ISO 27001 Security Standards

All data is hosted and supported by Microsoft, and not Paritor.

No	Standard / Guidance Document(s)	Document Reference	Area	Rating	Security Standard	Response regarding:	
						Hosting Provision and Support	Software Application Development, Provision and Support
1	ISO27001 / NCSC Cloud Security Principle 4: Governance framework	5.1.1 - 5.1.2	Information Security Policy / Information security policy document & review of information security policy	**MUST**	**INFORMATION SECURITY POLICY** An information security policy must have been implemented within the Provider organisation and be the subject of a review at least annually. A) Confirm this is the case B) Provide a copy of this policy and state the date it was last reviewed.	*Paritor confirm a securtity policy is in place. All information including a report can be found at the following URL https://paritor.com/data-hosting-and-compliance, last reviewed April 2021.*	*Paritor confirm a securtity policy is in place. All information including a report can be found at the following URL https://paritor.com/data-hosting-and-compliance, last reviewed April 2021.*
2	ISO27001 / NCSC Cloud Security Principle 4: Governance framework	6.1.1 - 6.1.3	Organisation of Information Security / Internal organisation / management commitment, co-ordination and allocation of responsibilities	**MUST**	**INFORMATION SECURITY GOVERNANCE** An effective information security governance structure must be implemented within the Provider organisation. A) Detail how information security is governed within the Provider organisation B) Describe key areas of responsibility.	*Paritor's information security governance structure is available in our company policy at the following URL: https://paritor.com/data-hosting-and-compliance, last reviewed December 2021.*	*Paritor's information security governance structure is available in our company policy at the following URL: https://paritor.com/data-hosting-and-compliance, last reviewed December 2021.*
3	ISO27001 / NCSC Cloud Security Principle 4: Governance framework	6.1.4	Organisation of Information Security / Internal organisation / authorisation process	**MUST**	**NEW ICT SYSTEM AUTHORISATION** All new ICT systems within the Provider organisation must be properly authorised by management. A) Detail how this process is implemented	*Paritor is a small organisation and all decisions around ICT systems are made by and authorised by its MD*	*Paritor is a small organisation and all decisions around ICT systems are made by and authorised by its MD*
4	ISO27001 / NCSC Cloud Security Principle 4: Governance framework	6.1.5	Organisation of Information Security / Internal organisation / confidentiality agreements	**MUST**	**NON-DISCLOSURE AGREEMENTS** To protect GCC information assets all staff associated with the supply of services to GCC must have signed Non-Disclosure / Confidentiality agreements (NDA's) or equivalent as part of the employment process. A) Confirm this is the case B) Confirm that GCC would be provided copies of these if requested	*All employees sign a detailed employee contract which covers the management and conrtol of client data. A copy of our standard employee contract is avaliable if required.*	*All employees sign a detailed employee contract which covers the management and conrtol of client data. A copy of our standard employee contract is avaliable if required.*
5	ISO27001 / NCSC Cloud Security Principle 4: Governance framework	6.1.6 - 6.1.7	Organisation of Information Security / Internal organisation / contact with authorities & special interest groups	**MUST**	**SECURITY INCIDENTS** All incidents of unauthorised access and misuse of data must be reported. All those with access to GCC data need to be made aware of when and how to report incidents. Provide details of the major incident process in place to deal with serious security breaches including: A) How GCC are alerted and who is responsible for this. B) If and when incidents are reported to appropriate authorities and special interest groups C) If and when consultancy support would be used to investigate and resolve the incident. B) How this process is enforced.	*We have an internal instant reporting system, managed by our infrastructure manager, and breaches are imediatlky brought to the attention of the client by email. An investigation takes place and a report is written which is supplied to the client.*	*N/A.*

6	ISO27001 / NCSC Cloud Security Principle 4: Governance framework	7.1.1 - 7.1.2	Asset Management / Responsibility for Assets / inventory & ownership	**MUST**	**ASSET MANAGEMENT** Assets must be appropriately managed by the Provider A) Briefly detail how assets are managed within the Provider organisation, including details of asset registers and how their value/risk to the business is assessed.	*All equipment is recorded within our asset register. Assets are limited to personal computure equipment such as laptops, their value is assessed using standard accounting practice.*	*All equipment is recorded within our asset register. Assets are limited to personal computure equipment such as laptops, their value is assessed using standard accounting practice.*
7	ISO27001 / NCSC Cloud Security Principle 14: Secure use of the service	7.1.3	Asset Management / Responsibility for Assets / acceptable use of assets	**MUST**	**ACCEPTABLE USE POLICY** Provider staff use of systems and networks used to deliver services to GCC must be governed by an Acceptable Use Policy. A) Confirm that the Provider operates an Acceptable Use Policy with regard to Employee use of its assets. B) If so, then provide a brief outline of the areas that it covers and provide a copy of the policy.	*Yes we do have a use policy and this is defined within the employee contract and employee hand book. It gives guidelines around the use of laptops etc. Copy of handbook and contract is avaliable on request.*	*Yes we do have a use policy and this is defined within the employee contract and employee hand book. It gives guidelines around the use of laptops etc. Copy of handbook and contract is avaliable on request.*
