PROCUREMENT STAGE 1 – SELF ASSESSMENT

Approved by	Full Governing Body
Date Approved	5th March 2019
Version	1
Review Date	March 2022

Information Risk Questionnaire – Self-Assessment

Key Points

1. We have a number of requirements that bidders proposing a solutions/service must meet. These are based upon the UK government's Cyber Essentials Plus scheme and '10 Steps To Cyber Security' publication, along with the Information Commissioner's Office 'Guide to IT security for the small business', and the Data Protection Act 1998 (DPA); superseded by the General Data Protection Regulations 2016 (GDPR) from 25th May 2018.

2. The requirements are specified in a table below. The table also links to guidance and examples of the controls that must have been implemented, and actioned on an on-going basis, in order to comply with the requirement. Please check against the Business Categories section in the guidance, to identify which set of requirements are relevant to the solution/service you propose to provide. A full list of controls is not provided, but can be obtained by clicking on the links to the appropriate documents above.

3. The bidder, their partners, and sub- contractors/third parties involved in providing the solution/service must be able to comply with the requirements. This includes any parties that access, process, store or communicate information, or provide IT infrastructure components. It is the bidder's responsibility to respond on behalf of all parties involved, after checking their compliance with the requirements, and their ability to evidence they meet them. (Throughout this document "the bidder" means the bidder and any partners, third parties and subcontractors).

4. Requirements 1 to 5 require medium and large organisations to have either gained Cyber Essentials Plus certification, or be able to provide us 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 two size categories. Assurance is required annually.
5. The bidder's response must:
    a. Confirm whether or not the bidder (see key point 3) are able to fully meet the requirements specified (Yes or No)
    b. Confirm whether or not the bidder (see key point 3) is willing and able to complete the attached Information Risk Questionnaire (which requires both detail and evidence to be provided, rather than just 'Yes' or 'No'), should they be awarded the contract.
6. The Guidance provided must be reviewed before answering the questions.
7. Failure to confirm compliance with all the requirements in this questionnaire will result in a bid being rejected.

Requirements table

Ref	Requirement: Securely configure and maintain ICT Systems	Bidder's Response
1	The ICT systems used in the proposed solution/service must be securely configured and maintained. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No
Ref	**Requirement: Protecting networks from internal and external attack**	**Bidder's Response**
2	The networks used in the proposed solution/service must be protected from external and internal attack. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No
Ref	***Requirement: Account provisioning and approval process***	**Bidder's Response**
3	The proposed solution/service must include a user account provisioning process (account approval, creation, maintenance and deactivation), and a means of controlling privileged access. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No

Ref	***Requirement: Malware Protection***	**Bidder's Response**
4	The ICT systems used in the proposed solution/service must be protected from Malware. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No
Ref	***Requirement: Keep software up-to-date and secure***	**Bidder's Response**
5	There must be a process in place to keep the software on the ICT systems in the proposed solution/service, up to date. It must ensure the prompt installation of the latest software updates and security patches. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No
Ref	***Requirement: Logging and Monitoring***	**Bidder's Response**
6	The ICT Systems and Networks used in the proposed solution/service must have event logging enabled, and be monitored. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No

Ref	*Requirement: Information Risk Assessment and Management*	Bidder's Response
7	The bidder must have a documented Information Risk Management process in place, showing how it manages risk throughout its organisation. They must have undertaken a risk assessment on the solution/service being offered, and put measures in place to mitigate the risks found, to bring them to a low level. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No
Ref	***Requirement: Security Awareness***	**Bidder's Response**
8	The bidder must ensure Security Awareness throughout the Organisation. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No
Ref	***Requirement: Information Security Incident Response and Recovery***	**Bidder's Response**
9	The bidder must define and implement an Information Security Incident Response and Disaster recovery capability, produce and test information security Incident management response plans, and train the incident management team appropriately. Link: Further detail and control examples	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No

Ref	*Requirement: Data Protection Compliance*	Bidder's Response
10	The bidder must fully comply with the statutory obligations under the Data Protection law, and confirm that they will manage our information in line with the Data Protection Act 1998 and replacement legislation. The bidder must cooperate with Data Protection Compliance Audits as and when requested, as per the Organisation's Information Handling contract schedule. Link: Further details	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No
Ref	***Requirement: Information Risk Questionnaire (Winning Bidder)***	**Bidder's Response**
11	If confirmed as the winning bidder, the bidder must complete "Procurement Stage 2 – Evidence" at the Organisation's discretion, and repeat the process at a frequency to be determined in order to evidence ongoing compliance. Link: Further details	Do you confirm that your company (and any 3rd parties used) comply with this requirement, and are able to evidence it? ☐ Yes ☐ No

