	Question	Response and Evidence
	Security Policy	
1	What policies do we maintain and enforce for Information Security?	Our ISMS Policy is attached which outlines this (ISMS01 ISMS Policy V1.5)
2	Does the organisation have certification to an Information Security Standard (e.g. ISO/IEC27001, Cyber Essentials)?	ISO/IEC 270001:213 Certificate Number: IS 643968 Certification Date: 23.03.2019 Monthly Audited IS27001 Certificate 643968
3	State whether a Head of Information Security role is allocated and to whom.	Yes - Trayton Vance, CEO.
4	Does the organisation have a defined and deployed secure standard build for all servers, endpoint and network equipment servicing system and data?	Yes, we use Heroku platform as a service for hosting the web application and Amazon RDS and S3 for data and media files respectively. We do not have a standard build for devices but all devices have relevant software added before use. i.e. Bullguard provides our device protection
5	Does the organisation restrict access to removable media drives (e.g. CD-ROM, DVD-ROM, etc.) and data ports (e.g. USB, Firewire, etc.) on each device fitted with such drives and/or ports?	We do not use removable media drives and our policy states these MUST not be used (ISMS01 ISMS Policy V1.5)
	HR Security	
6	Are screening and background checks carried out for staff in the organisation?	Identification, proof of residence, right to work and employment history/references are checked prior to commencing employment.
7	Do the terms and conditions of employment for staff include responsibility for Information Security and the non-disclosure of confidential information?	Yes - extract from employee contract below. 1. Restrictions and Confidentiality 15.2 You will not at any time either during your employment or afterwards use or divulge to any person, firm, or company, except in the proper course of your duties during your employment by the Company, any confidential information identifying or relating to the Company, details of which are not in the public domain. 15.3 You may not during the period of six months from the termination date hold a material position in a business the same as or in competition with the Company anywhere in the United Kingdom or other territory where the Company operates or plans to operate. 15.4 You may not during your employment and for the period of six months from the termination date in relation to a business the same as or in competition with the Company, canvass, solicit or approach, or cause to be canvassed, solicited or approached for the purpose of obtaining business, order or custom any person, company or firm who was a prospective customer of the Company with whom at the termination date there were negotiations on-going with a view to it becoming a customer of the Company. 15.5 You may not for a period of six months following the termination date perform any services or supply goods to any person, company or firm who was a customer of the Company during the twelve-month period prior to the termination date. 15.6 You may not offer to employ or offer to conclude any contract for services with any key person or procure or facilitate the making of such offer by any person, firm, or company. 15.7 You agree that you had the opportunity to take advice regarding these restrictions and are satisfied that they are reasonable in the circumstances, and that each of the sub-clauses detailed in this section are entirely separate, severable, independent and an independent covenant and restriction on you. Further that the duration, extent and application of each of the sub-clauses in this section is no greater than is necessary for the protection of the goodwill and trade connections of the Company.

8	What formal Security Awareness Training is provided to staff?	Policies in place that all staff are aware of include: Acceptable Use, Back Up, Clear Desk and Screen, Data Privacy and Protection, Password Guidance and Policy, Teleworking. Staff also undergo GDPR and Legislative training.

	Access Control	
9	Describe the organisation's approach to Access Control	We have an access control policy which outlines this - ISMS09 Access Control Policy
10	Describe the organisations approach to passwords with regards to complexity	Internally, all passwords will be autogenerated by LastPass and will have the following characteristics: 1.Contain at least 12 alphanumeric characters. 2.Contain both upper and lower case letters. 3.Contain at least one number (for example, 0-9). 4.Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/). Account is locked out after 5 attempts Account lockout duration is 3 minutes
11	How does the organisation ensure passwords are compliant with our password policy?	The system will not let you create a password which does not comply with the above.
12	Are the password configuration settings the same across both applications and operating systems?	Yes
13	To what extent are passwords (and equivalent authentication secrets) securely hashed and/or encrypted (as appropriate) both at rest (e.g. within password files) and in transit (e.g. at the point of authentication)?	User access via the browser is over https. All passwords stored in the database are encrypted. From the Django docs, " By default, Django uses the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST."
14	Are the reasons for an account being locked out for repeated authentication failures investigated and reported?	Yes - the system is monitored
15	How are user privileges segregated between the Development, Test and Production environments (or equivalent)?	We have separate Development, Test and Production environments
	Data Security	
16	Where is client data physically located e.g. in any 'cloud' environment?	Amazon Data Center, located in Ireland.
17	What if any data minimisation practices do you follow? This includes use using anonymised or pseudo-anonymised data in development, test and data analytics environments?	Data is only kept as long as the contract between us and the client is live. Live data is not used in development or test environments.
18	If any client data is shared with a third party how is the 3rd party (including data centre providers or cloud environments) held accountable to comply with security policies?	Data is not shared with third parties outside of platform hosts.
19	Does the organisation have formally documented data classification and data handling procedures?	We have a Data Privacy and Protection Policy, which includes the outlines and definitions of the policy, the scope and how it aligns to GDPR. It outlines mye-coach's position in handling data and our commitment to protecting it. It also details roles and responsibilities for compliance to the standard.
20	Has the organisation defined a data retention policy?	We have adopted GDPR data retention policies. The system is decommissioned at the end of the contract with all data being destroyed.
21	Does the organisation hold any additional security certifications?	We are currently working towards Cyber Essentials Plus certification and expect to have this early 2022.