8	ISO27001 / NCSC Cloud Security Principle 6: Personnel security	8.3.1 - 8.3.3	Human Resource Security / Removal of Access Rights / termination responsibilities and return of assets / removal of access rights	**MUST**	**STAFF LEAVING PROCESS** Should a member of staff leave the Provider organisation, they must no longer be able to access systems and applications which handle GCC data A) Outline how the Provider manages the leaving process, the removal of access rights and any other measures that are in place to ensure that it is no longer possible to access GCC data. Ensure that the response includes any remote access solutions that are in place.	*All access to our system is managed by microsoft active directory and microsoft 365. When an emplyee leaves the company access to these accounts is removed. Any equipment held by the employee is returned.*	*All access to our coding repository is managed by Microsoft DevOps. When an emplyee leaves the company access to this repository is removed. Any equipment held by the employee is returned.*
9	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.1.1 - 9.1.3, 9.1.5, 9.1.6	Physical & Environmental Security / Secure Areas / physical security perimeter, entry controls, working in secure areas & public access areas	**MUST**	**PHYSICAL SECURITY** It is essential that information assets hosted by the Provider which contain GCC data are adequately protected from physical threats. All locations involved with the support of the data handling solution must also be physically secure A) Detail the physical security measures (including access control and housing of equipment) that are in place within core areas hosting GCC data. B) Detail the measures that will be in place to limit access to sensitive support system functionality only to staff with the relevant requirement and clearance. B) Confirm that visitors and external support staff are escorted at all times in sensitive areas (e.g. data centres and specific support areas).	*All equipment holding data is managed by and with microsoft azure data centres (UKSouth location) subject to their security.*	*Physical access to Paritor owned machines are secured by Windows sign-in and password. These machines can be remotely disabled using Azure Active Directory in the event of a lost device. Access to the code repository also requires a Microsoft account sign in.*
10	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.1.4	Physical & Environmental Security / Secure Areas / Protecting against external and environmental threats	**MUST**	**ENVIRONMENTAL THREATS** The location for hosting GCC data must have been assessed with regard to the risk against external and environmental threats, e.g. flooding, aircraft damage etc... and any identified risks must have been adequately mitigated. A) Confirm that a risk assessment has been conducted B) Describe how threats from external and environmental conditions have been adequately mitigated.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*Not applicable*

11	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.2.1	Physical & Environmental Security / Secure Areas / Equipment siting and protection	**MUST**	**OFFICE PRIVACY** Office areas used to support and deliver any aspect of the data handling solution should be sited in areas which cannot be overlooked by individuals inside or outside of the building. A) Confirm that it is not possible for external parties to observe screens or keyboards associated with the support or delivery of the service.	*Paritor confirm that this is not possible.*	*Paritor confirm that this is not possible.*
12	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.2.2	Physical & Environmental Security / Secure Areas / Supporting utilities	**MUST**	**UTILITY PROTECTION** Services relating to the delivery of systems and applications used to hold GCC data must be appropriately protected from issues associated with utilities, e.g. loss or degradation of power supplies or network outage. A) Detail the controls that are or will be implemented to support the business continuity objectives, for example physical data centre separation, ensuring continuity of power, network resilience etc...	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*N/A.*
13	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.2.3	Physical & Environmental Security / Secure Areas / Cabling security	**MUST**	**CABLE PROTECTION** Network and power cables associated with service provision must not be exposed and must be adequately protected from compromise. A) Describe how all cabling (power / network) relating to the delivery of systems and applications used to hold GCC data (including support environments) shall be adequately protected against accidental or deliberate threats.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*N/A.*
