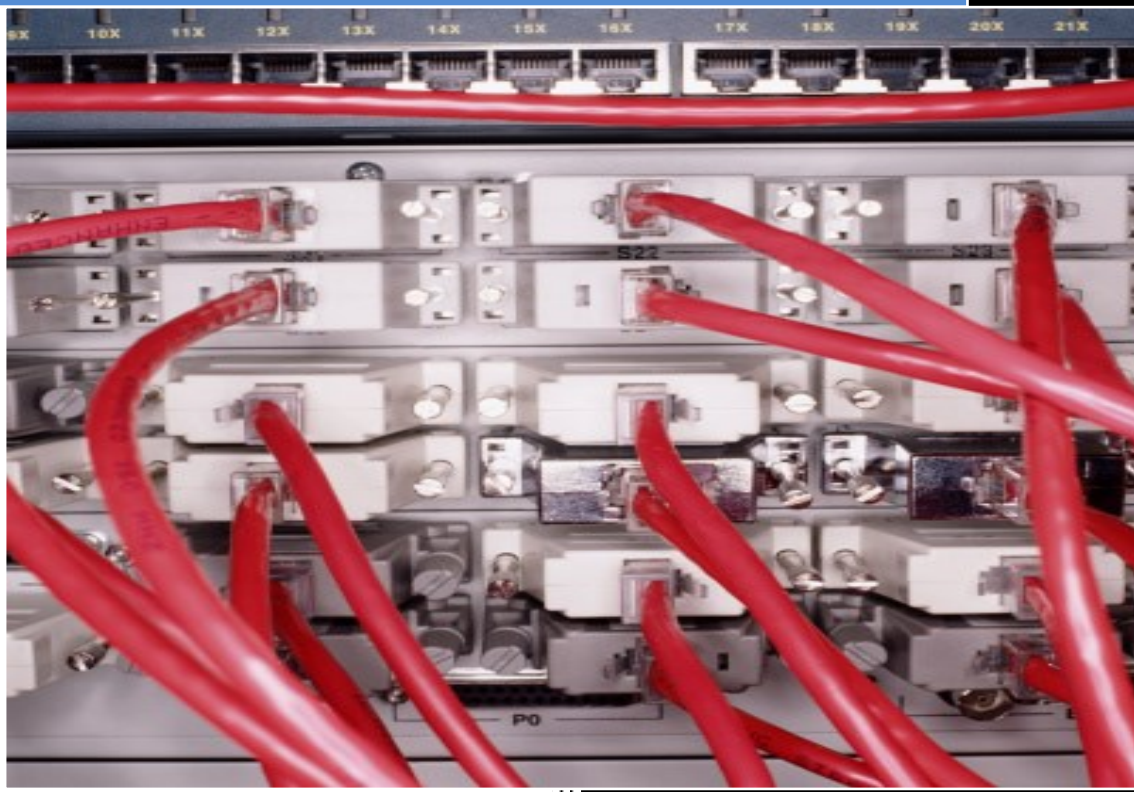
YourIT!
Your Logo Goes Here

GDPR Assessment

ISO 27001 Compliance Questionnaire



Scan Date: 1/18/2018

Prepared for:
My Client Company
Prepared by:
YourIT Company

1/18/2018

Table of Contents

INFORMATION SECURITY POLICY (ISO 27001-2013 A.5)

1.1 - Policy Last Reviewed (ISO 27001-2013 A.5.1.2)

When was the last time that the Information Security Policy and Procedures document was reviewed?

Less than a year ago

ORGANIZATION OF INFORMATION SECURITY (ISO 27001-2013 A.6)

2.1 - Documentation of Contact with Authorities (ISO 27001-2013 A.6.1.3)

Does your organization have documentation which specifies how to report security incidents in a timely manner, including which authorities to contact and when? If yes, please attach the document.

No

2.2 - Contact with special interest groups (ISO 27001-2013 A.6.1.4)

Does your organization maintain appropriate contacts with special interest groups, security forums, and professional organizations?

No

2.3 - Project management process (ISO 27001-2013 A.6.1.5)

Is information security integrated into the project management process, regardless of the type of project?

