LAMBLEY PRIMARY SCHOOL

Reaching for the Stars

PROCUREMENT STAGE 2: EVIDENCE

Approved by	Full Governing Body
Date Approved	5.3.19
Version	1
Review Date	March 2022

Use this form where a winning bidder has been identified for a service which will process higher risk personal data. The preferred bidder will be required to supply evidence to support the assurance statements given at stage 1.

Procurement Stage 2 – Evidence

1. Key Points

1. All activities which involve personal and/or sensitive personal data must comply with the Data Protection Act 1998 (DPA) and from May 2018, the General Data Protection Regulations 2016 (GDPR). The Organisation, as Data Controller for the data under this contracted work, must ensure that you as the Data Processor are fully aware of how data must be handled to comply with the law. In order to do so, we need to understand the general practices you employ with regards to data management in order to provide assurance to us and the Data Subjects to whom we are accountable.

2. If you undertook the previous stage of this procurement you will have stated that you comply with the requirements of Data Protection law. This stage of the process requires that you focus in more detail on your compliance with principle 7 (DPA) becoming principle 5(1)(f) (GDPR) to determine whether your technical and organisational measures appropriately manage the risk of unauthorised or unlawful processing and accidental loss/ destruction or damage to personal data.

3. Our requirements are based on the Cyber Essentials Plus scheme and the '10 Steps To Cyber Security' publication, both developed by the UK Government, along with the Information Commissioner's Office's 'Guide to IT security for the small business' and industry good practice. If you were required to undertake the first stage of this process, you will have confirmed that you meet our requirements by answering "Yes" to a number of compliance statements. Where this is the case, this questionnaire now requires you to provide detail and evidence to support those statements. In addition to being used as the second stage of a contract process, and irrespective of whether you have undertaken the first stage, this questionnaire is also used as a mandatory periodic review of continued compliance for contract holders.

4. The questions asked apply to the winning bidder (or existing contract holder, in the case of reviews), their partners, and any sub-contractors they use (or intend to use) to provide the solution/service. This includes any other parties that access, process, store or communicate information, or provide IT infrastructure components/ services. It is your responsibility to answer the questions on behalf of all parties involved after gaining detail and evidence from them to prove their compliance.

5. To comply with technical measures 1 to 5 below, medium and large organisations need to have either gained Cyber Essentials Plus certification, or be able to provide us with assurances and independent evidence that they meet the controls. For smaller organisations, the assessment of controls said to be in place will be performed by us. Guidance is provided later in this document for the size categories of organisation. Assurance is required to be refreshed periodically.

6. Any response that:
   - does not fully meet our requirements,
   - cannot be supported with sufficient evidence, or
   - is subsequently found not to comply when reviewed

   will require the bidder (or contract holder in a review) to take action so that their practices become compliant.

7. Please read the Information Commissioner's Office (ICO) guidance on the following link: The Guide to Data Protection to support your responses, and for further queries regarding Data Protection law and its application to your business, please contact the ICO for guidance (www.ico.org.uk or telephone 01625 545745)

2. Instructions

1. Please read the guidance provided in full before answering the questions.

2. Please read the requirements in the 'Question' column, and then provide a response to them in the adjacent 'Answer' column. Please do not provide this response on a separate document. The guidance will have told you what needs to be covered and supplied.

3. Use the links under each question ('Help Text') for guidance on what your response should cover, and ensure you use the Business Categories guidance to identify the correct requirements for the solution/service you are (or will be) providing.

4. When you attach supporting evidence (e.g. a policy document or copy of a certificate) to this document, please ensure that you reference the document title of the attachment accurately from within this document. If you are drawing attention to a specific comment or section within a supporting document, please ensure this is also fully and accurately referenced (section and page number).

5. If you are responding to this questionnaire as part of an annual review, please additionally specify any changes to processes and controls that have been made since you last responded.

