basis is provided as justification, requires the approval of the IG Lead. tmwk prevent personal information from being used for purposes other than those contracted for.

3.2 Confidentiality Audit Procedures

spa, tmwk's Software as a Service, keeps a full audit trail of all actions carried out by users. tmwk hold no identifiable personal information outside the spa system, which is entirely hosted on ISO 27001 certified servers at UKFast data centres in Trafford, Manchester.

Included in spa is a facility for recording complaints by people supported using spa and by agencies involved in that support. Breaches in confidential are reported using the Information Incident facility (see Appendix III) and serious incidents are recorded in the log (see Appendix VII).

The IG Lead takes responsibility for the investigation of confidentiality events. tmwk comply with confidentiality audit procedures of the organisation providing the NHS-related service.

3.3 Data Processed outside of the UK

No data is processed outside of the UK by tmwk. All tmwk services are hosted within the UK. It is the responsibility of the IG Lead to ensure that this remains the case.

3.4 New Processes, Services, Information Systems and Other Relevant Information Assets

tmwk ensure when new processes, services, systems and other information assets are introduced in relation to spa that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements.

Testing of new processes, services, systems and other information assets includes cases to test the impact on information quality, security, confidentiality and protection. The IG Lead is aware of any new development of the spa service to assess its information governance impact.

All tmwk release documentation includes specific consideration of the information governance implications of changes.

The following stages are reflected in project and release plans and controls, and an iterative approach is taken up to deployment so that possible breaches can be identified in testing:

- requirements analysis;
- functional specification;
- system architecture and design;
- creation or selection of software;
- testing;
- assuring fulfilment of project objectives;
- assuring quality;
- acceptance and implementation;
- operation and maintenance.

Development and test systems are separated from operational systems.

Access to development tools and system utilities is restricted to relevant authorised tmwk personnel only and are not accessible from operational systems: there are separate user IDs.

Test systems are subject to similar access and security controls as operational systems.

There is ample spare capacity on tmwk's servers which are hosted by UKFast on a server and network with ISO 27001 certification.

Changes to spa and to related processes, services, systems and other information assets, with their information governance implications, are communicated through the following means:

- Email,
- spa User Forum (http://spauser.forumotion.com/) and
- spa used internally within tmwk.

3.5 Transfers

All transfers of personal and sensitive information are conducted in a secure and confidential manner.

The spa websites are protected by Secure Socket Layer (SSL) trust, authentication and encryption: spa cannot be used except through "https". All logins, passwords and security questions for users are separately encrypted in a distinct security database.

All transfers of data carried out by tmwk outside of the spa application are done using SFTP, which uses the secure SSH protocol.

At tmwk identifiable personal confidential information is **not**:

- transferred by email (see Appendix IX for Email Notice and Disclaimer)
- stored by tmwk as documents or data on other than tmwk's secure ISO 27001 servers
- transferred by fax
- printed and stored as hard copy
- recorded at telephone message or virtual meeting recordings

Should a breach occur, the respective recordings, documents and/or data will be deleted immediately and the breach will be logged. Where information is printed or written, that paper will be shredded immediately.

tmwk's servers provide a "safe haven" for data and documents, protected by firewalls that only allow access for specific tmwk logons from a small number of specific IP addresses. Information moves to and from the "safe haven" using spa or through SFTP.

Where a decision is made to continue to transfer unencrypted information, this needs to be specifically signed off by the IG Lead and, where necessary, notified to the *commissioning organisation* with a description of how the information will be protected.

From time to time, tmwk use GotoMeeting to conduct virtual meetings with spa users, or GotoMyPC internally for remote access to workstations: both are services provided by Citrix Online. Citrix Online's privacy policy includes the following: "In-session information collected during meeting, webinar and training sessions is protected by the use of end-to-end encryption and only accessible by the authorized users, organizers and participants. "In-session information" includes all screen sharing data, keyboard/mouse control data and text chat information. This information is never exposed in unencrypted form while temporarily resident within Citrix Online's communication infrastructure servers or during transmission across public or private networks."

Before transferring information, tmwk, with our clients, answer the following questions based on the Caldicott Principles:

- is there a valid need to use/disclose confidential information?
- is it necessary to use confidential information?
- has the minimum possible confidential information been used?
- do the proposed recipients need to know all of the confidential information?
- have all staff members been informed of their responsibilities for protecting confidential information?
- is the use of confidential information lawful?
- does the stated purpose for transferring the information make it more important that the information is shared rather than withheld?

To comply with the provisions of the Data Protection Act 1998, personal information is not retained in spa for longer than is necessary to carry out the purpose for which the information was provided: the period of retention may be defined by the organisation using spa.

4. Information Security Assurance

4.1 Access Control

The spa Software as a Service supports appropriate access control functionality, and documented and managed access rights are in place for all users of these systems. tmwk's security policy is as stated in this document. User administration is through the IT user administration function of the service provider using spa.

