# Cyber Essentials Scheme

Applicant: Redray Ltd,

Thank you for applying for certification to the Cyber Essentials Scheme Self-Assessment.

Congratulations, you have been successful in your assessment under the Cyber Essentials scheme.

I include below the results from the form which you completed.

| Question | Answer | Score | Comments |
|---|---|---|---|
| Acceptance<br><br>Please read these terms and conditions carefully. Do you agree to these terms?<br><br>NOTE: if you do not agree to these terms, your answers will not be assessed or certified. | I accept | Compliant | |
| A1.1 Organisation Name<br><br>What is your organisation's name (for companies: as registered with Companies House)?<br><br>Please provide the full name for the company being certified. If you are certifying the local entity of a multinational company, provide the name of the local entity. | RedRay Limited | Compliant | |
| A1.2 Organisation Number<br><br>What is your organisation's registration number (if you have one)?<br><br>If you are a UK limited company, your registration number will be provided by Companies House, in the Republic of Ireland, this will be provided by Companies Registration Office. Charities, partnerships and other organisations should provide their registration number if applicable. | 290770682 | Compliant | |
| A1.3 Organisation Address<br><br>Where are you located?<br><br>Please provide the legal registered address for your organisation, or your trading address if a sole trader. | UK<br>Address Line 1: Lantern House 39-41 High Street<br>Address Line 2: Potters Bar<br>Town/City: Hertfordshire<br>EN6 5AJ | Compliant | |
| A1.4 Type of Organisation<br><br>What is your main business?<br><br>Please summarise the main occupation of your organisation. | Other service activities | Compliant | |
| A1.5 Website<br><br>What is your website address?<br><br>Please provide your website address (if you have one). This can be a Facebook/Linkedin page if you prefer. | www.redray.co.uk | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A1.6 Size of Organisation<br><br>What is the size of your organisation?<br><br>Based on the EU definitions of Micro (<10 employees, < €2m turnover), Small (<50 employees, < €10m turnover) , Medium (<250 employees, < €50m turnover) or Large (>250 Employees or >€50m turnover). | Small (<50 Employees and <€10m Turnover) | Compliant | |
| A1.7 Home Workers<br><br>How many staff are home workers?<br><br>Home workers are staff whose main work location is their home address and who work there for the majority of their time. This does not include office workers who occasionally work at home or when travelling. | 0 | Compliant | |
| A1.8 Certification Renewal Is this application a renewal of an existing certification or is it the first time you have applied for certification? | New Application | Compliant | |
| A1.9 Reason for Certification<br><br>What is your main reason for applying for certification?<br><br>Please let us know the main reason why you are applying for certification. If there are multiple reasons, please select the one that is most important to you. This helps us to understand how people are using our certifications. | To Generally Improve our Security<br>Applicant Notes: We take the security of our Cyber Networks extremely seriously and have worked hard to ensure we have the right policies and procedures in place in order to protect our staff and clients information on our network. Our reason for seeking Cyber Essentials certification is to ensure the systems we have worked hard to have in place are effective and meet industry best practice, becoming certified would allow us to communicate our commitment to the general public, clients and employees. | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A2.1 Assessment Scope<br><br>Does the scope of this assessment cover your whole organisation?<br><br>Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer 'No' to this question you will not be invited to apply for insurance.<br><br>Your whole organisation would include all divisions and all people and devices that use business data. | Yes | Compliant | |
| A2.5 Geographic Location<br><br>Please describe the geographical locations of your business which are in the scope of this assessment.<br><br>You should provide either a broad description (i.e. All UK offices) or simply list the locations in scope (i.e. Manchester and Glasgow retail stores). | Headquarters Lantern House, 39-41 High Street Potters Bar Hertfordshire EN6 5AJ | Compliant | |
| A2.6 Devices<br><br>Please provide a summary of all laptops, computers and servers that are used for accessing business data and have access to the internet (for example, "We have 25 laptops running Windows 10 Professional version 1709 and 10 MacBook Air laptops running macOS Mojave").<br><br>You do not need to provide serial numbers, mac addresses or further technical information.<br><br>**It is essential to include the Edition and Version number for Windows 10** - the assessor will be unable to mark the assessment without this. | 12 MacBooks total, broken further down as 2 MacBook pro's and 10 Macbook Airs which are all running the latest available MacOS Catalina. 1 Windows laptop using Windows 10 PRO version 2004 os build 19041.572 1 synology server | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A2.7 Mobile Devices<br><br>Please list the quantities of tablets and mobile devices within the scope of this assessment. You must include model and operating system version for all devices.<br><br>All tablets and mobile devices that are used for accessing business data and have access to the internet must be included in the scope of the assessment. You do not need to provide serial numbers, mac addresses or other technical information. | 5 Iphone 11's running iOS14 3 Ipad Pros 2018 running iPadOs 14.1 | Compliant | |