3. Your Details

1	**Name of Company / Individual:** (Help text)	
2	**Contact Details:** (Help text)	
3	**Contact reference:** (Help text)	

4. ICO Notification

Duty to 'Notify' the ICO		Answer	
1	Have you complied with the duty to notify the Information Commissioner's Office that you are processing personal data? (What's required?)	☐ Yes (Go to Q2)	☐ No (Go to Q3)
Link to Notification Register Page		Answer	
2	Please provide a working link to your current notification record on the ICO's Register of Data Controllers. (What's required?)	*Please replace this text with a link*	
Notification Self-Assessment ***Only answer this question if you have not 'notified'.***		Answer	

3	If you believe that you do not need to notify, have you undertaken the ICO's self-assessment check? (What's required?)	☐	**Yes**, we do need to notify and we will do so within four weeks of submitting this questionnaire	☐ **No**, we do not need to notify. See below
				Please replace this text with the reason

5. Organisational Measures

Policies		Answer
1	What Information security/ governance/ management policies do you have in place? What subject areas do they cover? What is the review and approval process? (What's required?)	*Please replace this text with a detailed answer and attach evidence*
Security Awareness & Training		Answer
2	How do you ensure Security Awareness throughout the organisation to a level appropriate to your defined roles and responsibilities? (What's required?)	*Please replace this text with a detailed answer and attach evidence*
Information Risk Assessment and Management		Answer
3	What programme and processes do you have in place to effectively manage Information Risk? What is your approach to making risk assessments and how do you identify, assign and monitor risk controls? What were the results of your risk assessment? (What's required?)	*Please replace this text with a detailed answer and attach evidence*
Security Incident Response and Recovery		Answer

4	Has the organisation defined and implemented an Information Security Incident Response and Disaster recovery capability? Has it produced and tested Information Security Incident Management Response plans, and trained the incident management team appropriately? (What's required?)	*Please replace this text with a detailed answer and attach evidence*

6. Technical Measures

Secure Configuration and Maintenance of ICT Systems		Answer
1	How have the ICT systems in the solution/service provided (or to be provided) been configured, to ensure they are secure, and how are their configurations maintained? (What's required?)	*Please replace this text with a detailed answer and attach evidence*
Protecting Network and Devices from Attack		Answer
2	How are the networks in the solution/service provided (or to be provided) protected from external and internal attack? (What's required?)	*Please replace this text with a detailed answer and attach evidence*
Account Provisioning and Approval Process		Answer
3	What is the user account provisioning process (account approval, creation, maintenance and deactivation) in the solution/service provided (or to be provided), and how is privileged access controlled? (What's required?)	*Please replace this text with a detailed answer and attach evidence*
Malware Protection		Answer
4	How are the ICT Systems used in the solution/service provided (or to be provided) protected from Malware? (What's required?)	*Please replace this text with a detailed answer and attach evidence*
Keeping Software up-to- date and Secure		Answer
5	What process is used to keep the software on the ICT Systems in the solution/service provided (or to be provided) up to date? How does it ensure the prompt	*Please replace this text with a detailed answer and attach evidence*

	installation of the latest software updates and security patches? (What's required?)	
Logging and Monitoring		Answer
6	What event logging and monitoring is performed on the ICT Systems and Networks used in in the solution/service provided (or to be provided)? (What's required?)	*Please replace with a detailed answer and attach evidence*

7. Guidance

1. In order to assist the supplier in responding to the requirements stated, guidance notes have been provided on the pages that follow. The guidance starts with a section on the use of Third parties and the Cloud, which applies to all the organisational and technical measures if the cloud and / or third parties form part of the solution/service provided (or to be provided). It then goes on to provide examples of the controls the supplier (and any third parties it uses) need to have in place to comply with each requirement, and the detail and evidence of these they need to provide to us for review.

2. As the size of organisations providing services to us varies, the guidance has been split in to two Business Categories to help you understand the requirements, based on your IT setup. Please identify which category your organisation falls under, and then read the guidance provided for that category.

3. Where the organisation falls into the 'Medium or Large' category, they must either provide us with Cyber Essentials Plus certification evidence to review, or assurances and independent evidence that they meet the Cyber Essentials controls. It must include covering the controls that Cyber Essentials specifies as required (see the Cyber Essentials Common questionnaire), and equivalent assessment and testing (see the Cyber Essentials Common Test Specification).

4. Where the organisation falls into the 'Small Business' category, has no designated IT function, and has not had its controls independently assessed (like in Cyber Essentials Plus), we will assess the controls the organisation states in this questionnaire are in place by reviewing the details and evidence provided. This is only possible where sufficient information is provided.