Each user of spa has an individual logon (see Appendix III) and their actions are fully audited. Access to spa outside of tmwk is only possible through the spa website.

In spa there are two levels of access with regard to security:

- Officer, who can only see cases on the service to which that officer is allocated.
- Manager, who can maintain services and, if necessary, look at cases across services. Managers in spa should only those with staff management positions in the organisation using spa.

A spa help sheet is provided for the technical setup of the initial access to spa.

When a user logs on to spa for the first time, that person sets up security questions (see Appendix III). These questions need to be answered when the user accesses spa for the first time from a particular device. They are required to answer the questions again if they do not access spa regularly from the same device.

A written procedure is established with the organisation using spa for the authorisation of access requests and for the removal of access. Access controls are reviewed annually.

All users logging on to spa for the first time need to set their passwords. This is covered in tmwk's familiarisation of key users, to be passed on in training for all users. Passwords must be at least six characters long. All passwords are stored and transmitted using encryption.

If spa is not used for 40 minutes, it times out. Users receive frequent reminders to save data. tmwk staff lock access to their workstations when they are not using them for periods during the day.

tmwk are also aware of responsibilities under the Freedom of Information Act 2000, including the duty to disclose. Freedom of Information requests are handled initially by the IG Lead.

Our domain names are hosted on secure DNS servers minimising the risk of loss of service.

tmwk run quarterly security reviews with UKFast, involving deep tests of the spa webserver infrastructure: the site aims to maintain the highest rating, "A", using Qualys SSL Labs SSL Server Test. Further penetration and infrastructure testing by third parties is carried out on a regular basis.

tmwk Limited are Cyber Essentials certified, certificate number 7498763290882269 (see Appendix X).

tmwk use cookies on the spa and tmwk websites to help us improve, promote and protect our services. See Appendix XI for our cookie policy.

4.2 Networks

Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely. The server network hosting the spa website and database has ISO 27001 certification (tmwk can provide the certificate on request). Only tmwk staff have access to this network. No other networks come under tmwk's control. spa itself is used over the Internet and security mechanisms are described in the Transfers section above and below.

4.3 Mobile Computing and Teleworking

Although spa can be accessed over the Internet, no personal customer (person supported by the organisation using spa) data is stored on mobile devices. Otherwise access controls to spa are described above. Initially after three months and then annually, audits are carried out of all tmwk resources outside of spa to check personal confidential data is not held outside of spa, whether as emails, documents or data files.

4.4 Information Asset Register

The system configuration for spa is diagrammed in Appendix VIII. tmwk's system configuration document includes all key information, software, hardware and services relevant to the spa Software as a Service.

Investigation and identification of all remaining assets relevant to information governance is planned as follows:

- Identify all hardware and software in use on servers and networks, and in use in applications relevant to spa.
- Add details to the tmwk system configuration document.
- Schedule reviews of the information asset register, initially in three months and subsequently annually.

4.5 Restricted Access

Unauthorised access to the premises, equipment, records and other assets is prevented. For tmwk's spa servers this is covered by ISO 27001 certification. tmwk staff only are able to access servers from specific IP addresses using SQL Server, Remote Desktop Connection and FTP. tmwk hold no personal confidential information locally.

Should unauthorised access occur related to the spa infrastructure, the following actions should taken:

- Take all reasonable action to ensure security of spa assets (data and documents, in particular)
- Notify hosting providers (UK Fast in the case of spa's servers)
- Document the incident as a breach of security and information governance
- Subsequently identify action for such access not to occur in the future

4.6 Business Continuity

There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions:

- tmwk have separate web server and database servers: the website server is configured to run as a database server if required and, likewise, the database server can be used as a web server.
- tmwk provide a copy of the database of the organisation using spa overnight if requested (encrypted and transferred using SFTP).
- Backups of data are taken every night to location outside of the production network.
- There have been no issues with performance, no loss of data and no security breaches in more than five years of spa's use.

4.7 Incident Management and Reporting Procedures

There are documented incident management and reporting procedures: there is a Serious Incident Log (see Appendix VII). Further incidents are recorded using spa internally at tmwk (see Appendix III, which includes output from a Contact report including information governance near-misses).

Responsibility for managing information incidents is the IG Lead's. Where appropriate, the incident is escalated using the IG Toolkit Incident Reporting Tool.

Staff are aware that it is essential to report information governance incidents and near-misses.

4.8 Data Protection Measures

All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures. It is tmwk policy to hold identifiable confidential information only on our securely hosted servers, covered by ISO 27001 certification and protected by security measures stated above. See Appendix V Confidentiality and Non-Disclosure Policy for tmwk staff and contractors.

Where, for whatever reason, an organisation ceases to use spa, all personal confidential data is deleted from the spa infrastructure using a defined “off-boarding” process. Related documents are also removed.

