Supplier Information Security Questionnaire

This questionnaire is to be completed when personal and / or confidential data is shared by The Growth Company (GC) with a third party. We do this in order to comply with the Data Protection Act, our ISO 27001 accreditation and in some cases, to meet funding requirements. If no personal or confidential data is being exchanged, it is unlikely you will need to complete this questionnaire, please speak to the GC individual who has sent you the questionnaire to complete.

Suppliers who meet **ANY** of Tier 1 Critical Supplier criteria are required to complete **all sections** of the questionnaire (Sections 1-7). Suppliers who are Tier 2 Moderate Risk must complete **sections 1 to 3 only**.

Category	Tier 1 - Critical	Tier 2 - Moderate Risk
Personal Data (Employees, Clients, Customers, Service Users)	Process or have access to significant amounts of personal and confidential data. Handling or processing **more** than a total of 50 Data Sets. This is the cumulative total number of data sets over the entire life of the contract	Process or have access to personal and confidential data. Handling or processing **less** than a total of 50 Data Sets. This is the cumulative total number of data sets over the entire life of the contract. One off exchange of employee, client or customer contact data where GC is supplying the data to the Supplier (may be more than 50 data sets, but the disclosure is limited to email addresses/ participant names for a one off event)
Access to GC Confidential Data, Documents, Systems	Ability to view, copy, download, export GC data held in a system or software or on premises	Restricted View / Limited Access where any potential data loss or a breach of confidentiality would not lead to significant loss for GC
Example Types of Supplier	Supply Chain Partners, Finance and Payroll System, Travel Provider, Auditors, Learning platform	Contractors, Associates, Event Organiser

Supplier Information Security Questionnaire

Instructions for Completion

- Please complete **all required** sections in full and provide additional information where requested.
- Please return your completed form and any attachments to your contact at GC who will evaluate the questionnaire. For more information on how the questionnaire will be evaluated, please see the evaluation grid at the bottom of this document and the detailed guidance provided.

Please note that you may be asked for further information or clarification during the evaluation of your questionnaire.

You should retain duplicate copies of your completed response for your own records.

SECTION 1: Background Information

Date of Assessment	
Organisation Name	
Registered Address	
Trading Address if different from above	
Contact name in relation to this questionnaire	
Contact details	
Number of employees in your organisation	

Supplier Information Security Questionnaire

SECTION 2: Data Governance

	REQUIREMENT	STATUS		FURTHER INFORMATION
		Yes	No	: Where 'No' has been ticked, please explain why this is the case and provide further details on the current controls/processes that are in place. : Where 'Yes' has been ticked, provide additional information where requested.
2.1	Do you have a named person with day to day responsibility for data protection? Is there an executive level role with overall accountability for our information compliance programme?	Answer for information only		Please provide the name and contact details of person responsible for data protection. Tick if this person is a Data Protection Officer ☐
		☐	☐	
2.2	Do you have a GDPR compliant Data Protection policy to cover personal data?	☐	☐	: Please supply a copy. :
2.3	Do you have a data protection and information security training programme in place for your employees, with refresher training, which tests staff understanding? As a sole trader or micro business have you taken sufficient steps to ensure you and your staff are able to protect GC data?	☐	☐	:
2.4	Will all the personal data that you are processing be kept within the UK.	☐	☐	: Please explain what data will be transferred outside of the UK and confirm how you will fulfil the obligation of adequate protection in respect of that personal data.

Supplier Information Security Questionnaire

SECTION 3: Information Security

	REQUIREMENT	STATUS		FURTHER INFORMATION
		Yes	No	: Where 'No' has been ticked, please explain why this is the case and provide further details on the current controls/processes that are in place. : Where 'Yes' has been ticked, provide additional information where requested.
3.1	Do you hold any current certifications or registrations, such as ISO 27001, Cyber Essentials, Cyber Essentials Plus or Public Services Network (PSN) Compliance? Note: if your organisation does not currently hold any certificates you must agree to complete Cyber Essentials as minimum within 6 months. See information at Annex 2.	☐	☐	: Please state what certificates you hold: : If no, are you willing to commit to obtaining Cyber Essentials if you are awarded the contract? YES ☐ **For sole traders or personal service companies (single employee)** : If no, are you willing to undertake and successfully pass GC's Information Security Training if you are awarded the contract? YES ☐

To be Completed by the Contract or Supply Chain Manager			
	Pass, Fail or Remedial Action Plan		**Please explain reasons for Fail or Remedial Action Plan**
SECTION 2: Data Governance			
SECTION 3: Information Security			
Signed:		**Date:**	
Remedial Action Plan agreed by:		**Date:**	

Supplier Information Security Questionnaire

Sections 4-7 are to be completed by Critical Suppliers.

