

Information Security Questionnaire

CONFIDENTIAL (when completed)

1. Company Information

1.1	Company Name
1.2	Registered Office
1.3	Company Registration Number
1.4	Does the company trade under any other name or corporate identity to that identified in question 1.1, if yes please provide details below
1.5	Are you registered with the Information Commissioners Office (ICO)? If so please provide your registration number below

2. Key Contact Information

2.1	Full Name
2.2	Job Title
2.3	Role in Responding to this Questionnaire
2.4	Office Address
2.5	Phone Number
2.6	Email Address

--	--

3. Products, Services & Architecture Overview

3.1	Please give a summary description of the services to be provided to Service Recipients
3.2	Please describe the business processes and IT systems used to provide the services. Please try to show the flow of data where possible, including a simple diagram/flowchart. Inclusion of this will help our understanding greatly. <i>We are particularly interested in any web services (FTP/SFTP etc) or websites that will be used as part of the service to Service Recipients.</i>
3.3	Will you be processing data provided by Service Recipients as part of this service? Or will you be collecting all data yourselves/from third parties and submitting to Service Recipients afterwards?

4. Data management

4.1	Please describe your (existing) overall approach to data protection and information security <i>e.g. your data protection, information security and/or acceptable usage policies</i>
4.2	If applicable, please detail how and where you will be collecting data to be used for this service, including who will be performing these collection activities
4.3	If applicable, please detail how and where you will be storing and handling data to be used for this service, including who will have access to this stored data
4.4	Please detail how you will be transmitting/transferring/moving data that is used as part of this service, please include the start and end locations of that data, please also include what the data is

5. Access Control

5.1	How do you control access to the data being used to supply this service to Service Recipients? <i>For example, what technology do you use to secure/protect files whether physical or electronic? Is there a process for granting, monitoring and removing access to that data?</i>
-----	--

--	--

5.2	Does your organisation allow admin accounts on your IT systems? If yes, which areas of your organisation hold admin accounts?
5.3	If applicable, is the use of these admin accounts restricted, monitored and auditable? If so can you explain how please?

6. Third party services

6.1	<p>Do you use third party suppliers for any part of the service being offered to Service Recipients? If so, please detail <u>what services they provide</u> to you and <u>how these services relate</u> to the offering to Service Recipients.</p> <p><i>This may include for example sub-contracted companies that collect data for you or specialist IT service providers you use for your IT support, data storage or web hosting etc</i></p>
-----	--

7. Human Resources Information Security

7.1	Does your organisation <u>conduct personnel screening</u> for employees and contractors who are involved with the administration or handling of systems holding customer/personal information? Please provide summary details.
-----	---

8. Physical Security

8.1	<p>Are the <u>data storage</u> and <u>processing</u> systems (servers, desktops, paperwork etc) to be used for the provision of products & services to Service Recipients, housed in a <u>physically secure environment</u>? If yes, please describe <i>e.g. lockable filing cabinets, cages, dedicated areas, CCTV?</i></p> <p>If you also use an offsite backup facility then please also detail its facilities.</p>
-----	---

9. Communications & Operations Security

9.1	How is your IT operated and supported? Please tell us who supports your IT and where they are based. <i>Please also include third parties who provide remote access for example.</i>
9.2	Is internet access available from the same device (e.g. PC) to the employees engaged in processing Service Recipients data? If yes, please justify the requirements for this access and what security measures are in place.
9.3	Do you have firewalls and other security systems (anti-virus software etc) within your infrastructure and if so do you test their effectiveness? <i>Please look at all aspects e.g. network, servers, desktops, mobile devices/tablets</i>
9.4	How do you ensure that your operating systems and anti-virus solutions are kept up to date and are operating effectively?
9.5	Are the IT systems used to provide the service to Service Recipients also used to provide a service to other customers? If so, how do you separate and secure the data?
9.6	Do you allow staff to work remotely? If so how is this remote working managed? <i>For example, do staff remotely log into your IT systems? Do staff take data home to work on?</i>
9.7	Are removable and writable storage devices (e.g. USB "sticks") allowed on the devices being used to process Service Recipients data?
9.8	How would you identify a case of loss/theft/unauthorised access to crucial data? If this had happened and been identified how would you inform Service Recipients?

10. Business Continuity Management

10.1	<i>Please describe your overall approach to business continuity management and disaster recovery.</i>
------	---

Thank You for completing this questionnaire.