Where it is the policy of an organisation using spa to remove customers after a pre-defined period of time, tmwk have processes for the expiry of data. There is planned improvement to this and the “off-boarding” process through closer integration of data and document connections.

tmwk have reviewed, and continue to review, data protection policies in the light of the forthcoming General Data Protection Regulation (see Section 5).

5. The GDPR, tmwk and spa

5.1 Introduction

This section makes use of IGA guidance, developed by the national GDPR (General Data Protection Regulation) working group, chaired by NHS England. This section will be integrated with the rest of the document after 25th May 2018, the GDPR implementation date. Under the GDPR with regard to spa, tmwk are the data processor. With regard to contact information of individuals at organisations using spa held by tmwk for support purposes, tmwk are the data controller.

5.2 Information Asset Register

tmwk will provide an Information Asset Register to each organisation using spa. As well as the system diagrams in this document, the information asset register is comprised of:

- System reports in spa, and
- Database documentation

Audit logs and backups of those audit logs record of all processing carried out in spa.

Input to spa is through use of the website, and through specific uploads and modifications for organisations using spa. This input is recorded:

- In the audit log, and
- In a maintenance log in the database.

Output is through use of the website, including through the use of spa's reporting facilities. Where an organisation has a specific interface involving output from spa, documentation on this will be provided to the organisation.

5.3 Legal Basis for Processing

As with the Data Protection Act, under GDPR a lawful basis is needed for processing and these are listed within Article 6 of the GDPR. For health and care, most likely to be used is 6(1)(e): "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". There is also (b): "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

In order to process special categories data (sensitive personal data such as health data) an additional lawful basis is required. These are under Article 9 in the GDPR, specifically 9(2)(h): "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services…". The GDPR confirms the wide interpretation of this condition. Thanks to the ICO for advice on this subject.

Using consent as the basis for processing has several complications under the GDPR: the suggestion is that the above approaches are preferable if applicable. Where applicable, the consent process is the responsibility of the data controller and outside of the direct scope of spa and tmwk, being applied before the person is recorded on spa.

Where tmwk hold contact information for support or administrative purposes of individuals at organisations that use spa (such as names, emails and telephone numbers), this "processing is necessary for the performance of a contract to which the data subject is party" and "is necessary for the purposes of the legitimate interests pursued by the controller". Where tmwk wish to provide a contact to a third party as a reference for spa, the consent of that contact will be required and sought by tmwk. The contact information will not be used for other purposes.

5.4 Data Retention Rules

Dependent on an organisation's data retention policies, maintenance routines are applied to an organisation's data to remove data that is beyond the period of retention. Consideration should be given to the risks of removing data and as to whether the data should be retained "in the public interest". Similar principles apply to the data subject's "Right to erasure", for which tmwk are able to provide the technical capability.

5.5 Data Security

tmwk are in the process of updating our entry in IG Toolkit (see reports), which will become the Data Security and Protection Toolkit later this year.

tmwk are certified under the government's Cyber Essentials scheme: see the Certificate in Appendix X.

tmwk apply "privacy by design" to each new release of spa.

5.6 Data Protection Officer

Tim Kendall is tmwk's Data Protection Officer.

5.7 Data Processor

Although data processors in the context of the GDPR, tmwk are currently registered with the ICO as data controllers. Under the GDPR, registration is not required. In the meantime, tmwk are maintaining our data controller registration for continued guidance and contacts at ICO (reference Z1719113).

5.8 Customer and Case Identifiers

tmwk undertake not to hold, or otherwise use, outside of spa, personal confidential data related to data subjects recorded in spa. There is sometimes a need to identify data in spa in communication outside of spa, such as in support emails between spa users and tmwk: currently the spa "customer id" and/or the "case id" are used for this purpose. It is appreciated that, under the terms of the GDPR, these anonymous identifiers themselves may be deemed personal data because it may be possible under some circumstances to identify the person in question outside of spa using associated information. Because is considered to be sufficiently important for the resolution of issues, and because the risk of loss of confidentiality is sufficiently low, it is currently the intention that these identifiers from spa are continued to be used in this context: staff at tmwk, organisations using spa, and any involved third parties will be made aware of the risk involved.

Appendix I. Responsibilities Grid

References Signatures against the roles below indicates awareness of the responsibilities of that role and agreement to take on those responsibilities.