Guidance and control examples

We (and other organisations) are allowed to use a 'third party' data processor to process personal data on our behalf. Data Protection law contains special provisions that apply in those circumstances. It says that, where a data processor is to be used:

- The organisation must choose a data processor that provides sufficient guarantees about its security measures to protect the processing it will perform;
- The organisation must take reasonable steps to check that those security measures are being put into practice; and
- There must be a written contract setting out what the data processor is allowed to do with the personal data. The contract must also require the data processor to take the same security measures that the organisation would have to take if it were processing the data.

For the purposes of this questionnaire, the bidder (and any partners and sub-contractors it uses to deliver the solution/service) is seen as the data processor.

In order to assist the bidder 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 requirements 1 to 10, if the cloud and / or third parties form part of the bidder's solution/service. It then goes on to provide examples of the controls the bidder (and any partners and sub-contractors it uses) need to have in place to comply with each requirement. Should the bidder be successful and be awarded the contract, they will need to provide details on these controls and how they have been implemented, along with evidence to support it.

As the size of companies submitting bids will vary, the guidance has been split in to two business categories to help the bidder understand the requirements, based on their own IT setup. Please identify which category your organisation falls under, and then read the guidance provided for that category.

Where a bidder is successful and 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).

Where a bidder is successful, 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 they state as in place in the “Information Risk questionnaire’ they return, and review the evidence provided. The bidder should therefore be aware that they will need to be able to provide sufficient information, to make this possible.

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) with no 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 the DPA (then GDPR) • If you use a contractor to erase data and dispose of or recycle your IT equipment, make sure they do it adequately / securely. Source – A practical guide to IT security Ideal for the small business (Information Commissioner's Office)	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

Requirement 1 - Securely configure and maintain ICT Systems *(Return to Requirement)*

Small Business Category	Corporate IT Category

Almost all hardware and software requires some level of set-up and configuration in order to provide effective protection. Please read key point 3 on page 1 before considering the following:
 	
Examples
• Identify and remove software and services that are not required on the organisations computers, in order to reduce the number of potential vulnerabilities.
• Change the default passwords in all software and hardware used
• Remove software that is no longer supported (or where security updates are not provided) by manufacturers.
• Disable or remove any unnecessary user accounts.
• Use 'standard' user accounts for day-to-day work, rather than 'administrator' accounts that have higher privileges.
• Use Encryption software where required – This is a means of ensuring that data can only be accessed by authorised users and requires a (strong) password to 'unlock'. Example types are:
  ◦ Full disk encryption – Encrypts all the data on the computer
  ◦ File encryption – a method of encrypting individual files
• Use and promote the use of strong (complex) passwords
• Control the use of removable media (such as memory sticks)
• If available, setup a remote disable or wipe facility on mobile devices, to allow remote deletion, should a device be lost or stolen.
• Where possible, disable the 'Auto-run' feature on removable media (and network drives if used)
• Perform regular data backups to protect against threats such as ransomware
	This requirement requires appropriate 'Secure Configuration' controls to have implemented and be maintained on an on-going basis. Please read key points 3 and 4 on page 1 before considering the following:
	
	Examples
	• Create baseline security builds for workstations, servers, firewalls and routers.
	• Lock down operating systems and software and disable or remove default accounts and services, if no required.
	• Remove or disable software and services not required on devices
	• Strengthen passwords and remove software that is not required
	• Implement controls to manage/control access to removable media
	• Implement hardware and software inventories, and provide a means to track all the organisation's devices
	• Perform regular vulnerability scans and promptly resolve any vulnerabilities found
	• Perform regular backups
	• Maintain security and event logs on servers, workstations and laptops
	
	Based on: Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice

Based on: Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	

Requirement 2 - Protect internal and external networks from attack *(Return to Requirement)*