5. Evidence can be presented in the in the form of 'screen shots' (showing software and settings in place), as well as copies of policies, diagrams, designs, registers and reports (or screen shots / extracts from these). If evidence is requested and is not available, please provide details instead. All evidence must be clearly labelled and linked to the question asked

6. The abbreviation 'ICT' stands for Information and Communications Technology, which covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form, e.g. Desktop computers, laptops and servers

Business Categories

Small Business Category	Corporate IT Category
Possible scenarios may include: • Self-employed or Micro business (0 to 9 employees) • Small business (10 – 49 employees) without a designated IT function • Simple IT configuration – maybe single device storing our data. • Simple IT configuration plus use of cloud services such as webmail or cloud storage containing our data. • Simple IT configuration plus a third party provider processing or storing our data.	Possible scenarios may include: • Medium business (50 to 249 employees) • Large organisation (250 + employees) • Any size organisation with a designated IT function • Likely to include servers, networks, end user devices and firewalls. • More complex IT configuration with central management of services. • Private or corporately managed cloud services used to store our data. • Third parties providing additional services and processing or storing our data.

Securing data in the Cloud and checking third parties

Small Business Category	Corporate IT Category
A wide range of online services require users to transfer data to remote computing facilities – commonly known as the cloud. Data being processed in the cloud represents a risk because the personal data you are responsible for leaves your network and be processed in systems managed by your cloud provider. It is therefore important to check that they have security measures in place: • Make sure you know what data is stored in the cloud, as modern computing devices, especially those targeted at consumers, can have cloud backup or sync services switched on by default. • Ensure you know in which country your cloud service provider hosts its data and whether the locations they use comply with the requirements of Data Protection law. • Check whether your cloud service provider complies with the CESG Cloud Security Principles • Consider the use of two factor authentication especially for remote access to your data in the cloud. • Check that third parties are treating your data with at least the same level of security as you would. • Ask for a security audit of the systems containing your data. • Review copies of the security assessments of your IT provider. • If appropriate, visit the premises of your IT provider to make sure they are as you would expect. • Check the contracts you have in place. They must be in writing and must require your contractor to act only on your instructions and comply with certain obligations of data protection law • If you use a contractor to erase data and dispose of or recycle your IT equipment, make sure they do it adequately / securely.	Ensure that the CESG Cloud Security Principles are being adhered to. The principles are: • Data in transit protection • Asset protection and resilience • Separation between consumers • Governance framework • Operational security • Personnel security • Secure development • Supply chain security • Secure consumer management • Identity and authentication • External interface protection • Secure service administration • Audit information provision to consumers • Secure use of the service by the consumer Source – CESG Cloud Security Principles

Source – A practical guide to IT security Ideal for the small business (Information Commissioner's Office)	

Your Details

		Small Business Category	Corporate IT Category
1	**Name of Company / Individual** (return to requirement)	*Details required* Provide the name of the company or organisation you are representing in bidding for this contract	Details required As per Small Business category
2	**Contact Details:** (return to requirement)	*Details required* • Provide the name of the individual who is acting as the main point of contact for your company • Please supply an Email address • Please supply a Postal address • Please supply a work Telephone number	Details required As per Small Business category
3	**Contact reference:** (return to requirement)	*Details required* • Please provide the reference number for the procurement you are bidding for	Details required As per Small Business category

ICO Notification

		Small Business Category	Corporate IT Category
1	**Duty to 'Notify' the ICO** (return to requirement)	*Details required* • Please tick 'yes' if you have a current entry on the ICO's register of Data Controllers, and will maintain a current entry for the duration of this contract • Please tick 'no' if the above is not the case	Details required As per Small Business category
2	**Link to Notification Register Page** (return to requirement)	Details required • Please provide a working URL link to the specific page in the register of Data Controllers which contains your company's entry	Details required As per Small Business category
3	**Notification Self-Assessment (Only answer this question if you have not 'notified')** (return to requirement)	*Details required* • Please do not respond to this question if you have answered 'Yes' to question 1 • Please undertake the check and advise of the outcome by ticking one of the boxes. • The result will either be that: • *Yes, you do need to notify the ICO. You will need to do this within the next four weeks. Or;* • *No, you do not need to notify. Please state in the below box why you do not need to notify.*	Details required As per Small Business category