14	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.2.4	Physical & Environmental Security / Secure Areas / Equipment maintenance	**MUST**	**MAINTENANCE** All equipment and associated software must be appropriately maintained and kept up to date. Those responsible for carrying out this maintenance must be escorted at all times in sensitive areas (e.g. data centres and key support locations). A) Outline how hardware and software is maintained within the Provider organisation, including the frequency of updates. B) Confirm that all those responsible for carrying out the maintenance of equipment and associated software will have appropriate level of clearance (e.g. BPSS) or will be escorted by a member of staff with such clearance at all times.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*Any OS security updates are automatically managed and applied by Microsoft. In terms of local devices, we use Azure AD to ensure that auto-update is enabled on any company machines.*

15	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.2.5	Physical & Environmental Security / Secure Areas / security of equipment off premises	**MUST**	**OFF PREMISE SECURITY** Appropriate policies and procedures must be in place to protect the security of equipment (e.g. staff laptops) off premises if used to support or provide administrator access to solutions handling GCC data. A) Outline whether there will be a requirement for administrative staff to support or access data handling solutions from remote locations (e.g. home). B) Detail the periods when remote provision of support or system administration may be necessary. C) Describe the procedural (e.g. mobile working policy), personnel and technical controls that will be implemented to provide suitable levels of assurance of the security of equipment used to support or administer data handling solutions off premises.	*Theres not a requirement.*	*N/A.*
16	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.2.6	Physical & Environmental Security / Equipment Security / Secure disposal or re-use of equipment	**MUST**	**EQUIPMENT DISPOSAL** All GCC information stored as part of the service must be properly sanitised and disposed of in a secure manner at end of life, or in the event that GCC no longer consumes the service. Disposal must be to BS EN 15713:2009 standard or equivalent. A) Detail how equipment (including servers, workstations, mobile devices, hard drives, memory) and media (including CD-ROMs, USB devices etc.) are disposed of when they reach end of life and confirm that this is to BS EN 15713:2009 or equivalent. B) State the impact level to which the data will be securely erased both as part of the offloading process (to prevent reading by commercial data recovery tools) and as part of the disk replacement and maintenance processes, such that assurance can be gained that residual data no longer exists within the Provider organisation. Ensure the response includes production, test and development facilities as well as backup media. C) If the disposal service is outsourced to a third-party, confirm their company details and compliance with BS EN 15713:2009.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*No sensitive information is stored on Paritor owned local devices. In the event of a device being decomissioned - a comprehensive harddisk wipe will be accompanied and afterward the harddisk will be destroyed to BS EN 15713:2009 standard.*
17	ISO27001 / NCSC Cloud Security Principle 2: Asset protection and resilience	9.2.7	Physical & Environmental Security / Secure Areas / Removal of Property	**MUST**	**THEFT PROTECTION** Controls must be in place to ensure that equipment, storage devices and electronic media associated with the delivery and support of the data handling solution cannot be easily removed without authorisation. A) Detail the controls that are in place to provide protection from theft.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*Physical access to Paritor owned machines are secured by Windows sign-in and password. These machines can be remotely disabled using Azure Active Directory in the event of a lost device. Access to the code repository also requires a Microsoft account sign in.*

18	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.1.1	Communications and Operations Management / Operational procedures & responsibilities / Documented Operating Procedures	**MUST**	**SECURITY OPERATING PROCEDURES** Security Operating Procedures (SyOps) must be produced and followed with regard to the management of the service. Common areas covered within SyOps include procedures associated with password management, anti-malware and patching updates, secure use of administrative facilities (e.g. locking consoles / logging off when not in use) etc... A) Describe the specific applicable SyOps that will be produced for the service B) Confirm that these SyOps will be followed by administrative and support staff.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*SysOps is in place for all local staff and machines, with our guidelines available upon request.*
19	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.1.2	Communications and Operations Management / Operational procedures & responsibilities / Change Management	**MUST**	**CHANGE CONTROL PROCEDURES** All changes made to the infrastructure or application of the data handling solution must be made under formal change control procedures. A) Outline the change control and roll back procedures that will be documented and followed (for both planned changes and in emergency conditions). B) Explain how GCC will be kept informed of any planned or emergency changes that could impact the service we receive. C) Detail the notice period that will be provided for changes that could impact the service we receive and the retention period of change records.	*For both the desktop and web applications we have testing/staging sites which are thoroughly subject to QA before the switch is made to live. Using staging slots, if a bug becomes apparent after making it to live, we can quickly revert the change back to a previous version with no downtime. Publishing to live is not possible with our deployment process. (Publish to staging, then swap staging with live). GCC will be informed if such a sitatuion arises, and if there is planned downtime - an email will be sent out at least 7 days before.*	*For both the desktop and web applications we have testing/staging sites which are thoroughly subject to QA before the switch is made to live. Using staging slots, if a bug becomes apparent after making it to live, we can quickly revert the change back to a previous version with no downtime. Publishing to live is not possible with our deployment process. (Publish to staging, then swap staging with live). GCC will be informed if such a sitatuion arises, and if there is planned downtime - an email will be sent out at least 7 days before.*