| A2.8 Networks<br><br>Please provide a list of the networks that will be in the scope for this assessment.<br><br>You should include details of each network used in your organisation including its name, location and its purpose (i.e. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software). You do not need to provide IP addresses or other technical information. | We have two networks in operation at our headquarters in Potters Bar, both networks operate behind our firewall and each offer different levels of access. The two networks are RedRay and RedRay Guest. RedRay The RedRay network is the network that users with the highest level of Manging Director authorisation a permitted access to. Currently 6 members of staff have access to the most secure of our two networks. RedRay Guest This network is for staff without the need for access to higher security resources and guests. The network offers limited access to secure resources, with only internet and printing privileges authorised. | Compliant | |
| A2.9 Network Equipment<br><br>Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers).<br><br>You should include all equipment that controls the flow of data such as routers and firewalls. You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic. | 1 x netgate firewall Ubiquity networks UBI-UAO-AC-PRO Access Point | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A2.10 Responsible Person<br><br>Please provide the name and role of the person who is responsible for managing the information systems in the scope of this assessment?<br><br>This should be the person who influences and makes decisions about the computers, laptops, servers, tablets, mobile phones and network equipment within your organisation. This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider. | Operations Director Riceal Reddin | Compliant | |
| A4.1 Firewalls<br><br>Do you have firewalls at the boundaries between your organisation's internal networks and the internet?<br><br>You must have firewalls in place between your office network and the internet. You should also have firewalls in place for home-based workers, if those users are not using a Virtual Private Network (VPN) connected to your office network. | Yes | Compliant | Good, having a firewall is the most basic line of defence for any business. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A4.2 Change Default Password<br><br>When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices? How do you achieve this?<br><br>The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Hub) You can change the default password by logging into the web interface for the device (often located at 192.168.1.1 or 192.168.1.254) | Yes. Passwords on our router and on the hardware firewall have been changed by our specialist IT consultants (Mainstream Systems Ltd). The first step when setting up new equipment is recognising that default passwords are a security risk, as such it is a key step in our installation process to ensure that the passwords are changed in accordance with our strict Password Security Policy, RRQ050. The same parameters that apply to user accounts also apply to the formation of passwords for hardware operating on our network : • Be at least eight characters in length • Consist of a mix of alpha, and at least one numeric, and special characters • Not be dictionary words • Not be portions of associated account names (e.g., user ID, log-in name) • Not be character strings (e.g., ABC or 123) • Not be simple keyboard patterns | Compliant | A written information security policy with password policy is good practice. |
| A4.3 Password Quality<br><br>Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess?<br><br>A password that is difficult to guess will be unique and not be made up of common or predictable words such as 'password' or 'admin', or include predictable number sequences such as '12345'. | Yes<br>Applicant Notes: Yes, all our passwords must conform to our strict Password Security Policy RRQ050. | Compliant | Good, passwords that are at least 8 characters long are less likely to be compromised. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A4.4 Password Management<br><br>Do you change the password when you believe it may have been compromised? How do you achieve this?<br><br>Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs. | Passwords are changed monthly as a precaution in order to help strengthen our networks security. If we believe that a password has been compromised, the incident is reported to the Operations Director who alongside the Managing Director will conduct a Security Incident Investigation. The investigation will be conducted within the parameters issued in our Security Incident Management Policy and Procedure RRQ054. The password that is believed to be effected will be immediately changed to prevent the network from being compromised. A full investigation will be conducted to identify the source of the breach. Any breach will be rectified and any actions learnt will become part of our Information Security best practice. Any lessons learnt will enable us to revise our policies and procedures which will prevent any incidents occurring in the future. | Compliant | This is good practice, and it is good that passwords are changed monthly. |
| A4.5 Services Enabled<br><br>Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case?<br><br>At times your firewall may be configured to allow a system on the inside to become accessible from the internet (such as a VPN server, a mail server or a service that is accessed by your customers). This is sometimes referred to as 'opening a port'. You need to show a business case for doing this because it can present security risks. If you have not enabled any services, answer 'No'. By default, most firewalls block all services. The business case should be documented and recorded. | No | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A4.7 Service Blocking<br><br>Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet?<br><br>By default, most firewalls block all services from inside the network from being accessed from the internet, but you need to check your firewall settings. | Yes | Compliant | This is best practice. |