1. Policies (return to requirement)	
Small Business Category	**Corporate IT Category**
Please read key point 4 on page 1, then provide evidence of any Information security policies your organisation has in place, along with evidence that they are signed off by management, regularly reviewed and evaluated for effectiveness. If you don't have dedicated policies, please note down what your policy on Information Security is (including acceptable and secure use of systems) and provide it to us for review. Some information is available on policies in A practical guide to IT security Ideal for the small business from the Information Commissioner's Office, and examples of such polices are provided free by the SANS Institute	Please read key point 4 on page 1 then provide evidence of the policies your organisation has in place covering Information Security and acceptable and secure use of the organisation's systems, including: • What they cover and how • How often they are reviewed • Who agrees and signs them off • How they are checked for effectiveness • How it is ensured they are adhered to and whether adherence is a condition of employment In addition to the guidance provided in the adjacent 'Small Business' category, further information can found in the UK Governments 10 Steps to Cyber Security publication, and ISO 27001:2013 (Clause 5.2 and section A.5 (Annex A), ISO 27001:2013)

2. Security Awareness and Training (return to requirement)

Small Business Category	Corporate IT Category
Please read key point 4 on page 1, then provide details (and evidence where specified) of the following: • Details of how / if employees at all levels are made aware of their roles and responsibilities. • Evidence of security awareness being promoted within the organisation, and details of how this is accomplished • Details of how staff keep their knowledge of security threats up-to-date • Evidence of training provided to staff so they recognise threats such as phishing emails and other malware, and risks involved in posting information relating to business activities on social networks, and details of how this is accomplished *Source:* Information Commissioner's Office guide and UK Government guide on IT Security for Small business, plus best practice	Please read key point 4 on page 1, then provide details (and evidence where specified) of the following: A) **Programme:** Describe the process which provides and maintains security awareness, to include: • Identification of specific roles which require tailored training and awareness • How users have been made aware of their information security responsibilities relative to their roles • Evidence of the staff induction processes to include general responsibilities for Information Security • Evidence of routine training provided to employees on their Information Security responsibilities (including refresher training) • Details of measures taken to monitor the effectiveness of the process • Evidence of promoting a security incident reporting culture within the organisation B) **Change:** Explain how new Cyber threats, risks to the organisation and legislation/ policy change are communicated and provide examples as evidence C) **Skills:** Explain how employees are encouraged to assess, develop and validate their Information Assurance skills, and provide evidence Source –10 Steps to Cyber Security (HM Government)

3. Information Risk Assessment and Management (return to requirement)

Small Business Category	Corporate IT Category
Please read key point 4 on page 1, then provide details (and evidence where specified) of the following: • Evidence of the identification and assessment of information security risks, as a result of delivering the service us. If this has not been undertaken, please perform an identification and assessment exercise, and provide the results to us for review. • Details of the severity of the risks your organisation has identified • Details of the actions taken to resolve the risks identified. • If risks have been identified but no actions taken to resolve them, please note down the organisations proposals on reducing their impact, or resolving them • Evidence of written security arrangements in place with any third parties used to deliver the service to us • Details of actions taken to address the risks presented from 'mobile working' (including working from home/ remote/ another location), if it is performed. • Details of how the locations used to process / store our data are 'Physically' protected from unauthorised access. The Physical security of equipment is important to consider as devices containing personal data could be stolen in a break-in or lost whilst away from the office. Information Commissioner and UK Government IT Security guides for Small business, the CPNI Perimeters and Access Control guidance	Please read key point 4 on page 1, then provide details (and evidence where specified) of the following: A) Programme: Evidence of the approach to information risk management to include: • Policy or policies which mandate the programme, describing the content • Defined roles and responsibilities showing clear ownership of the programme's activities • How role holders are made aware of their responsibilities • Applicability to any third parties who process data on your behalf • The review process to monitor the effectiveness of the programme • How new (or changes to existing) systems or processes are assessed for risk, with reference to the requirements of the ICO's Conducting Privacy Impact Assessments Code of Practice B) Risk Assessment: Evidence of the Information Security Risk assessment performed on the service to be provided, including: • How risks are identified • How risks are recorded; ensuring they are dated, consistently graded and described CONTINUED ON NEXT PAGE