20	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.1.3	Communications and Operations Management / Operational procedures & responsibilities / Segregation of Duties	**SHOULD**	**SEGREGATION OF DUTIES** Sensitive functions within the development, support and management of the data handling solution should be subject to the concept of 'segregation of duties'. For example, code development, code testing and the releasing of new code should not be carried out by the same person to avoid introduction of malware. A) Detail any segregation of duties that will be implemented in the development, support and management of the data handling solution, including new application code release, administrative account functions, database operations and/or protective monitoring log management.	*Access is controlled via Azure - with only select users able to write to the hosting platform.*	*We use Azure DevOps access control to apply different roles associated to employees. This comes in 2 forms, permission management and access level management. More below.* *Permission management controls access to specific functional tasks at different levels of the system. Object-level permissions set permissions on a file, folder, build pipeline, or a shared query. Permission settings correspond to Allow, Deny, Inherited allow, Inherited deny, and Not set. To learn more about inheritance, see Permission inheritance and security groups later in this article.* *Access level management controls access to features provided via the web portal, the web application for Azure DevOps. Based on what has been purchased for a user, administrators set the user's access level to Basic, Basic + Test, VS Enterprise (previously Advanced), or Stakeholder*

21	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.1.4	Communications and Operations Management / Operational procedures & responsibilities / Separation of development, test and operational facilities	**MUST**	**SEPARATION OF FACILITIES** There must be a clear separation of facilities associated with the development and testing process and the live facilities for the data handling solution. A) Provide information on how new application code and infrastructure changes will be developed and tested. B) Describe the measures that are in place to protect support and development staff from accidentally or maliciously rolling out code to the wrong platform (i.e. live instead of test)	*For both the desktop and web applications we have testing/staging sites which are thoroughly subject to QA before the switch is made to live. Using staging slots, if a bug becomes apparent after making it to live, we can quickly revert the change back to a previous version with no downtime. Publishing to live is not possible with our deployment process. (Publish to staging, then swap staging with live).*	*For both the desktop and web applications we have testing/staging sites which are thoroughly subject to QA before the switch is made to live. Using staging slots, if a bug becomes apparent after making it to live, we can quickly revert the change back to a previous version with no downtime. Publishing to live is not possible with our deployment process. (Publish to staging, then swap staging with live).*
22	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.4.1	Communications and Operations Management / Protection Against Malicious and Mobile Code / Controls against Malicious Code	**MUST**	**MALICIOUS CODE PROTECTION** Data handling solutions associated with the delivery of GCC services must be protected from malicious code, where any such solution is commonly exposed to such risks. Any information exchanged as part of GCC service (e.g. attachments or data within application records) must also be protected. A) Describe all host and network-based Anti-Virus and Anti-Malware controls that will be implemented as part of the data handling solution and how frequently signatures are updated. B) Outline any additional protection that is implemented within the data handling solution, for example Intrusion Protection Products / Endpoint Protection / Server Lockdown / Desktops / Laptops / Browser Settings etc.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*
23	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.4.2	Communications and Operations Management / Protection Against Malicious and Mobile Code / Controls against Mobile Code	**SHOULD**	**MOBILE CODE PROTECTION** Provider servers should be protected against the risk of mobile code execution (malicious JavaScript, ActiveX, Java etc.). A) Describe any measures that will be implemented to protect Provider servers from the threat of malicious mobile code.	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*	*All equipment holding data is managed by and with microsoft azure data centres subject to their security.*