	Communications and Operations Management	
22	Describe the controls that are implemented to prevent and detect breaches of security due to malicious code infections/attacks (e.g. anti-virus, worm, Trojans, etc.). Include an explanation of how the efficacy of the control measures are maintained, monitored and updated.	mye-coach is a simple web application built on the Django framework. As such, the most common web vulnerabilities are addressed out of the box. All coding and design decisions are made to ensure those mechanisms are not circumvented and taking the most common web vulnerabilities into account including the OWASP Top Ten (https://owasp.org/www-project-top-ten/). Further information can be found here - https://docs.djangoproject.com/en/3.0/topics/security/. mye-coach is hosted on Heroku (platform as a service), who have their own security and vulnerability tests in place - see more information here https://www.heroku.com/policy/security
23	Has the organisation experienced any major incidents as the result of malicious code infections/attacks in the last year? If so please give details and explanation of how these were dealt with.	N/A - no incidents
24	Describe the organisation's control measures for maintaining the security of the perimeter of the network, including how Internet access is controlled and monitored for all employees.	Our office network is protected by Bullguard Premium protection which provides us malware protection, home network monitoring, anti-virus, firewall and other protection for our office devices - it alerts us when any device has joined the network.
25	What controls do you have in place to prevent the unauthorised removal of information from the organisation?	Access to all internal systems is protected by a password manager (Last Pass) and secure passwords are used. All laptops are stored in locked containers and the office premises are securely locked when vacant.
	Business Continuity	
26	To what extent has the organisation defined and documented (e.g. within a business continuity plan or similar) how the organisation intends to continue to deliver contracted services to clients in the event of a foreseeable disruptive event (e.g. fire, flood, power failure, etc.)?	We have a secondary location that is set up to replicate the services provided at the main location. In this location all the operational functions can be fulfilled. All employees are also able to work from home in an emergency and can access all emails and documentation as required. When working virtually all staff must adhere to ISMS23 Acceptable Mobile Use. This was last tested May 2021 ISMS11 Business Continuity Planning V1.2
27	Describe the schedule for testing of the Plans, including frequency, coverage and areas involved.	There is no agreed schedule for this however the process is outlined in the BCP document
	Change Management	
28	Explain what change controls and standards are applied to ensure data accuracy and service availability.	Our Change Management and Control Policy outlines this - ISMS12 Change Management & Control Policy V1.1

	Risk Management	
29	What steps has the organisation taken to ensure the platform is secure against unauthorised access?	We use a third party supplier (Fidus) to conduct PEN testing and this exercise will be completed annually.
30	Describe the information security risk management process for new projects before they go live.	A System Development Life Cycle is used to minimise the risks this is as follows; Initiation Phase. During the initiation phase, we establish the need for a system change and document its purpose. Security planning begins in the initiation phase with the identification of key security roles to be carried out in the development of the system change. The information to be processed, transmitted, or stored is evaluated for security requirements, and all stakeholders should have a common understanding of the security considerations. Security considerations are key to the early integration of security, and to the assurance that threats, requirements, and potential constraints in functionality and integration are considered. Requirements for the confidentiality, integrity, and availability of information should be assessed at this stage. Development/Acquisition Phase. During this phase, the system change is designed, agreed, programmed, developed, or otherwise constructed. A key security activity in this phase is conducting a risk assessment and using the results to supplement the baseline security controls. In addition, the organization should analyse security requirements; perform functional and security testing; prepare initial documents for system certification and accreditation; and design the security architecture. The risk assessment enables the organization to determine the risk to operations, assets, and individuals resulting from the operation of information systems, and the processing, storage, or transmission of information. After categorizing the risks minimum security requirements should be implemented and the appropriate security controls and assurance requirements that are described in IS Management Guide. Recommended Security Controls for Information Systems. Another essential element is the development of security plans, which establish the security requirements for the information system, describe security controls that have been selected, and present the rationale for security categorization, how controls are implemented, and how use of systems can be restricted in high-risk situations. Security plans document the decisions made in the selection of controls and are approved by management. The developmental testing of the technical and security features and functions of the system ensure that they perform as intended, prior to launching the implementation and integration phase. Implementation Phase. In the implementation phase, we configure and enable system security features, tests the functionality of these features, installs or implements the system, and obtains a formal authorization to operate the system. Design reviews and system tests should be performed before placing the system into operation to ensure that it meets all required security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed. This approach ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the organization's official records. Operations/Maintenance Phase. In this phase, system functionality is in place and operating, enhancements and/or modifications to the system functionality are developed and tested. The organization should continuously monitor performance of the system to ensure that it is consistent with pre-established user and security requirements, and that needed system modifications are incorporated. We follow traditional System Development Lifecycle processes we ensure any risks are minimised at all phases. The process we follow is: Documenting information system changes and assessing the potential impact of these changes on the security of a system are essential activities to assure continuous monitoring and prevent lapses in the system security accreditation. Disposal Phase. In this phase, plans are developed for discarding system information and making the transition to the new functionality. The information may be moved to another system, archived, discarded, or destroyed. If performed improperly, the disposal phase can result in the unauthorized

		disclosure of sensitive data. When archiving information, the organization should consider the need for and the methods for future retrieval. Usually, there is no definitive end to a system. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information for the original system should still be relevant and useful when the organization develops the security plan for the follow-on system. The disposal activities ensure the orderly termination of the system functionality and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access. The removal of information from a storage medium should be done in accordance with the organization’s security policy.