Small Business Category	Corporate IT Category
This requirement covers 'Boundary firewalls and Internet gateways', which are your first line of defence against an intrusion from the internet. Please read key point 3 on page 1 before considering the following: *Examples* • At the boundary of the public network (Internet) and the organisations private network, install a firewall(s) to protect the organisation, and change its default password. Routers commonly have these built in to them. A well configured firewall can stop breaches happening before they penetrate deep into the network. • Disable or protect the firewalls administrative interface (configuration settings etc.) from being accessed remotely • Install personal firewalls on your computers – These are software applications that control network traffic to and from a computer, permitting or denying communications based on a security policy. These often come as part of anti-malware packages • Implement a way of preventing users in the organisation from accessing websites or other online services that present a threat, or that you do not trust. This can be done by installing an Internet Gateway, or using some software that is aware of potentially dangerous sites, and warns the user before they reach the site, or blocks their access to it. *Based on:* Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	This requirement requires appropriate network security controls (including 'Boundary Firewalls and Internet Gateways') to have implemented and be maintained on an on-going basis. Please read key points 3 and 4 on page 1 before considering the following: *Examples* • Police the organisations network and implement multilayer defences • Protect internal networks, including installing firewalls / equivalent network devices on boundaries • Change the default password on the firewall(s) • Manage and control firewall rules and require justification and approval to open firewall ports • Disable unapproved or vulnerable services at boundary firewall(s) • Remove or disable firewall rules that are no longer required, in a timely manner. • Disable or protect the firewall administrative interface from being accessed remotely. • Perform network monitoring • Install personal firewalls and configure them to block unapproved connections by default • Undertake regular penetration tests • Where there is no requirement for a system to have Internet access, implement a 'Default Deny' policy and ensure it is applied correctly, thus preventing the system from making connections to the Internet

	Based upon: Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice

Requirement 3 - Account provisioning and approval process *(Return to Requirement)*

Small Business Category	Corporate IT Category
This requirement covers 'Access Control' which consists of restricting the access to your system(s) to only users and sources that you trust. Please read key point 3 on page 1 before considering the following: *Examples* • Create an Access Control Policy that states how the organisation controls access to its systems • Assign users their own unique username and password, ensure these are not shared, and require them to be used to logon to the organisations computers and applications. • Disable any user accounts that are no longer required • Ensure each user's account only has the access permissions their role requires, and these are regularly reviewed and documented. • Only use administrator accounts when strictly necessary (eg for installing known and trusted software), and change their passwords at least every 60 days. • Promote and enforce the use of strong passwords • Limit the number of times a user can type in the wrong logon ID and password, before locking their account. This helps in the prevention of brute force password attacks, where login attempts keep being made by a computer, until the correct one is generated. • Force users to change their password on a regular basis • Cancel passwords or other access immediately if a staff member leaves the organisation or is absent for long periods.	This requirement requires appropriate 'User Access Management 'controls and controls to manage user privileges, to have implemented and be maintained on an on-going basis. Please read key points 3 and 4 on page 1 before considering the following: *Examples:* • Define and Implement a starters, movers and leavers processes which includes justification, provisioning, approval, and assigning to named individuals • Ensure all users have and use their own username and password, and are only granted the minimum level of access their role requires • Regularly monitor for / disable inactive accounts, and those no longer required • Manage all account privileges, document and regularly review • Restrict the number of privileged accounts created / used, and ensure their passwords are changed at least every 60 days • Enforce regular password changes • Enforce the use of strong passwords • Control the use of administration accounts • Ensure adequate authentication is performed before granting users access to networks, systems, application and computers • Monitor accounts with access to sensitive information / privileged access

Based on: Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	Based on: – Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice

Requirement 4 – Malware protection *(Return to Requirement)*

Small Business Category	Corporate IT Category
This requirement requires you to protect your systems, computers and files from malicious code, known as malware (viruses, Trojans worms, ransomware etc.). Please read key point 3 on page 1 before considering the following: *Examples* • Install malware protection software (also known as anti-virus) products on the organisations computers, and keep it up to date. Anti-malware definitions (or signatures) tend to be updated frequently throughout the day, so setting your product to update automatically is the easiest option • Ensure the malware protection remains switched on and is configured to scan for malware as files are accessed / downloaded • Scan the organisations computers for malware daily, and if you are using a network, regularly scan it to detect and prevent threats • Ensure that alerts issued by malware protection products, are reacted to. • Scan removable media, such as memory sticks, CD's and DVD's for malware, before use. • Take action 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) and Internet Gateways, some malware protection software 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	This requirement requires appropriate 'Malware Protection' controls to have implemented and be maintained on an on-going basis. Please read key points 3 and 4 on page 1 before considering the following: *Examples* • Define and implement a policy on malware that helps manage the risks to business processes, and includes the process of re-acting to an alert / infection • Implement malware protection defences and ensure they are kept up to date (engine and signatures), and configured to detect malware when files are accessed / downloaded. This should form part of the malware policy • Perform daily scans for malware • Prevent users from making connections to malicious websites • Control what executable code (including macros and scripts) users can run. • Prevent malware infection from the use of removable media Based on – Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice

Based on: Information Commissioner and UK Government IT Security guides for Small business, and the Cyber Essentials Scheme	

Requirement 5 – Keeping software up-to-date and secure *(Return to Requirement)*

Small Business Category	Corporate IT Category
Perform regular maintenance on computer equipment and software, to keep it running smoothly and remove any security vulnerabilities. Please read key point 3 on page 1 before considering the following: *Examples* • Ensure all software installed on the organisations computers is licensed and supported • Regularly update security software such as anti-virus and anti-malware. This is required in order for it to continue to provide adequate protection. • Keep the operating system and the application software on the organisations computers up-to-date by checking regularly for updates and applying them. Ensure all security updates are installed within 14 days of release. Most software can be set to update automatically. • Perform regular reviews to ensure the protection in place on the organisations computers is still adequate. • Keep 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	This requirement requires appropriate 'Patch Management' controls to have implemented and be maintained on an on-going basis. Please read key points 3 and 4 on page 1 before considering the following: *Examples* • Ensure software running on ICT Systems is licensed and supported (by the software vendor or supplier) to ensure security patches for known vulnerabilities are made available for install • Define and implement a patching policy and process • Install software updates, firmware updates and security patches within a timely manner – Ensure all Operating System and Application security patches are installed within 14 days of release (or automatically when they become available from vendors). • Define and implement a policy on removing out-of-date software that's no longer supported • Perform regular reviews to ensure the protection in place on the organisations computers is still adequate. • Require mobile devices (including BYOD) to be kept up to date with vendor updates and app patches, as part of the mobile working policy Source – Cyber Essentials Scheme + 10 Steps to Cyber Security (HM Government) and best practice

Requirement 6 – Logging and Monitoring *(Return to Requirement)*

Small Business Category	Corporate IT Category
Cyber criminals or malware can attack your systems and go unnoticed for a long time. Many people only find out they have been attacked when it is too late. Monitoring the warning signs and acting on them assists with preventing this. Please read key point 3 on page 1 before considering the following: *Examples* • Check the security software messages, access control logs and other reporting systems the organisation has in place on a regular basis. 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. • Act on any alerts that are issued by monitoring services. • Make sure you know / are able to check what software and services are running on your network, so it can be seen if there is something there that should not be. • Run regular vulnerability scans - Basic vulnerability scanners sometimes form part of anti-malware suits (as well as being available separately). They scan your computer and tell you if any products are vulnerable and need updating. *Based on:* Information Commissioner and UK Government IT Security guides for Small business, plus best practice	This requirement requires appropriate 'Logging and Monitoring' processes to have been implemented, actively taking place and maintained on an on-going basis. Please read key point 3 on page 1 before considering the following: *Examples* • Define and implement a monitoring strategy that includes monitoring all networks and host systems, is based upon risk and takes into account any previous security incidents and attacks and aligns with the organisation's incident management policy • Monitor inbound and outbound network traffic traversing network boundaries • Monitor all user activity, but ensure it complies with legal and regulatory constraints • Fine-tune monitoring systems so they only collect relevant logs, events and alerts • Define the logs that will be captured and how they will be protected • Define log inspection frequency and the method of analysing logs for unexpected activity • Ensure there is sufficient log storage • Provide resilient and synchronised timing • Provide adequate training on monitoring Source – 10 Steps to Cyber Security (HM Government)

Requirement 7 – Information Risk Assessment and Management *(Return to Requirement)*

Small Business Category	Corporate IT Category

Before you can establish what level of security is right for your business you will need to review the personal data you hold and assess the risks to that data. You should consider all processes involved that require you to collect, store, use and dispose of personal data. Consider how valuable, sensitive or confidential the information is and what damage or distress could be caused to individuals if there was a security breach. With a clear view of the risks you can begin to choose the security measures that are appropriate for your needs. Please read key point 3 on page 1 before considering the following:
 	