	C) Controls: Details of how appropriate controls are identified, implemented and monitored, to include: • How controls are identified and understood and their effectiveness in reducing risk is monitored and recorded • Details of Physical security controls in place, including Perimeter security, Physical entry controls (door entry), Swipe cards, Picture ID cards, Secure area security, Monitoring, CCTV, Visitor access, Security guards, Cable protection and Loading bay protection How appropriate ownership of risks is ensured and recorded • How the level of risk tolerance is determined, and embedded in the assessment process • Whether information security controls are established and agreed with each third party that may access, process, store, communicate, or provide IT infrastructure to our data, and how compliance monitored • Evidence of the change control process, including details of notification to affected stakeholders • Treatment of issues caused from unplanned changes CONTINUED ON NEXT PAGE

	D) Mobile Working: Evidence of managing / controlling the risk from working from home/ remote/ another location, including: ○ Whether there is an increased level of monitoring on all remote connections and the corporate systems being accessed ○ How and if the amount of information stored on mobile devices in minimised to only that which is needed to fulfil the business activity ○ Whether full disk encryption is installed on mobile devices, and where this is not possible, the data held on the devices is encrypted ○ Whether when working remotely and connecting back to a corporate network, devices and the information exchange is protected by using an appropriately configured Virtual Private Network (VPN) ○ E) Administrator accounts: Details of the approach to controlling the risks with administrator accounts, how they are managed and how they access network components Source –10 Steps to Cyber Security (HM Government), CPNI Perimeters and Access Control guidance, and ISO 27001:2013, Annex A, Section 11 – 'Physical and environmental security', and Section 15 – 'Supplier Relationships'

4. Information Security Incident Response and Recovery (return to requirement)

Small Business Category	Corporate IT Category
Please read key point 4 on page 1, then provide details (and evidence where specified) of the following: • Evidence that the organisation has considered what measures need to be put in place to deal with data breaches, should one occur. Please include a copy of the organisations incident management plan, if it has one, or if not, note it down and provide to us for review. • Evidence of reviews held on the personal data the organisation currently holds / processes, including details on whether the protection was found to be adequate • Evidence of reviews undertaken to ensure the organisation is compliant with industry guidance or other legal requirements. • Evidence of reviews undertaken on the controls in place, including detail of how often the reviews are performed, and how any improvements required are identified • Evidence of the monitoring and adjustment of the controls in place • Evidence of alternate locations identified where the organisation could perform the service from, in event of the usual location becoming unavailable • Evidence of arrangements / plans in place to repair, replace, or use alternate PC's and systems, in the event of a failure • Evidence that any security incidents that have occurred, have been analysed, to identify actions that can be taken to prevent them occurring again *Based upon:* A practical guide to IT security Ideal for the small business (Information Commissioner's Office) and Best Practice	Please read key point 4 on page, then provide details (and evidence where specified) of the following: A) Evidence of Incident Management plan(s) in place, including: • What the plan(s) cover, whether they cover the full range of incidents that may occur, and the support from senior management • Roles and responsibilities identified, how these have been communicated, and how training needs are identified and met • Reporting incidents of a criminal nature and management • Data recovery facilities available / how they're engaged • Testing of incident management and supporting plans (Business Continuity and Disaster Recovery), and its frequency • How and if it is ensured that Information Security is maintained when Business Continuity plans have to be invoked • Staff incident management awareness training performed • Reporting of incident statistics, analyses and feed into lessons learnt and training need reviews • The formal disciplinary process undertaken if policies are demonstrated to have been breached B) Evidence of the process for identifying, managing and resolving information security breaches , including: • Reporting to the appropriate role/ team, and action tracking recording, for response and recovery, and for later review • Investigated by the appropriate role/ team

	• Escalated to senior roles and what determines this • Notified to data controllers and the ICO and what determines this • Resolved and closed Source-10 Steps to Cyber Security (HM Government) and best practice