No

MOBILE DEVICE AND TELEWORKING (ISO 27001-2013 A.6.2)

3.1 - Mobile devices (ISO 27001-2013 A.6.2)

Are mobile devices allowed to connect to your network?

Yes

Follow-up to 3.1 if you answered Yes above
- Use of Mobile Device Management (MDM) (ISO 27001-2013 A.6.2.1)

Do you employee a Mobile Device Management (MDM) system to ensure the protection of mobile devices connecting to your environment?

Yes

Follow-up to if you answered Yes above

Name of the Mobile Device Management (MDM) system

RFT MDM

3.2 - Teleworking (ISO 27001-2013 A.6.2.2)

Is teleworking or remote access allowed in your networking environment?

Yes

Follow-up to 3.2 if you answered Yes above
- Remote connectivity secured (ISO 27001-2013 A.6.2.2)

Is remote connectivity provided to remote workers in a secure manner?

Yes

Follow-up to if you answered Yes above

Describe the manner of remote access (VPN, Remote Desktop, Virtualization, etc.)

VPN and Remote Desktop

HUMAN RESOURCE SECURITY (ISO 27001-2013 A.7)

4.1 - Background checks (ISO 27001-2013 A.7.1.1)

Are background checks performed on all employees prior to employment?

Yes

4.2 - Terms and conditions of employment (ISO 27001-2013 A.7.1.2)

Review the contractual agreements with employees and contractors. Do the agreements reflect the organization's policies for information security, confidentiality, legal responsibilities, classification and management of information, responsibilities for handling information, and punitive action if the employee or contractor disregards these requirements?

Yes

4.3 - Information security awareness training (ISO 27001-2013 A.7.2.2)

Do all employees receive information security awareness training?

No

EMPLOYEE TERMINATION (ISO 27001-2013 A.7.3)

5.1 - Off-boarding process (ISO 27001-2013 A.7.3.1)

Do you have a documented off-boarding process that communicates any ongoing information security responsibilities to the employee or contractor?

Yes

Follow-up to 5.1 if you answered Yes above
- Records of off-boarding activities (ISO 27001-2013 A.7.3.1)

Where is a record of off-boarding activities documented? Attach documentation if applicable.

Bamboo

ASSET MANAGEMENT (ISO 27001-2013 A.8)

6.1 - Documented information labeling process (ISO 27001-2013 A.8.2.2)

Do you have a documented procedure for labeling information assets in both physical and electronic formats?

No

MEDIA HANDLING (ISO 27001-2013 A.8.3)

7.1 - Physical media transfer (ISO 27001-2013 A.8.3.3)

Regarding physical media, verify the following best practices are adhered to.

☑	Only reliable transport or couriers are used
☑	Authorised couriers are agreed upon with management
☑	A procedure exists to identify couriers
☑	Packaging is sufficient to protect contents in transit
☑	Logs are kept identifying the content and protections applied as well as recording times of transfer to the transit custodian and receipt at destination

USER ACCESS MANAGEMENT (ISO 27001-2013 A.9.2)

8.1 - Documented user access procedures (ISO 27001-2013 A.9.2)

Do you have a documented procedure for user registration and de-registration as well as provisioning user access privileges?

Yes

Follow-up to 8.1 if you answered Yes above
- User access procedure description (ISO 27001-2013 A.9.2)

Briefly describe the process for granting and revoking user access? Attach documentation if applicable.

Creating an account in AD and set access rights to the appropriate level depending on position.

8.2 - Application Access

Identify the various applications used in the environment and what log-on procedure is used.

Application	Log-on Procedure	Is the Application Secure?
SalesForce	Web login	Yes
Support Portal	Web Login	Yes

Application	Log-on Procedure	Is the Application Secure?
Fusebill	Web login	Yes
Network Detective	Local pc login	Yes

8.3 - Access control to program source code (ISO 27001-2013 A.9.4.5)

Does your organization maintain or develop programs where access to source code is required?