24	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.5.1	Communications and Operations Management / Backup / Information Backup	**MUST**	**BACK UPS** All GCC data held within the solution must be regularly backed up such that it can be restored in the event of corruption or data loss. Backups must be available and working at all times. It must be possible to restore backup data within acceptable timeframes. A) Describe how data will be backed up as part of the data handling solution, including information within open object stores such as databases. B) Define the backup nature (full, differential etc.). C) Outline any additional measures (e.g. journaling) that will be implemented. D) Detail where any backup media will be stored and how it shall be transported to any offsite locations. E) Provide details of how often the backup and restore process shall be tested to ensure ongoing functionality and integrity.	*Not applicable*	*Paritor take daily, weekly, and monthly backups of all databases – which are encrypted at rest. Git methodology is used to maintain source control/backups of source code.*

25	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.7.3	Communications and Operations Management / Media Handling / Information Handling Procedures	**MUST**	**INFORMATION HANDLING PROCEDURES** Information handling procedures must exist within the Provider organisation. The Provider must also be aware of the requirements listed within the HMG Security Policy Framework (SPF, for further details see: https://www.gov.uk/government/publications/security-policy-framework) with regard to the delivery of this contract. A) Describe any appropriate information handling procedures that exist within the Provider organisation.	*Only support team members can access customer data and only after they have received adequate training. Sales and development team members can only access test data. Employees are subject to DBS checks as on-site training is often at locations where children may be present,* *e.g. schools.*	*Only support team members can access customer data and only after they have received adequate training. Sales and development team members can only access test data. Employees are subject to DBS checks as on-site training is often at locations where children may be present, e.g. schools.*
26	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.7.4	Communications and Operations Management / Media Handling / Security of System Documentation	**MUST**	**SECURITY INFORMATION PROTECTION** Information pertaining to the security of the data handling solution (including design documentation, support information such as security operating procedures and administrative credentials) must be adequately protected at all times. A) Describe where such information shall be stored B) Describe the measures (e.g. network segregation, role-based access control) that will be implemented to protect such information to only those members of staff with a need to access.	*Security information is contained in a secure blob storage container with no public access. IP-based access/RBAC is implemented to protect such information.*	*Security information is contained in a secure blob storage container with no public access. IP-based access/RBAC is implemented to protect such information.*
27	ISO27001 / NCSC Cloud Security Principle 13: Audit information for users	10.10.1	Communications and Operations Management / Monitoring / Audit Logging	**MUST**	**PROTECTIVE MONITORING & AUDIT LOGGING** It must be possible to extract appropriate levels of logging detail in the event of a security incident affecting the service. Data handling solutions should be capable of generating audit logs for all users, including system administrators. A) Describe all areas of the solution (e.g. servers, firewalls, IDS/IPS, application logging etc…) that will provide protective monitoring and audit logging capabilities B) Confirm the level of detail that will be provided and log retention periods. C) Describe any capability in the solution for monitoring acceptable use (e.g. by administrators) - including administrator logins / login failures, change of privilege levels etc.	*Comprehensive logging and system alerts are enabled on all production hosting systems and are frequently monitored and reviewed. Login failures are monitored from within Azure Active Directory B2C - information such as IP address, location, authentication level are all recorded.*	*Comprehensive logging and system alerts are enabled on all production hosting systems and are frequently monitored and reviewed. Login failures are monitored from within Azure Active Directory B2C - information such as IP address, location, authentication level are all recorded.*

28	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.10.2	Communications and Operations Management / Monitoring / Monitoring System Use	**SHOULD**	**PROTECTIVE MONITORING PROCESSES & PROCEDURES** There should be clearly defined policies and procedures (e.g. in Security Operating Procedures) for ongoing protective monitoring with regard to the data handling solution, including the requirement for regular log reviews and escalation paths etc. A) Describe the Providers processes and procedures that are in place with regard to protective monitoring.	