Role	Person	Signature	Date
Information Governance Lead	Tim Kendall		29/03/18
All employees/contractors aware of IG Policy	Tim Kendall		29/03/18
"	Martin Woolley		29/03/18
"			
"			

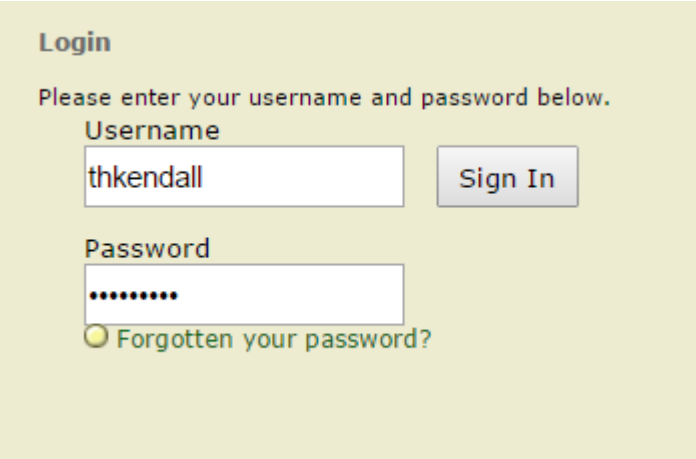
Appendix II. References

Description	Reference
Caldicott Review	https://www.gov.uk/government/publications/the-information-governance-review
The General Data Protection Regulation	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
The General Data Protection Regulation – ICO advice	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
Information Governance Alliance guidance on the GDPR	https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance
Information Governance Training Toolkit	https://www.igt.hscic.gov.uk/
Information Commissioner's Office	http://ico.org.uk/
National Data Guardian: Review of Data Security, Consent and Opt-Outs	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
Qualys SSL Test	https://www.ssllabs.com/ssltest/index.html
tmwk Limited	http://www.tmwk.co.uk/
UK Caldicott Guardian Council	https://www.gov.uk/government/groups/uk-caldicott-guardian-council

Appendix III. Screen Shots from spa

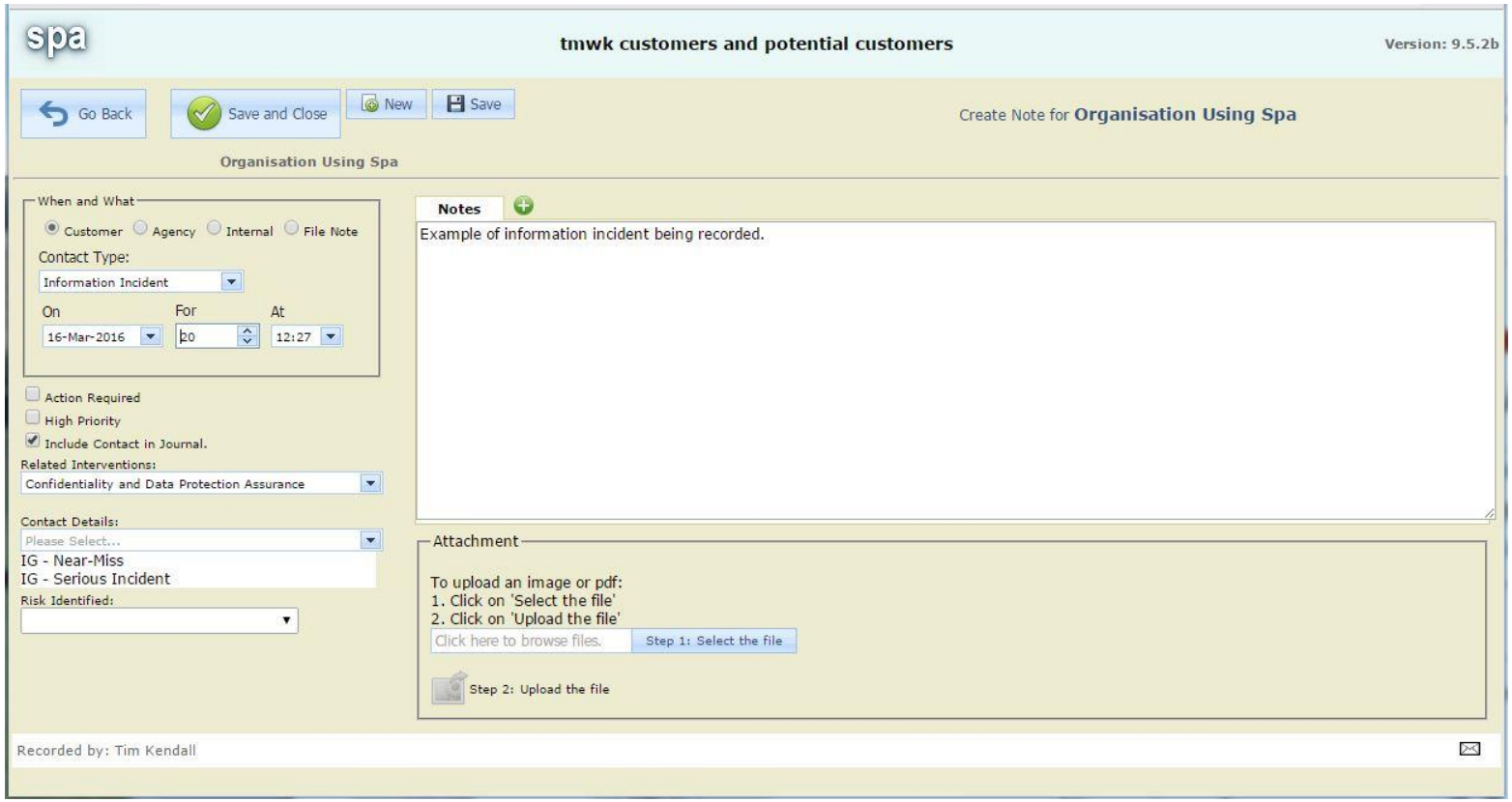
tmwk use a spa database to maintain their own records of customers and related processes and documentation, including information governance.