Technical Measures

1. Secure Configuration and Maintenance of ICT systems (return to requirement)	
Small Business Category	**Corporate IT Category**
Please read key point 4 on page 1, then provide details (and evidence where specified) of the following: • Details on identifying software and services on the organisations computers, and subsequently removing it, to reduce the number of potential vulnerabilities. • Details of changing the default password in the software and hardware used • Details of disabling or removing unnecessary user accounts • Details of removing software that is no longer supported (or where security updates are not provided) by manufacturers. • Evidence of 'standard' user accounts being used by users, rather than 'administrator' accounts • Evidence of encryption software being used where appropriate. e.g. Full disk and File encryption • Details of the organisations promotion and use of strong passwords • Evidence that removable media (such as memory sticks) is being controlled and managed appropriately • Evidence of 'Remote Wiping of data' being enabled on the organisations mobile devices, where possible / required • Evidence of disabling the 'Auto-run' feature on removable media (and network drives where used) where possible • Details on taking regular backups *Based on:* Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	Please read key points 4 & 5 on page 1, then provide details (and evidence where specified) of the following: • Evidence of baseline security builds created for workstations, servers, firewalls and routers, and operating system and software lockdowns performed • Details of disabling or removing unnecessary user accounts, and changing default passwords on user accounts • Evidence of removing / disabling unnecessary software and services on computers • Evidence of removable media controls and management in place, including restricting use, types of media allowed, type of information permitted to be stored, encryption used, and secure destruction • Evidence of hardware and software inventories in place and device tracking • Evidence of vulnerability scans performed, including details of how regular they are, what scanning tools are used, and the timescales • Evidence of disabling Auto-run on network drives +removable media • Details on taking regular backups • Evidence of maintaining security and event logs. • Cyber Essentials Plus certification evidence (or Independent evidence – See Guidance) that covers annual assessment and testing, and includes the Secure Configuration controls in place

	Source – Cyber Essentials Scheme +10 Steps to Cyber Security (HM Government

2. Protect networks from Internal and external attack (return to requirement)	
Small Business Category	**Corporate IT Category**
Please read key point 4 on page 1, then provide details (and evidence where specified) of the following: • Details of the firewall(s) installed at the boundary of the public network (Internet) and the organisations private network. Routers commonly have these built in to them. Include confirmation that the firewalls default password has been changed. • Evidence of disabling or protecting the firewalls remote administrative interface. • Evidence of personal firewalls installed on the organisations computers. These are software applications that control network traffic to and from a computer, permitting or denying communications based on a security policy. They often come as part of anti-malware packages, and the operating system. • Details of any Internet gateways in place / used, or methods used to prevent (or discourage) users within the organisation from accessing websites or other online services that present a threat or that you do not trust *Based on:* Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	Please read key points 4 & 5 on page , then provide details (and evidence where specified) of the following: • Details of Network perimeter protection, including whether the defence is multi-layered and whether there is protection between the untrusted external network and the trusted internal networks • Details of Internal network protection, including details of firewalls or equivalent network devices installed on the boundary of the internal network(s). Include details of changing default firewall passwords. • Evidence of the firewall rule management and approval process, and the justification and approval of firewall port opening • Evidence of the disabling of unapproved services or services typically vulnerable to attack at the boundary firewall • Evidence of disabling or protecting the firewalls remote administrative interface. • Evidence of Network monitoring performed, including details on whether intrusion monitoring tools are used, and the policy on auditing activity logs. • Evidence of personal firewalls installed, and their configuration • Evidence of testing performed – regular penetration tests and simulated cyber-attack exercises for instance. • Where there is no requirement for a system to have Internet access, implement a 'Default Deny' policy, thus preventing Internet access

	• Cyber Essentials Plus certification evidence (or Independent evidence – See Guidance) that covers annual assessment and testing, and includes the Network controls in place. Base on: Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice.