| A4.8 Configuration Settings<br><br>Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet?<br><br>Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet. If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer 'no' to this question. | No | Compliant | |
| A4.11 Software Firewalls<br><br>Do you have software firewalls enabled on all of your computers and laptops?<br><br>You can check this setting on Macs in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings and searching for 'windows firewall'. On Linux try 'ufw status'. You can also use the firewall that may be provided by your anti-virus software. | Yes | Compliant | This offers another layer of protection. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A5.1 Remove Unused Software<br><br>Where you are able to do so, have you removed or disabled all the software that you do not use on your laptops, computers, servers, tablets and mobile phones? Describe how you achieve this.<br><br>To view your installed applications on Windows look in Start Menu, on macOS open Finder -> Applications and on Linux open your software package manager (apt, rpm, yum). You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use. | Yes. Any application, system utility and network service that is no longer necessary in day to day use is removed or disabled from RedRay's ICT Equipment. We regularly review the applications, system utilities and network services we use to determine their necessity , if they are deemed to be no longer relevant we remove them from our Hardware. We also remove any programs which are no longer receiving updates from their publisher. | Compliant | Good practice. |
| A5.2 Necessary User Accounts<br><br>Have you ensured that all your laptops, computers, servers, tablets and mobile devices only contain necessary user accounts that are regularly used in the course of your business?<br><br>You must remove or disable any user accounts that are not needed in day-to-day use on all devices. You can view your user accounts on Windows by righting-click on Start -> Computer Management -> Users, on macOS in System Preferences -> Users & Groups, and on Linux using 'cat /etc/passwd'. | Yes | Compliant | |
| A5.3 Change Default Password<br><br>Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more?<br><br>A password that is difficult to guess will be unique and not be made up of common or predictable words such as 'password' or 'admin', or include predictable number sequences such as '12345'. | Yes | Compliant | Good. Default passwords are a significant vulnerability. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A5.4 Password Quality<br><br>Do all your users and administrators use passwords of at least 8 characters?<br><br>The longer a password, the more difficult it is for cyber criminals to guess (or brute-force) it. | Yes<br>Applicant Notes: All default passwords are changed on all RedRay devices, in accordance with the RedRay Password Security Policy RRQ050. The same parameters that apply to user accounts also apply to the formation of passwords for hardware operating on our network : • Be at least eight characters in length • Consist of a mix of alpha, and at least one numeric, and special characters • Not be dictionary words • Not be portions of associated account names (e.g., user ID, log-in name) • Not be character strings (e.g., ABC or 123) • Not be simple keyboard patterns | Compliant | A strong password is the first line of defence. |
| A5.5 Sensitive or Critical Information<br><br>Do you run software that provides sensitive or critical information (that shouldn't be made public) to external users across the internet?<br><br>Your business might run software that allows people outside the company on the internet to access information within your business via an external service. This could be a VPN server, a mail server, or an internet application that you provide to your customers as a product. In all cases these applications provide information is confidential to your business and your customers and that you would not want to be publicly accessible. This question does not apply to cloud services such as Google Drive, Office365 or Dropbox. If you only use such services and do not run your own service you should answer no to this question. | No | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A5.10 Auto-Run Disabled<br><br>Is 'auto-run' or 'auto-play' disabled on all of your systems?<br><br>This is a setting which automatically runs software on a DVD or memory stick. You can disable 'auto-run' or 'auto-play' on Windows through Settings, on macOS through System Preferences and on Linux through the settings app for your distribution. It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option you can answer yes to this question. | Yes<br>Applicant Notes: We recognise the security risk associated with having auto-run and auto-play enabled on our systems. Recognising this risk to Cyber Security we have taken the steps to insure that these features have been disabled on all our hardware. | Compliant | This is good as reduce the risk of malware. |
| A6.1 Operating System Supported<br><br>Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems?<br><br>Please list the operating systems you use so that the assessor can understand your setup and verify that all your operating systems are still in support. Older operating systems that are out of support include Windows XP/Vista/2003, mac OS El Capitan and Ubuntu Linux 17.10 | Yes We understand the security risks of having outdated operating systems and firmware on our network. Our Software Patching Management Policy RRQ066 outlines our procedures in further detail. The vast majority of our staff use Apple Operating Systems, all of which run the latest software, Mac OS 10.15 Catalina. One member of staff uses a Windows laptop . 1 Windows laptop using Windows 10 PRO version 2004 os build 19041.572 On our phones and tablets: 5 Iphone 11's running iOS14 3 Ipad Pros 2018 running iPadOs 14. | Compliant | |