Logon and Security Questions



A message similar to the below is displayed when a new officer is added. The manager should inform the new officer of the initial security question answers, as well as the username and password. Note that the answers to the security questions are not case-sensitive.

Information Incident

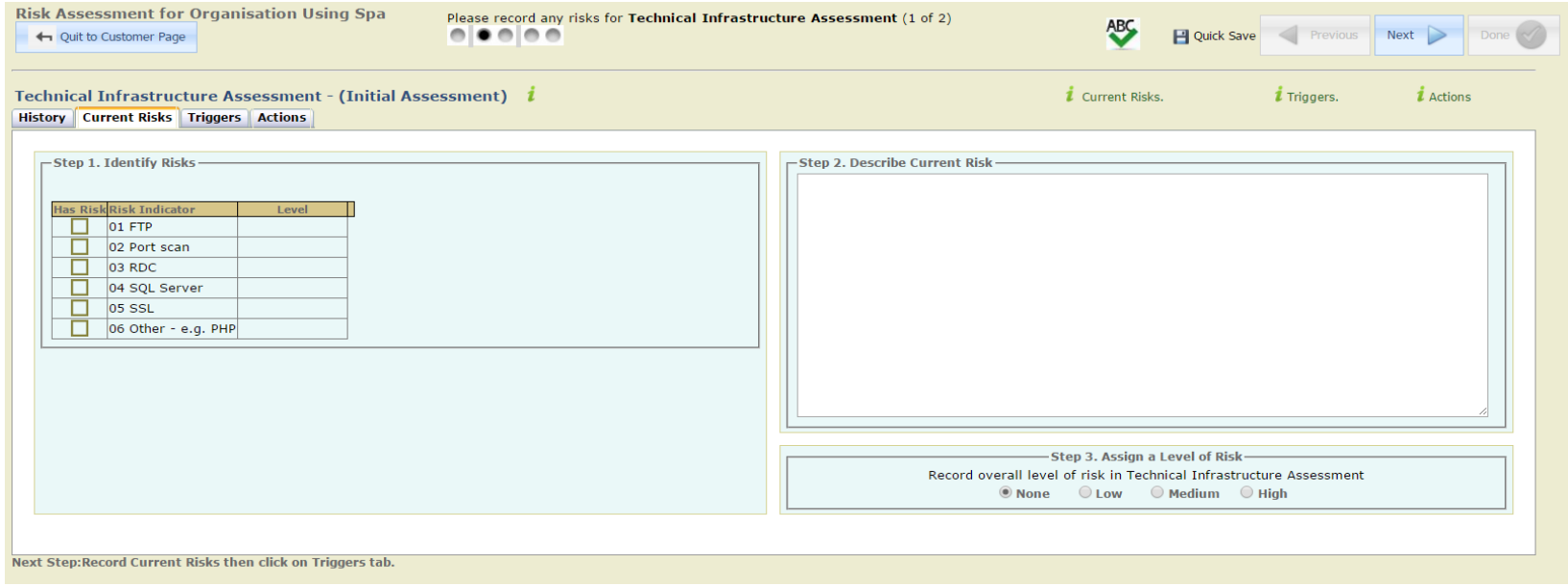


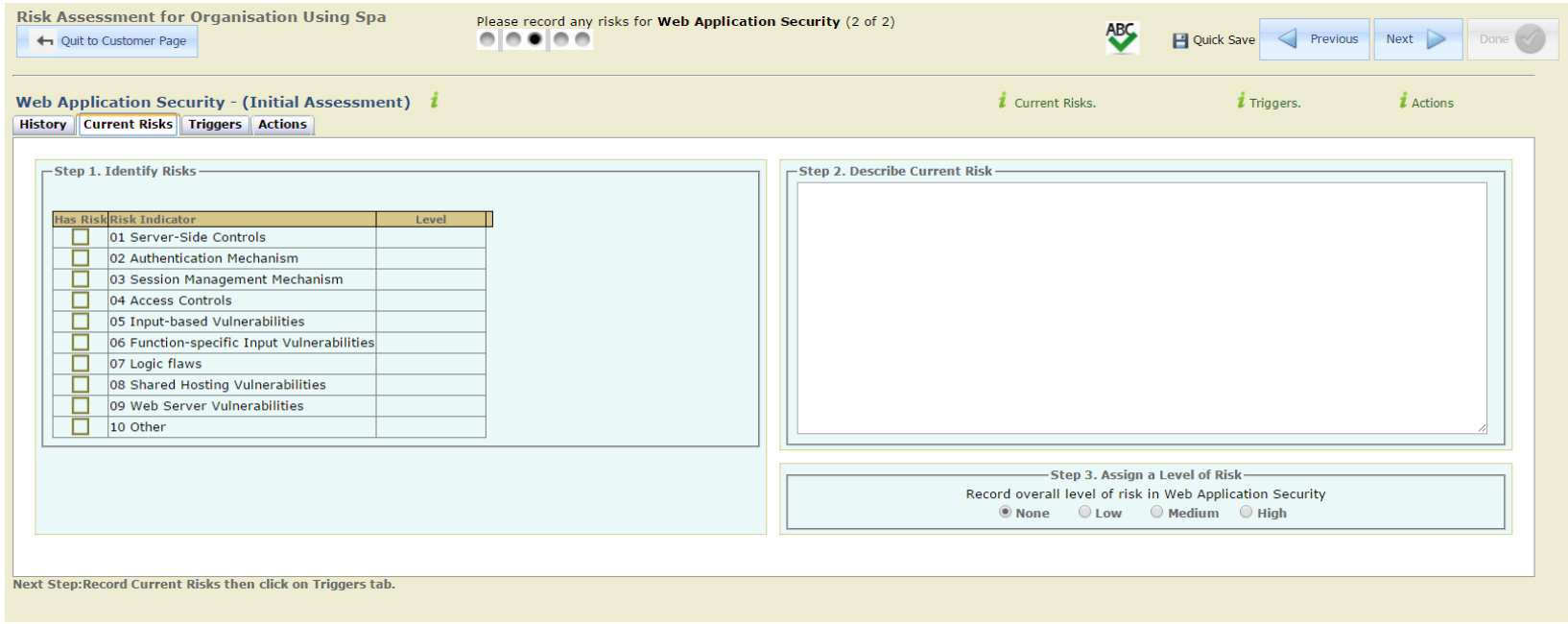
Contacts Report Showing Information Governance Near-Misses

Breakdown of all 721 Contact(s) by Contact Detail				
Gateway project	16	2		
Support - bug report	91	7		
Support - advice on front end usage	116	7		
New System Report request	55	5		
Request for new functionality	61	7		
Administration	81	8		
Support - correction of data	309	6		
Browser Compatibility	1	1		
Business knowledge	3	2		
Change Request	1	1		
Compliment	14	5		
Demo logon sent	4	3		
End of St Andrews	3	1		
Familiarisation	1	1		
IG - Information Governance knowledge in general	3	2		
IG - Near-Miss	12	4		
Interfaces	1	1		
Logout issue	1	1		
Marketing	1	1		
Mobile working	8	2		
Off-boarding	20	2		
On-premise spa	12	1		
Other - use this if you think a new one is needed	3	3		
Outcome Star licensing	11	3		
Sales	23	10		
Security / IG	4	3		
spa day	15	8		
Support - downtime	8	5		
Support - extension of use	3	2		
Support - issue with outcome forms	42	3		
Support - local database copy	3	1		
Support - login problem	6	3		
Support - performance issue	9	3		
Support - security issue	2	1		
Technical	28	5		

This was for the current reporting year, from 4th April 2016 to when the report was run, 29th March 2017.

Security Risk Assessment




Risk Assessment for Organisation Using Spa
Quit to Customer Page