Examples
• Assess what risks there are in you providing the service (what may stop you, what may go wrong / how could information breaches occur), and then determine if there is any action you can take to minimise them. Document your findings.
• Document the severity of the risks the organisation has identified
• Take action to resolve the risks identified as achievable.
• Where risks cannot be resolved, take action to reduce the impact they would have, should they occur
• Ensure security arrangements are in writing with any third parties the organisation works with, to deliver the service
• Take action to address the risks presented from 'mobile working' (including working from home/ remote/ another location), if it is performed.
• Ensure the location is physically secure and take action to resolve any issues found. 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.
	This requirement requires an information risk assessment of the service be undertaken, and risks to be managed and treated on an on-going basis. Please read key point 3 on page 1 before considering the following:
	
	Examples
	• Define and implement the risk management policy, approach, responsibilities, process and appetite
	• Perform a risk assessment of the service offered, covering the entire end-to-end process
	• Ensure the risks found are documented, controlled, have ownership assigned and are tracked
	• Treat the risks found, removing them or treating them so they become 'low' level risks
	• Implement physical security controls to mitigate risks, including perimeter, physical entry, secure area, monitoring, visitor access and cable protection
	• Implement third party access controls to mitigate risk, and formally agree these, plus define who has access to what information
	• Where policy allows mobile working (including working from home/ remote/ another location), or the use of mobile equipment (Laptops for example), implement controls to mitigate the risks this presents.
	  ○ Consider an increased level of monitoring on all remote connections and the corporate systems being accessed.
	  ○ Minimise the amount of information stored on mobile devices to only that which is needed to fulfil the business activity
	  ○ Install full disk encryption where possible on mobile devices, or where not, encrypt the data held on the device

Based on: Information Commissioner and UK Government IT Security guides for Small business, the CPNI Perimeters and Access Control guidance, and best practice.	○ When working remotely and connecting back to a corporate network, protect the device and the information exchange by using an appropriately configured Virtual Private Network. • Establish and agree Information security requirements with each third party involved in the service offered, to mitigate risk • Ensure supplier agreements include the need to address information security risks and protect the supply chain • Review third party agreements (and controls) on a regular basis • To mitigate risks resulting from administration, administrator access to any network component should only be carried out over dedicated network infrastructure and secure channels using communication protocols that support encryption. • Mitigate the risk of issues caused from unplanned changes, by implementing a change control process, which provides all parties involved with advanced notice of service impacting changes Source –10 Steps to Cyber Security (HM Government)

Requirement 8 – Security Awareness and Training *(Return to Requirement)*

Small Business Category	Corporate IT Category
Your employees may have a limited knowledge of cyber security but they could be your final line of defence against an attack. Accidental disclosure or human error is also a leading cause of breaches of personal data. This can be caused by simply sending an email to the incorrect recipient or opening an email attachment containing malware. It's therefore important to ensure a good level of Security Awareness. Please read key point 3 on page 1 before considering the following: *Examples* • Make employees at all levels aware of what their roles and responsibilities are. Train staff to recognise threats such as phishing emails and other malware or alerting them to the risks involved in posting information relating to your business activities on social networks. • Encourage general security awareness within the organisation. A security aware culture is likely to identify security risks. • Keep your knowledge of threats up-to-date by reading security bulletins or newsletters from organisations relevant to your business. • Provide training 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 if so, how *Based on:* Information Commissioner and UK Government IT Security guides for Small business, plus best practice	This requirement requires appropriate security awareness processes to have been implemented and be maintained on an on-going basis. Please read key point 3 on page 1 before considering the following: *Examples:* • Define, implement and communicate policies covering Information Security, including the acceptable and secure use of systems, and make complying with these a condition of employment • Establish a formal disciplinary process • Define, implement and communicate security procedures for all ICT systems • Define and implement a process on providing and maintaining security awareness • Ensure all users are aware of their information security responsibilities • Define and implement a staff induction processes • Provide staff training on Information Security and the responsibilities (including refresher training) • Monitor the effectiveness of security training • Define and implement a process that covers communicating new Cyber threats to the staff • Encourage staff to formally assess and validate their Information Assurance skills. • Promote an incident reporting culture Source –10 Steps to Cyber Security (HM Government)

Requirement 9 – Information Security Incident Response and Recovery *(Return to Requirement)*