| A6.2 Applications Supported<br><br>Are all applications on your devices supported by a supplier that produces regular fixes for any security problems?<br><br>Please summarise the applications you use so the assessor can understand your setup and confirm that all applications are supported. This includes frameworks and plugins such as Java, Flash, Adobe Reader and .NET | Yes The applications we use that are supported with regular updates are; Office 365, Adobe, Photoshop, Mac OS, iPhone OS, Java and flash. | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A6.3 Software Licensed<br><br>Is all software licensed in accordance with the publisher's recommendations?<br><br>All software must be licensed. It is acceptable to use free and open source software as long as you comply with any licensing requirements. | Yes<br>Applicant Notes: All our software is purchased and licensed in accordance with the publishers recommendations. | Compliant | Good. Licensed software ensures you have access to updates. |
| A6.4 Security Updates - Operating System<br><br>Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release? Describe how do you achieve this.<br><br>You must install any such updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates. | Yes. As part of our Software Patching Management Policy it is a clear requirement that all software updates are conducted within the most efficient timescale possible on all our inventory of ICT equipment. The Operations Director will deploy Emergency patches within eight hours of availability. As Emergency patches pose an imminent threat to the network, the release may proceed testing. In all instances, the Operations Director will perform testing (either pre- or post-implementation) and document it for auditing and tracking purposes. The Operations Director will obtain authorisation for implementing Critical patches via an emergency RTC. The Operations Director will implement Not Critical patches during regularly scheduled preventative maintenance. Each patch will have an approved RTC. All high risk critical security updates for operating systems and firmware will be installed within 14 days of release. All software used by RedRay is licensed in accordance with the publishers recommendations, RedRay comply with all licensing requirements. For new network devices, each platform will follow established hardening procedures to ensure the installation of the most recent patches. | Compliant | Good practice. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A6.5 Security Updates - Applications<br><br>Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) installed within 14 days of release? Describe how you achieve this.<br><br>You must install any such updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates. | Yes. In accordance with our Software Patching Management Policy all updates are required to installed within 14 days of release. To ensure we are aware of the latest security updates, the Operations Director will monitor security mailing lists, review vendor notifications and Web sites, and research specific public Web sites for the release of new patches. Monitoring will include, but is not limited to, the following: • Scanning RedRay's network to identify known vulnerabilities • Identifying and communicating identified vulnerabilities and or security breaches to RedRay's Managing Director. • Monitoring notifications and websites of all vendors that have hardware or software operating on RedRay's network. Once alerted to a new patch, the Operations Director will download and the review the new patch. The Operations director will categorise the criticality of the patch according to the following : • Emergency- An imminent threat to RedRay's network • Critical- Targets a security vulnerability • Not Critical- A standard patch release update • Not Applicable to RedRay's network environment Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that included assessing the risk, testing, scheduling, installing and verifying. | Compliant | Very good practice. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A6.6 Unsupported Applications<br><br>Have you removed any applications on your devices that are no longer supported and no longer received regular fixes for security problems?<br><br>You must remove older applications from your devices when they are no longer supported by the manufacturer. Such applications might include older versions of web browsers, frameworks such as Java and Flash, and all application software. | Yes<br>Applicant Notes: Any applications on RedRay's Network that no longer support software updates and security patches are removed from users devices and the network. All applications no longer supported by the manufacturer are removed these include: older versions of Operating Systems (e.g. mac OS El Capitan) web browsers, frameworks such as Java and Flash and all application software. | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A7.1 Account Creation<br><br>Are users only provided with user accounts after a process has been followed to approve their creation? Describe the process.<br><br>You must ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business. | Yes. Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of RedRay's which must be managed with care. All information has a value, however, not all of this information has an equal value or requires the same level of protection. Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change (For further information refer to RRQ050 Password Security Policy). The first step in User account creation is the authorisation of the Managing Director who will authorise the creation of a user account and determine the level of access they require in order to perform their job role. User account management procedures must be implemented for user registration, modification and de-registration on all RedRay information systems. These procedures include processes for monitoring redundant and inactive accounts. All additions, deletions, suspensions and modifications to user accesses are captured in an audit log showing who took the action and when. These procedures shall be implemented by the Operations Director with authorisation from the Managing Director. Access control standards have been established for | Compliant | Very good practice. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| | all information systems, at an appropriate level for each system, which minimises information security risks yet allows the organisation's business activities to be carried out without undue hindrance. All access to RedRay information systems are controlled by RRQ050 Password Security Policy, an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user's identity. Users are limited to only one user account for each individual information system for non-administrative purposes. Any variations from this policy must be authorised by the Managing Director. All users have a user ID for their sole use for access to all computing services. All individual user IDs are unique for each user and never duplicated. All administrator and privileged user accounts are based upon job function and authorised by the Managing Director prior to access being given. Procedures are established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organisation. Users' access rights will be reviewed at regular intervals no longer than annually. Access to systems by individual users must be authorised by the Operations Director. | | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A7.2 Unique Login<br><br>Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password?<br><br>You must ensure that no devices can be accessed without entering a username and password. Users cannot share accounts. | Yes<br>Applicant Notes: All RedRay devices can only be accessed as a minimum by entering a password and username which comply with our Password Security Policy, where possible on newer technology we utilise fingerprint and face recognition security measures. | Compliant | Good, all devices need to be secured by a username and password. It is especially good that you utilise fingerprint and face recognition security measures. |
| A7.3 Leavers Account Management<br><br>How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?<br><br>When an individual leaves your organisation you need to stop them accessing any of your systems. | By keeping an up to date User Access Audit log we are able to see who is authorised to use our networks, as part of an employees leaving process their accounts are disabled on their last day of employment. | Compliant | Good to have a clear procedure as this avoids inconsistencies and mistakes. |
| A7.4 Staff Privileges<br><br>Do you ensure that staff only have the privileges that they need to do their current job? How do you do this?<br><br>When a staff member changes job role you may also need to change their access privileges to systems and data. | RedRay staff only have privileges that they need to do their current job. Our User Access Audit Log keeps detailed information of the level of information our employees can view. If an employee requires greater access to our information to complete a task which differs from their day to day responsibilities, increased access privileges are granted and documented, increased information privileges are revoked upon completion of the task. When an employee has a change in job role they may need greater or lesser access to privileged information. Levels of access are determined by the Managing Director who has ultimate responsibility for Cyber Security. | Compliant | This is good - many companies do not have a transfer process. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A7.5 Administrator Process<br><br>Do you have a formal process for giving someone access to systems at an “administrator” level? Describe the process.<br><br>You must have a formal, written-down process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation. | Yes, due to increased access to privileged information and the security risks associated with administrator level we limit the amount of accounts operating at Administrator level. Only the Managing Director and as authorised by the Managing Director the Operations Director have admin access to our systems. Should internal staff require access they would need to follow our admin access process and complete a request form. If access is deemed necessary to their work task the Managing Director would grant access for a limited time. | Compliant | |
| A7.6 Use of Accounts<br><br>How do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?<br><br>You must ensure that administrator accounts are only used when absolutely necessary, such as when installing software. Using administrator accounts all-day-long exposes the device to compromise by malware. | We ensure administrator accounts are only given to those who need them to do their job, at present this is the Managing Director and the Operations Director. Administration accounts are only used to carry out administrative activates which includes installing new software and changing configuration settings. We also outline in our Information Security Policy RRQ002 that no users who log in as administrator should perform any tasks other than administrative duties. | Compliant | This is good practice. A suggestion would be to periodically monitor logs to ensure admins are abiding by these requirements. |
| A7.7 Managing Usage<br><br>How do you ensure that administrator accounts are not used for accessing email or web browsing?<br><br>You must ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff. | Administration accounts are only to be used for administrative activities, tasks such as email access and web browsing should only be performed in standard user accounts. Our Information Security Policy RRQ002 prohibits the use of administration accounts for anything other than administration activities. | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A7.8 Account Tracking<br><br>Do you formally track which users have administrator accounts in your organisation?<br><br>You must track by means of list or formal record all people that have been granted administrator accounts. | Yes<br>Applicant Notes: Yes, administration accounts like user accounts are formally tracked and recorded in our User Access Audit log. | Compliant | This should be reviewed regularly. |