3. Account provisioning and approval process (return to requirement)	
Small Business Category	**Corporate IT Category**
Please read key point 4 on page 1, and then provide details (and evidence where specified) of the following: • Evidence of the organisations Access Control Policy, if it has one, or details of how access to systems is controlled. • Details of how it is ensured that all the organisations users are assigned unique usernames and passwords, do not share them, and require them to logon to computers and applications. • Details of how the organisation ensures that its users only have permissions appropriate to the role they perform, and these permissions are regularly reviewed and documented • Details on disabling users accounts that are no longer required • Evidence of the restriction of Administrator accounts / their use, and the changing of their passwords at least every 60 days • Details of how strong password use is enforced / promoted • Evidence of the limiting of failed logon attempts. Login should be prevented after a small number of unsuccessful logins, to prevent what's known as a 'Brute Force' attack, where login attempts keep being made by a computer, until the correct one is generated. • Evidence of enforcing regular password changes • Details of how the organisation ensures that passwords are cancelled immediately upon staff members leaving, or being absent for long periods *Based on:* Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	Please read key points 4 & 5 on page 1, and then provide details (and evidence where specified) of the following: • Evidence of the Starters, movers and leavers process in place, including details of justification, provisioning, approval, and assignment to named individuals • Details on disabling or deleting leaver and inactive accounts • Details on the management of account privileges, including whether they are documented, how often they are reviewed, how it's ensured that all users have their own username and password, and are only granted the minimum access required to perform their roles. • Details of restrictions in place to minimise the number and use of Administrative accounts, ensure they are only used to perform legitimate administrative activities, and whether they have access to email or the internet. • Evidence of configuring user accounts to require regular password changes (and admin password changes at least every 60 days) • Evidence of actions taken to ensure the use of strong passwords • Details that demonstrate the authentication steps performed before users are granted network, system, application, or computer access • Evidence of user activity monitoring + controlled access to audit logs • Details of providing standard user accounts to administrators, to use when performing non-administrative actions • Cyber Essentials Plus certification evidence (or Independent evidence – See Guidance) that covers annual assessment and

	testing, and includes the account provisioning and approval controls and process in place Source – Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government)

4. Malware Protection (return to requirement)

Small Business Category	Corporate IT Category
Please read key point 4 on page 1, and then provide details (and evidence where specified) of the following: • Evidence of the malware protection (also known as anti-virus) installed on the organisations computers, and details of how it is kept up to date • Details of the malware protection configuration, including whether it is set to scan files upon access / download, and how the organisation ensures it remains switched on • Details of the scans for malware being performed on computers and the network, including the frequency. • Details of actions taken upon receiving an alert from the malware protection. • Details of the policy on scanning removable media, such as memory sticks, CD's and DVD's for malware, before use. • Details of any actions taken to deter (or preferably prevent) users from accessing information on potentially unsafe web sites. As well as there being dedicated software to perform this function (black listing), some anti-malware can perform these actions. There are also web browser add-ons that grade the likely safety of sites shown in search results. e.g. Web of trust *Based on:* Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	Please read key points 4 & 5 on page, and then provide details (and evidence where specified) of the following: • Evidence of Malware (viruses, worms, Trojans and spyware etc.) prevention policy and how it helps manage the risks to business processes, and includes the process of re-acting to an infection • Evidence of the malware protection defences implemented • Evidence of the Malware protection software used, including details of whether it is set to scan files upon access / download, and how it is kept up to date (engine and signatures) • Details of Malware scanning performed on computers and the network, and the frequency • Evidence of controls in place to prevent users from making connections to malicious websites on the internet (e.g. website blacklisting). • Evidence of preventing users from running executable code or programs form any media to which they also have write access • Details of policy on scanning removable media for malware • Cyber Essentials Plus certification evidence (or Independent evidence – See Guidance) that covers annual assessment and testing, and includes the malware protection controls in place. Based on: Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice.