SECTION 4: Data Governance (detailed)

	REQUIREMENT	STATUS		FURTHER INFORMATION
		Yes	No	: Where 'No' has been ticked, please explain why this is the case and provide further details on the current controls/processes that are in place. : Where 'Yes' has been ticked, provide additional information where requested.
4.1	Do you carry out Data Protection Impact Assessments (DPIA) where you are legally required to do so and build the findings into your processes?	☐	☐	:
4.2	Do you have processes in place to assess, review and amend your GDPR and information security compliance systems (e.g. spot-checks, internal audit, external audit), the outcomes of which are reported back into senior management.	☐	☐	: Briefly describe the processes you have in place. :
4.3	Are you able to delete or amend all The Growth Company data held on your systems on request?	☐	☐	:
4.4	For every instance where Growth Company data is held by a third-party company or system, do you have written contractual agreements that address confidentiality,	☐	☐	

Supplier Information Security Questionnaire

	information security, GDPR, intellectual property rights and accessibility etc. Tick here if not relevant ☐			

SECTION 5: Data Breaches

	REQUIREMENT	STATUS		FURTHER INFORMATION
		Yes	No	: Where 'No' has been ticked, please explain why this is the case and provide further details on the current controls/processes that are in place. : Where 'Yes' has been ticked, provide additional information where requested.
5.1	Do you have a formal procedure for identifying and reporting *data leaks/breaches, including suspected data leaks/breaches and information security incidents*?	☐	☐	: Please supply a copy. :
5.2	Has your business or any of your directors been subject to any regulatory investigation or disciplinary action for a personal data breach?	☐	☐	: Please provide a brief explanation:
5.3	Has your organisation had any data breaches in the last 12 months?	☐	☐	: Provide number of actual data breaches : Did any of these breaches involve personal data : Provide details of the breaches involving personal data, including whether they were reportable to a Controller or Data Subject (attached as a separate sheet if necessary).

Supplier Information Security Questionnaire

				■: Identify steps taken to mitigate the risk of future similar breaches.
5.4	Has your organisation had any personal data breaches which were reportable to the ICO in the last 2 years?	☐	☐	■: Provide number of reportable data breaches ■: Provide details of the reportable breaches (attached as a separate sheet if necessary). ■: Identify steps taken to mitigate the risk of future similar breaches.
5.5	Has your organisation received any complaints from data subjects in respect of your treatment of their personal data?	☐	☐	■: Provide further information and describe the steps taken to respond to the complaints.

SECTION 6: Specific Data Processing Activities

	INFORMATION PROCESSED ON BEHALF OF THE GROWTH COMPANY	
6.1	Do you formally classify documentation? If so, what categories do you use?	
6.2	Describe the categories and type of data processed by your organisation on behalf of the Growth Company. Tick here if the data contains personal and/or special category data ☐	
6.3	In what format(s) is the data stored? e.g data files, audio, image, paper.	
6.4	What arrangements do you have in place for archiving hard copy data and ensuring it is retained in line with contractual requirements?	
6.5	What physical and logical controls do you have in place to segregate Growth Company data from data you are processing for other clients?	

Supplier Information Security Questionnaire

SECTION 7: Information Security (detailed)

	REQUIREMENT	STATUS		FURTHER INFORMATION
		Yes	No	■: Where 'No' has been ticked, please explain why this is the case and provide further details on the current controls/processes that are in place.
	Requirement – Firewall Security			**Further Information**
7.1	Have you installed Firewalls or similar devices at the boundaries of your network?	☐	☐	■:
7.2	Have the default usernames/passwords on all boundary firewalls (or similar devices) been changed to a strong password?	☐	☐	■:
7.3	Have all open ports and services on each firewall (or similar device) been subject to justification and approval by an appropriately qualified and authorised business representative, and has this approval been properly documented?	☐	☐	■:
7.4	Confirm that there is a corporate policy requiring all firewall rules that are no longer required to be removed or disabled in a timely manner, and that this policy has been adhered to	☐	☐	■:

Supplier Information Security Questionnaire

	(meaning that there are currently no open ports or services that are not essential for the business).			
7.5	Confirm that any remote administrative interface has been disabled on all firewall (or similar) devices. Please provide documentation or screenshots of these secure methods.	☐	☐	■:
7.6	Confirm that where there is no requirement for a system to have Internet access, a Default Deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the Internet. Please provide evidence of a default deny policy being enforced.	☐	☐	■:
	Requirement – Secure Configuration			**Further Information**
7.7	Have all unnecessary or default user accounts been deleted or disabled?	☐	☐	■:
7.8	Confirm that all accounts have passwords, and that any default passwords have been changed to strong passwords.	☐	☐	■:
7.9	Has all unnecessary software, including OS utilities, services and	☐	☐	■:

Supplier Information Security Questionnaire

	applications, been removed or disabled?			
7.10	Has the Auto Run (or similar service) been disabled for all media types and network file shares? Please provide evidence that this setting is in place to ensure it has been disabled.	☐	☐	:
7.11	Has a host-based firewall been installed on all desktop PCs or laptops, and is this configured to block unapproved connections by default? Please submit evidence on which firewalls are in use and a screenshot of rules configured.	☐	☐	:
7.12	Is a standard build image used to configure new workstations, does this image include the policies and controls and software required to protect the workstation, and is the image kept up to date with corporate policies? Please provide evidence on how the build process is managed and screenshots of such security policies in place.	☐	☐	:
7.13	Do you have a backup policy in place, and are backups regularly taken to protect against threats such as ransomware? Please provide evidence of configured backup jobs and frequency of these backups.	☐	☐	:

Supplier Information Security Questionnaire

7.14	Are security and event logs maintained on servers, workstations and laptops?	☐	☐	■:
	Requirement – Access Control			**Further Information**
7.15	Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?	☐	☐	■:
7.16	Are accounts removed or disabled when no longer required?	☐	☐	■:
7.17	Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorised individuals?	☐	☐	■:
7.18	Do you have a documented password policy which requires strong complex password?	☐	☐	■:
	Requirement – Malware Protection			**Further Information**
7.19	Does corporate policy require all malware protection software to have all engine updates applied, and is this applied rigorously? Please provide evidence of which malware protection you are using and the frequency of updates.	☐	☐	■:

Supplier Information Security Questionnaire

7.20	Have all anti malware signature files been kept up to date (through automatic updates or through centrally managed deployment)?	☐	☐	■:
7.21	Has malware protection software been configured for on-access scanning, and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning? Please provide evidence this is in place.	☐	☐	■:
7.22	Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function? Please provide evidence of what systems are in place.	☐	☐	■:
	Requirement – Patch Management			**Further Information**
7.23	Are all Operating System security patches applied within 14 days of release or do you have a patch management policy that states patch management releases?	☐	☐	■:
7.24	Is a mobile working policy in force that requires mobile devices (including BYOD) to be kept up to date with vendor updates and app patches?	☐	☐	■:

Supplier Information Security Questionnaire

	Requirement – Business Continuity and Encryption			Further Information
7.25	Do you have a business continuity/and or disaster recovery plan?	☐	☐	■:
7.26	Have you conducted a test of your business continuity and disaster recovery plan within the last 12 months?	☐	☐	■:
7.27	In the event of a major outage at your system provider(s), would your ability to provide the Growth Company services be unaffected.	☐	☐	■:
7.28	Will the information you are holding on behalf of The Growth Company be encrypted during transit?	☐	☐	■:

Declaration			
I declare that to the best of my knowledge the answers submitted to these questions are correct and I am authorised to sign on behalf of my organisation. I understand that GC may reject my application if there is a failure to answer all relevant questions fully or if I provide false/misleading information.			
Name		Role	
Date		Authorised Signature	

Supplier Information Security Questionnaire

To be Completed by the GC Contract or Supply Chain Manager			
	Pass, Fail or Remedial Action Plan		**Please explain reasons for Fail or Remedial Action Plan**
SECTION 4: Data Governance (detailed)			
SECTION 5: Data Breaches			
SECTION 6: Specific Data Processing Activities			
SECTION 7: Information Security (detailed)			
Signed:		**Date:**	
Remedial Action Plan agreed by:		**Date:**	

Annex 1 – Evaluation Guidance

Supplier Information Security Questionnaire	
Criteria	**Weighting**
Section 1: Background Information	Information Only
Section 2: Data Governance	Pass or Fail
Section 3: Information Security	Pass or Fail
For Critical Suppliers Only	
Section 4: Data Governance (detailed)	Pass or Fail
Section 5: Data Breaches	Pass or Fail
Section 6: Specific Data Processing Activities	Information Only
Section 7: Information Security (detailed)	Pass or Fail

Supplier Information Security Questionnaire

The scored sections of the questionnaire will be marked according to the below methodology.

Scoring Method

Pass	Organisation provides adequate assurance of data security for our data and information and those of our clients
Fail*	Supplier fails to provide assurance that data will be held and processed in accordance with the Data Protection Act 2018 and is therefore considered to represent a significant and unacceptable risk to GC. In these circumstances, in GC's sole opinion, the supplier lacks sufficient capability and capacity to rectify the insufficiencies in data protection arrangements the organisation has in place in a suitable time period. Where the supplier is failed, GC is unable to work or contract with the supplier. If a contract is already in place it may be terminated on this basis.
Remedial Action Plan	Where the provider has partially failed the evaluation, a remedial action plan may be put into place with the partner. The Action Plan cannot exceed 6 months to deliver and failure to achieve the requirements of the Action Plan will result in the supplier failing the questionnaire (see above). Extensions for completion of the Action Plans will NOT be granted under any circumstances.

Annex 2 - References and Useful Links

Data Protection and Cyber Essentials
Cyber Essentials was developed by central Government to improve cyber security. You can find out more about cyber security by following this link https://www.ncsc.gov.uk/ and more about Cyber Essentials and Cyber Essential Plus at the following website: https://www.cyberessentials.ncsc.gov.uk/

Centre for Assessment, one of The Growth Company's subsidiaries provides Cyber Essentials and Cyber Essentials Plus, alongside ISO27001 services. You can find out more information here.
https://www.centreforassessment.co.uk/all-services/information-cyber-security/cyber-essentials/
There are other suppliers who provide similar services and suppliers are under no obligation to engage with CFA for this service.