Please record any risks for Web Application Security (2 of 2)
Quick Save
Previous
Next
Done
Web Application Security - (Initial Assessment)
Current Risks.
Triggers.
Actions
History
Current Risks
Triggers
Actions
Step 1. Identify Risks
Has Risk
Risk Indicator
Level
01 Server-Side Controls
02 Authentication Mechanism
03 Session Management Mechanism
04 Access Controls
05 Input-based Vulnerabilities
06 Function-specific Input Vulnerabilities
07 Logic flaws
08 Shared Hosting Vulnerabilities
09 Web Server Vulnerabilities
10 Other
Step 2. Describe Current Risk
Step 3. Assign a Level of Risk
Record overall level of risk in Web Application Security
None
Low
Medium
High
Next Step:Record Current Risks then click on Triggers tab.

Appendix IV. Information Governance Lead Responsibilities

Key responsibilities of an Information Governance lead

- To ensure there is an up-to-date IG policy in place;
- To ensure that the organisation's approach to information handling is communicated to all staff and made available to the public;
- To coordinate the activities of staff given data protection, confidentiality and Freedom of Information Act responsibilities;
- To monitor the organisation's information handling activities to ensure compliance with law and guidance;
- To ensure staff are sufficiently trained to support their role;
- To ensure that the organisation submits their annual IG Toolkit assessment;
- To support monitoring visits from the commissioning organisation (where appropriate).

As IG Lead, I am aware of the above responsibilities and able to fulfil them:

Signature:	Date:

Appendix V. Confidentiality and Non-Disclosure Policy

This policy applies to those undertaking work on behalf of tmwk.