| A7.9 Access Review<br><br>Do you review who should have administrative access on a regular basis?<br><br>You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed. | Yes<br>Applicant Notes: Our User Access Audit log is reviewed whenever there is a change of employees access privileges and no less frequently than every 12 Months, by senior management. | Compliant | Good practice - suggestion for admins this could be more frequently. |
| A7.10 Two-factor Authentication<br><br>Have you enabled two-factor authentication for access to all administrative accounts?<br><br>If your systems supports two factor authentication (where you receive a text message, a one-time code, use a finger-print reader or facial recognition in addition to a password), then you must enable this for administrator accounts. | No | Compliant | |
| A7.11 Two-factor Unavailable<br><br>Is this because two-factor authentication is not available for some or all of your devices or systems? List the devices or systems that do not allow two-factor authentication.<br><br>You are not required to purchase any additional hardware or install additional software in order to meet this requirement. Most standard laptops do not have two-factor authentication available. If your systems do not have two-factor authentication available answer yes to this question. | Administration task are conducted on Apple Mac computers which don't have native 2FA functionality | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A8.1 Malware Protection<br><br>Are all of your computers, laptops, tablets and mobile phones protected from malware by either:<br><br>A - having anti-malware software installed,<br><br>B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or<br><br>C - application sandboxing (i.e. by using a virtual machine)?<br><br>Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B. | A - Anti-Malware Software,B - Only allowing software from an App Store or Application Whitelisting<br>Applicant Notes: A) We have anti-malware software that protects our computers and laptops. B) Our iPhones aren't jailbroken and only official App Store Apps are permitted to be installed | Compliant | |
| A8.2 Update Daily<br><br>(A) Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access?<br><br>This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-virus software. You can use any commonly used anti-virus product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose. | Yes | Compliant | Malwarebytes is a good tool to use. |
| A8.3 Scan Web Pages<br><br>(A) Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?<br><br>Your anti-virus software should have a plugin for your internet browser or for the operating system itself that prevents access to known malicious websites. On Windows 10, SmartScreen can provide this functionality. | Yes | Compliant | Malwarebytes is a good tool to use. |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A8.4 Application Signing<br><br>(B) Where you use an app-store or application signing, are users restricted from installing unsigned applications?<br><br>By default, most mobile phones and tablets restrict you from installing unsigned applications. Usually you have to 'root' or 'jailbreak' a device to allow unsigned applications. | Yes<br>Applicant Notes: Yes. We do not permit jailbreaking or rooting so users are unable to install unsigned apps | Compliant | This is the main protection for iOS devices. |
| A8.5 List of Approved Applications<br><br>(B) Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you document this list of approved applications?<br><br>You must create a list of approved applications and ensure users only install these applications on their devices. This includes employee-owned devices. You may use Mobile Device Management (MDM) software to meet this requirement but you are not required to use MDM software if you can meet the requirements using good policy, process and training of staff. | Yes<br>Applicant Notes: Yes. We have an approved software list which users reference before downloading software | Compliant | |
| A3.1 Head Office<br><br>Is your head office domiciled in the UK and is your gross annual turnover less than £20m?<br><br>This question relates to the eligibility of your company for the included cyber insurance. | Yes | Compliant | |
| A3.2 Cyber Insurance<br><br>If you have answered 'yes' to the last question then your company is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element please opt out here.<br><br>The cost of this is included in the assessment package and you can see more about it<br>at<br>https://www.iasme.co.uk/cyberessentials/automatic-insurance-cover/. | Opt-In | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A3.3 Total Gross Revenue<br><br>What is your total gross revenue? Please provide figure to the nearest £100K. You only need to answer this question if you are taking the insurance.<br><br>The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification. Please be as accurate as possible - figure should be to the nearest £100K | £2.7 million | Compliant | |
| A3.4 FCA<br><br>Is the company or its subsidiaries any of the following: medical, call centre, telemarketing, data processing (outsourcers), internet service provider, telecommunications or an organisation regulated by the FCA? You only need to answer this question if you are taking the insurance.<br><br>The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification. | No | Compliant | |
| A3.5 Domiciled Operation<br><br>Does the company have any domiciled operation or derived revenue from the territory or jurisdiction of Canada and / or USA?<br><br>You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification. | No | Compliant | |