Small Business Category	Corporate IT Category
You should consider what actions you should put into place should you suffer a data breach. Good incident management can reduce the damage and distress caused to individuals. Please read key point 3 on page 1 before considering the following: *Examples* • Create an incident management plan, stating the actions to be taken in the event of an information security incident • Review what personal data you currently have and the means of protection you have in place. • Make sure you are compliant with any industry guidance or other legal requirements. • Document the controls you have in place and identify where you need to make improvements. Monitor the controls and perform regular reviews • Identify alternate locations where the organisation could perform the service from, in event of the usual location becoming unavailable • Put arrangements / plans in place to repair, replace, or use alternate PC's and systems, in the event of a failure • Analyse any security incidents that occur, in order to identify any actions that can be taken to prevent them occurring again • Ensure Information Security is maintained in the event of needing to provide the service from an alternate location, or use alternative PC's and systems *Based upon:* Information Commissioner's Office guide on IT Security for Small business, plus best practice	This requirement requires appropriate information security incident management controls to have been implemented and maintained on an on-going basis. Please read key point 3 on page 1 before considering the following: *Examples:* • Establish an incident management capability that can address the full range of incidents that may occur, and includes senior management backing • Define, implement and communicate incident management policy, process and response plans, including roles and responsibilities • Regularly test incident management plans and supporting plans (Business Continuity Disaster Recovery) • Provide training to the incident response team and ensure all criminal incidents are reported. • End ensure Information Security is maintained when Business Continuity plans are invoked • Define and implement a data recovery capability and educate users and maintain their awareness • Collect and analyse post-incident evidence and conduct lessons learned reviews Source –10 Steps to Cyber Security (HM Government)

Requirement 10 - Data Protection Compliance *(Return to Requirement)*

Small Business Category	Corporate IT Category
This requirement asks bidders to confirm their compliance with the Data Protection Act 1998 (DPA) superseded by the General Data Protection Regulations 2016 (GDPR) from 25th May 2018 where they act as Data Controllers for their own data. The statement also confirms assurance that bidder compliance practices as a Data Controller will support the Organisation's compliance where acting as a Data Processor on our behalf. In responding to this requirement bidders should consider their overall compliance with the principles contained in Data Protection law and practices in support of safeguarding Data Subject rights. Please see key point 3 on page 1.	As per Small Business category

Requirement 11 - Winning Bidder *(Return to Requirement)*

Small Business Category	Corporate IT Category
Should the bidder be successful, and be awarded the contract, they will need to complete "Procurement Stage 2 – Evidence" at the Organisation's discretion if the processing is deemed to be high risk, and repeat the process at a frequency to be determined in order to evidence ongoing compliance. This specifies the same requirements as this questionnaire, but requires detail and evidence to be provided, to support the assurances provided, rather than a 'Yes' or 'No' response. *Examples:* • Details of actions taken to securely configure computers • Details of firewalls installed • Details of encryption being used • Details of how you control access to your computers and systems • Details of your malware protection product and its configuration • Logging and monitoring reports • Details of the risks you have identified and what you have done about them • Details of the Physical protection you have put in place • Details of how the organisation ensures Security Awareness • The plan of actions you take in the event of a security breach • The security arrangements you have in writing with any third parties you will work with to deliver the service • Screen shots (showing software and settings in place etc.) • Policies, diagrams, designs, registers and reports (or screen shots / extracts from these).	Should the bidder be successful, and be awarded the contract, they will need to complete "Procurement Stage 2 – Evidence" at the Organisation's discretion if the processing is deemed to be high risk, and repeat the process at a frequency to be determined in order to evidence ongoing compliance. This specifies the same requirements as this questionnaire, but requires detail and evidence to be provided, to support the assurances provided, rather than a 'Yes' or 'No' response. *Examples*: • Cyber Essentials Plus certificate OR evidence of Independent Cyber Essentials controls assessment and testing • Copies of Information Security policies and copies of process and procedure documents • Risk management policies and assessments • Secure baseline build/configuration details and Incident Management process and plans • Staff induction, training and Security awareness processes, and security sections in suppler agreements • Physical Security policy and monitoring and malware protection policies • Defined roles and responsibilities • Incident management and recovery processes • Screen shots (showing software and settings in place etc.) • Policies, diagrams, designs, registers and reports (or screen shots / extracts from these).