Yes

Follow-up to 8.3 if you answered Yes above
- Program source libraries are not held in operational systems

Yes

Follow-up to 8.3 if you answered Yes above
- Program source code and libraries are managed according to established policies

Yes

Follow-up to 8.3 if you answered Yes above
- Support personnel do not have unrestricted access to program source libraries

Yes

Follow-up to 8.3 if you answered Yes above
- Updating program source libraries and issuing of access to program source libraries to programmers is only performed after appropriate authorisation is received

Yes

Follow-up to 8.3 if you answered Yes above
- Program listings are help in a secure environment

Yes

Follow-up to 8.3 if you answered Yes above
- An audit log is maintained of all accesses to program source libraries

No

Follow-up to 8.3 if you answered Yes above
- Maintaining and copying of program source libraries should be subject to strict change control procedures

No

CRYPTOGRAPHY (ISO 27001-2013 A.10)

9.1 - Documented cryptographic controls procedures (ISO 27001-2013 A.10.1)

Do you have a documented procedure for the use of cryptography in your environment?

No

OPERATIONS SECURITY (ISO 27001-2013 A.12)

10.1 - Documented operating procedures (ISO 27001-2013 A.12.1.1)

Do you have documented operating procedures? If "Yes," attach the relevant documentation.

Yes

10.2 - Information backup (ISO 27001-2013 A.12.3.1)

Does your organization have an information backup policy? If "Yes," attach the relevant documentation.

Yes

Follow-up to 10.2 if you answered Yes above
- Information backup solution (ISO 27001-2013 A.12.3.1)

Name of information backup solution

N/A

Follow-up to 10.2 if you answered Yes above
- Last successful backup (ISO 27001-2013 A.12.3.1)

When was the last successful backup?

N/A

Follow-up to 10.2 if you answered Yes above
- Last successful restore test (ISO 27001-2013 A.12.3.1)

When was the last successful restore test?

N/A

COMMUNICATIONS SECURITY (ISO 27001-2013 A.13)

11.1 - Operational responsibility for networks (ISO 27001-2013 A.13.1.1)

Does your organization manage and control networks to protect information in systems and applications, including separating operational responsibilities for networks from computer operations?

Yes

11.2 - Agreements on information transfer (ISO 27001-2013 A.13.3.2)

There should be policies and procedures to protect information that is transferred within and outside of the organization. Agreements should define the responsibilities for how information is transferred between the organization and third-parties. In the table below, list each agreement between the organization and a third-party that governs the

transfer of information. Indicate whether the agreement defines management's responsibilities for ensuring information security. Also indicate whether the agreement details specific technical procedures to ensure security.

Agreement	Management responsibilities defined	Procedures to ensure traceability and non-repudiation
SalesForce	Yes	Yes
Datto	Yes	Yes
MYCO-IT	No	No

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE (ISO 27001-2013 A.14)

12.1 - Securing applications on public networks (ISO 27001-2013 A.14.1.2)

If your organization stores or transmits sensitive information on public web-based applications, list those in the table below. Indicate whether the application uses a secure protocol, and whether users must authenticate their identities.

Web Application (URL)	Is a Secure Protocol Employed?	Are Authentication Procedures Employed?
amazonaws.com	Yes	Yes
SalesForce	Yes	Yes
Fastbill	Yes	Yes

12.2 - In-house Development (ISO 27001-2013 A.14.2)

Does your organization perform in-house development?

Yes

INFORMATION SECURITY INCIDENT MANAGEMENT (ISO 27001-2013 A.16)

13.1 - Documented information security incident management system (ISO 27001-2013 A.16)

Do you have a documented procedure for information security incident management?

No

BUSINESS CONTINUITY MANAGEMENT (ISO 27001-2013 A.17)

14.1 - Documented Business Continuity Plan (ISO 27001-2013 A.17.1)

Do you have a documented Business Continuity Plan? Attach documentation if applicable.

Yes

14.2 - Redundancies for Information Processing Facilities (ISO 27001-2013 A.17.2)

Are information processing facilities implemented with redundancy sufficient to meet availability requirements?

Yes

COMPLIANCE (ISO 27001-2013 A.18)

15.1 - Applicable legislation (ISO 27001-2013 A.18.1.1)

List all applicable legislation (one per line) other than GDPR that are relevant.

UK Data Protection Act 1998