5. Keeping software up-to-date and secure (return to requirement)	
Small Business Category	**Corporate IT Category**
Please read key point 4 on page 1, and then provide details (and evidence where specified) of the following: • Details of how its ensured that the software running on the organisations computers is licensed and supported, thus ensuring the availability of security patches • Evidence that the organisations computers are set to automatically download and apply security and software updates, or alternatively, (if it has been chosen to apply the updates manually) details of the process followed that ensures they are applied within 14 days of release. • Evidence that the organisations computers are set to automatically download anti-malware signature and engine updates, as and when they become available, in order to ensure they can protect against the latest threats. • Details of how often the security products installed on the organisations computers are reviewed, in order to ensure they are up to date, effective and supportable by their manufacturer • Details of keeping mobile devices (used for mobile working) up to date with vendor updates and app patches *Based on:* Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	Please read key points 4 & 5 on page 1, and then provide details (and evidence where specified) of the following: • Evidence of the defined patching process in place covering the installation of application software updates from vendors (including operating system and firmware) and Security patches, and details of how its ensured they are installed within 14 days of release. • Details of how its ensured that the software running on the organisations ICT Systems is licensed and supported, thus ensuring the availability of security patches • Details on how often checks are made for out-of-date software (i.e. software that is no longer supported.) that needs to be removed / replaced. • Evidence of regular reviews performed to ensure the protection in place on the organisations computers is adequate. • Evidence of keeping mobile devices (used for mobile working) up to date with vendor updates and app patches • Cyber Essentials Plus certification evidence (or Independent evidence – See Guidance) that covers annual assessment and testing, and includes the controls in place to keep software up-to-date and secure. Source – Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice

6. Logging and Monitoring (return to requirement)

Small Business Category	Corporate IT Category
Please read key point 4 on page 1, and then provide details (and evidence where specified) of the following: • Evidence of monitoring tools in place. Dedicated monitoring tools are available, but a number of anti-malware products (sometimes known as Internet Security) provide notifications of threats in real time, and not just those relating to infected files – Attempts to illegally access your computer for instance from the internet. • Details of how often the security software messages, access control logs and other reporting systems the organisation has in place are checked. • Details of actions that would be performed in the event of receiving an alert issued by a monitoring service. • Details of how the organisation makes itself aware of what software or services are running on its computers and network, so it can identify if there is something present that shouldn't be. • Evidence of vulnerability scans run to identify and address any vulnerabilities in the organisations computers. Dedicated vulnerability scanning tools are available, but basic vulnerability scanners are sometimes included in anti-malware suits. These scan your computer and tell you if any products are vulnerable and need updating *Source:* Information Commissioner's Office guide and UK Government guide on IT Security for Small business, plus best practice	Please read key point 4 on page 1, and then provide details (and evidence where specified) of the following: • Evidence of the monitoring strategy and supporting policies the organisation has implemented, and the basis for these, including whether it takes into account previous security incidents and attacks and aligns with the organisation's incident management policy • Evidence of the network monitoring in place, how often it occurs, how and if inbound and outbound network traffic traversing the network boundaries is monitored, and how unusual activity or trends that could indicate an attack, are identified. • Details of the user activity monitoring performed and whether it complies with legal and regulatory constraints • Details of the fine-tuning of monitoring systems performed so only relevant logs, events and alerts are collected • Details of the logs being captured and how they are protected • The frequency of log inspection, the method used to analyse logs for unexpected activity and how long logs are kept for • Details of how the organisation ensures there is sufficient log storage • Evidence of ensuring that the time on systems is synchronised, to ensure the accuracy in logs • Evidence of training provided to staff on logging and monitoring *Source* – Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government)

Other Sources of Guidance

The ICO website (www.ico.org.uk) provides comprehensive information and guidance on the Data Protection Act 1998 and the General Data Protection Regulations 2016. Please ensure you comply with the relevant information to maintain compliance with Data Protection law

Specific guidance provided by the ICO to help businesses comply with Data Protection law includes:

- The Guide to Data Protection
- Overview of the General Data Protection Regulations 2016
- CCTV Systems and the Data Protection Act 1998
- CCTV Small User Checklist (to be read with the above)
- Brief Guide to Notification
- Employment Practices Code – A Quick Guide (PDF)
- FAQ's for Organisations (on website)
- CCTV Data Protection Code of Practice
- Privacy and Electronic Communications Regulations
- Website FAQs for Organisations
- Good Practice Note – Buying and selling customer databases
- Good Practice Note – Checklist for handling requests for personal information (subject access requests)
- Good Practice Note – Electronic mail marketing
- Good Practice Note – Outsourcing: a guide for small and medium-sized businesses
- Good Practice Note – Providing personal information to a third party
- Good Practice Note – Releasing information to prevent or detect crime
- Good Practice Note – Subject Access and employment references
- Good Practice Note – Training checklist for small and medium-sized organisations