Information or data to which suppliers, agency/temporary staff and contractors may have access, should be treated as confidential and not divulged, unless specifically stated otherwise or unless explicit approval is given to do so by tmwk in writing.

Data Protection

Any data processed on our behalf, be it manual or on any computer system is to be treated as confidential and stored and processed in accordance with the Data Protection Act 1998, to be superseded by the General Data Protection Regulation and the Data Protection Bill 2018 from 25th May 2018.

Confidentiality and Non-Disclosure

tmwk require that you safeguard information that you use in the course of carrying out work on tmwk's behalf, in particular:

- You have read and are compliant with tmwk Information Governance Policy;
- All information passed between you and tmwk is deemed to be private and confidential;
- You agree to employ all reasonable endeavours to maintain the security and confidentiality of information: such endeavour will be no less than the degree of care you employ to preserve the confidentiality of your own information;
- You undertake to ensure that access to information held by tmwk or data will be restricted to persons who have written confidentiality undertakings in their contracts of employment or service and reasonable steps have been taken to ensure the reliability of staff;
- You will not sub-contract the processing of or disclose any data to any third party without the prior written approval of tmwk;
- You agree to use the information or data provided solely for the purpose for which it was intended;
- You do not take copies in whole or in part of any data without prior written agreement;
- Any copies of data will be used solely for the purpose of improving service as part of a contract or formal agreement with tmwk;
- You agree not to disclose to any third party any information regarding your work with tmwk without prior written consent;
- On request or on completion or cancellation of the contract you will return all information or data supplied to you by tmwk, or otherwise undertake to destroy it and/or delete any electronically stored information including any backup copies or tapes within 5 working days;
- You may not re-use in full or part, any information supplied to you by tmwk without prior written consent;
- You will notify us immediately of any breach of this agreement. You agree to co-operate fully and promptly and to provide to us all reasonable assistance in investigating and dealing with any breach;
- You will not be liable for information provided to you that is already published in the public domain;
- You may not during or after the termination of your employment, disclose to anyone other than in the proper course of your employment or where required by law, any information of a confidential nature relating to the company or its business or customers. Breach of this clause may lead to dismissal without notice. Guidance on standards expected can be found in the staff code of conduct.

In all cases above, written consent, approval or agreement could be by email.

I agree to abide by the terms and the conditions of Confidentiality and Non-Disclosure Policy of tmwk.

Name …….

Signed …….

Date …….

On behalf of …….

Company Name

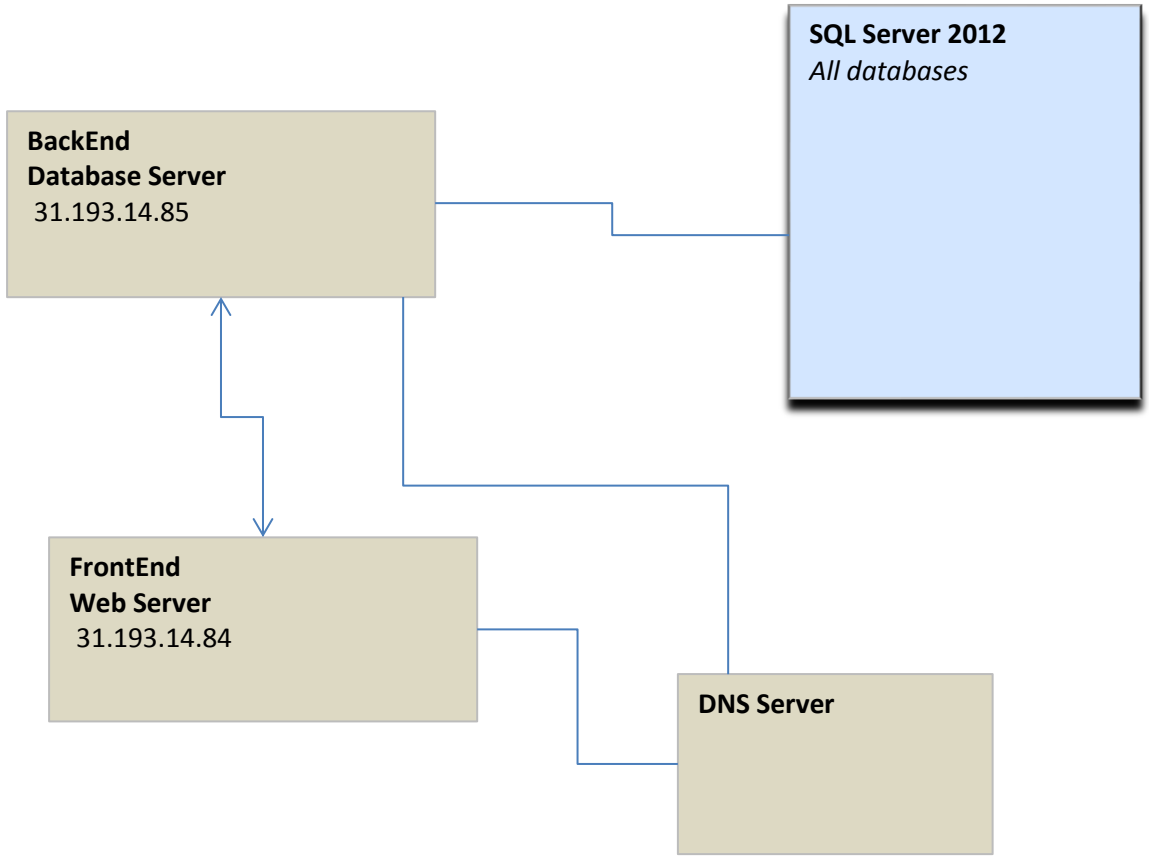
Appendix VI. Information Governance Training Log Update