| Question | Answer | Score | Comments |
|---|---|---|---|
| A3.6 Email Contact<br><br>What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance.<br><br>The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information. | accounts@redray.co.uk | Compliant | |
| All Answers Approved Have all the answers provided in this assessment been approved at Board level or equivalent? | Yes | Compliant | |
| Cyber Insurance Declaration Signed<br><br>Has the attached Cyber Insurance Declaration been downloaded (by clicking here), completed and signed (by a Board level or equivalent signatory), then uploaded (using the function provided below)?<br><br>Please note: The file upload must be in .PDF, .JPG or .PNG format and a maximum file size of 5MB. If your file is larger than 5 MB, please contact info@iasme.co.uk | Yes | Compliant | |

CYBER ESSENTIALS

# CERTIFICATE OF ASSURANCE

## RedRay Limited

Lantern House 39-41 High Street , Potters Bar, Hertfordshire EN6 5AJ

**COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME**

**NAME OF ASSESSOR :** Michael Adeoro

**CERTIFICATE NUMBER :** IASME-CE-007211

**PROFILE VERSION :** April 2020

**SCOPE :** Whole Company

**DATE OF CERTIFICATION :**

**RECERTIFICATION DUE :** 2021-10-26

CERTIFICATION MARK

CERTIFICATION BODY

CYBER ESSENTIALS PARTNER

This Certificate certifies that the organisation named was assessed as meeting the Cyber Essentials implementation profile released February 2017 and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against cyber attack.