Role	Name	Training	Signature	Date
Managing Director	Tim Kendall	Data Security Awareness		29/03/18
Technical Director	Martin Woolley	Data Security Awareness		29/03/18

Appendix VII. Serious Incidents Log

Date	Nature of incident	Nature of data involved	Number of data subjects potentially affected	Notification Steps

Appendix VIII. System Diagram



Appendix IX. Email Notice and Disclaimer

NOTICE AND DISCLAIMER

This e-mail (including any attachments) is intended for the above-named person(s). If you are not the intended recipient, notify the sender immediately, delete this email from your system and do not disclose or use for any purpose. Emails to and from tmwk related to spa should not include identifiable personal confidential data, unless under the specific terms of tmwk's and the sender/receiver's information governance policy. Where relevant email received does not meet these terms, the sender will be notified and the email deleted permanently. We have taken steps to ensure that this email and attachments are free from any virus, but it remains your responsibility to ensure that viruses do not adversely affect you.

Appendix X. Cyber Essential Certificate

nccgroup
freedom from doubt

CYBER ESSENTIALS

This is to certify that

TMWK Limited

40 Highbury Grove, London N5 2AG

Has been assessed
by Jonathan O'Reilly for NCC Group
against the Cyber Essentials Scheme Test Specification

Level of certification: Cyber Essentials

Scope: TMWK Limited Externally Facing Infrastructure

Certification date: April 17th, 2018
Recommended re-assessment date: April 16th, 2019
Certificate no.: 7498763290882269

CREST

This Certificate confirms that the organisation named was assessed against the Cyber Essentials Requirements dated June 2014, and at the time of testing, the organisation's ICT defences were assessed to meet the Requirements. Cyber Essentials Certification indicates that the organisation has implemented a sensible baseline of organisational cyber security only, and implies no guarantee of effective defence against commodity cyber attacks circumventing this baseline. Organisations are recommended to define and understand the risks to their organisation and take all appropriate action to mitigate or reduce any issues, which may require a greater degree of rigour or technical investment than is required for Cyber Essentials alone.

Appendix XI. Cookie Policy

tmwk ("us", "we", or "our") uses cookies on the spa and tmwk website (the "Service"). By using the Service, you consent to the use of cookies. Our Cookies Policy explains what cookies are, how we use cookies, how third-parties we may partner with may use cookies on the Service, your choices regarding cookies and further information about cookies.

What are cookies

Cookies are small pieces of text sent by your web browser by a website you visit. A cookie file is stored in your web browser and allows the Service or a third-party to recognize you and make your next visit easier and the Service more useful to you. Cookies can be "persistent" or "session" cookies. Persistent cookies remain on your personal computer or mobile device when you go offline, while session cookies are deleted as soon as you close your web browser.

How tmwk uses cookies

When you use and access the Service, we may place a number of cookies files in your web browser. We use cookies for the following purposes:

- To enable certain functions of the Service
- We use both session and persistent cookies on the Service and we use different types of cookies to run the Service:
- Essential cookies. We may use essential cookies to authenticate users and prevent fraudulent use of user accounts.

What are your choices regarding cookies

If you'd like to delete cookies or instruct your web browser to delete or refuse cookies, please visit the help pages of your web browser. Please note, however, that if you delete cookies or refuse to accept them, you might not be able to use all of the features we offer, you may not be able to store your preferences, and some of our pages might not display properly.

- For the Chrome web browser, please visit this page from Google: https://support.google.com/accounts/answer/32050
- For the Internet Explorer web browser, please visit this page from Microsoft: http://support.microsoft.com/kb/278835
- For the Firefox web browser, please visit this page from Mozilla: https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored
- For the Safari web browser, please visit this page from Apple: https://support.apple.com/kb/PH21411?locale=en_US
- For any other web browser, please visit your web browser's official web pages.

Where can you find more information about cookies

You can learn more about cookies and the following third-party websites:

AllAboutCookies: http://www.allaboutcookies.org/

Network Advertising Initiative: http://www.networkadvertising.org/