*Those members of the company's staff needing such access to perform their job in providing support and assistance to the client. Access to customer data is limited to consultants and support staff. These individuals all have up to date CRD/DBS checks in place. Furthermore, frequent information audits are in place, showing the time, IP address and name of the user accessing sensitive information, and these audits are frequently reviewed for sucpicious activity. Any data breaches by Paritor employees are classified as either malicious or nonmalicious. Malicious data breaches would result in immediate dismissal of the employee. Legal action may follow. (There has never been a malicious breach of data). Non-malicious breaches would result in written warnings being given to the employee. The situation would be investigated and any training/changes in procedure implemented. (There has never been a breach of any data held within our hosted data service). Paritor is protected via windows defender, and one drive E3 office 365 SCP security."*	*Those members of the company's staff needing such access to perform their job in providing support and assistance to the client. Access to customer data is limited to consultants and support staff. These individuals all have up to date CRD/DBS checks in place. Furthermore, frequent information audits are in place, showing the time, IP address and name of the user accessing sensitive information, and these audits are frequently reviewed for sucpicious activity. Any data breaches by Paritor employees are classified as either malicious or nonmalicious. Malicious data breaches would result in immediate dismissal of the employee. Legal action may follow. (There has never been a malicious breach of data). Non-malicious breaches would result in written warnings being given to the employee. The situation would be investigated and any training/changes in procedure implemented. (There has never been a breach of any data held within our hosted data service). Paritor is protected via windows defender, and one drive E3 office 365 SCP security."*
29	ISO27001 / NCSC Cloud Security Principle 13: Audit information for users	10.10.3	Communications and Operations Management / Monitoring / Protection of Log Information	**SHOULD**	**AUDIT LOG PROTECTION** In the event of any incident affecting the service it should be possible to rely on the integrity of audit logs. A) Describe any measures that will be implemented to protect audit logs from tampering. Examples might include regular shipping of logs to read only media or remote servers, real time event logging and the use of Security Incident Event Management (SIEM) solutions.	*Audit logs are available and stored on Azure with RBAC in place.*	*Audit logs are available and stored on Azure with RBAC in place.*
30	ISO27001 / NCSC Cloud Security Principle 13: Audit information for users	10.10.5	Communications and Operations Management / Monitoring / Fault Logging	**SHOULD**	**FAULT LOGGING** Data handling solutions should also have inherent capability for fault and performance logging and reporting to identify potential concerns with its availability. A) Describe any fault reporting capabilities within the data handling solution and how fault log events are generated and alerted B) Confirm that GCC will be made aware of any serious fault alerts affecting the data handling solution.	*Comprehensive logging and system alerts are enabled on all production hosting systems and are frequently monitored and reviewed.*	*Comprehensive logging and system alerts are enabled on all production hosting systems and are frequently monitored and reviewed.*

31	ISO27001 / NCSC Cloud Security Principle 5: Operational security	10.10.6	Communications and Operations Management / Monitoring / Clock Synchronisation	**SHOULD**	**CLOCK SYNCHRONISATION** To support cohesion of monitoring events across multiple parts of the data handling solution the Provider should ensure clock synchronisation is in place. A) Confirm whether clock synchronisation will be implemented as part of the Provider solution and describe its coverage (e.g. systems, firewalls, routers, switches etc.), the synchronisation source and method (e.g. NTP). B) Describe any processes and procedures (e.g. within Security Operating Procedures) to ensure that clock synchronisation continues to operate properly.	*Clock synchronisation is managed by Microsoft Azure.*	*Clock synchronisation is managed by Microsoft Azure.*
32	ISO27001 / NCSC Cloud Security Principle 9: Secure user management	11.1.1	Access Control / Access Control Policy (Management and Support)	**MUST**	**ACCESS CONTROL POLICY** Access to information, in addition to sensitive functions (e.g. admin / publishing functionality), for data handling solutions must be confined to those with a specific requirement and be governed by an access control policy covering both physical and logical access to solutions and GCC data. For both logical (e.g. the implementation of Role Based Access Control mechanisms, Active Directory Groups, use of Kerberos etc.) and physical (e.g. Card swipe required for access to data centre / support environment) domains: A) Describe the process by which access is granted to administrative support functions associated with the data handling solution. B) Describe the access control policy that applies C) Confirm that individual user IDs will be assigned for support functions and generic administrator accounts will not be used.	*Physical access is controlled by Microsoft as we are using a cloud-based hosting solution. RBAC is utilised to ensure that users within Azure AD only have access to the specific roles required for their job functionality.*	*Physical access is controlled by Microsoft as we are using a cloud-based hosting solution. RBAC is utilised to ensure that users within Azure AD only have access to the specific roles required for their job functionality.*
33	ISO27001 / NCSC Cloud Security Principle 10: Identity and authentication	11.2.2	Access Control / Privilege Management	**MUST**	**PRIVILEGE REVIEW** Data handling solution privileges must be regularly reviewed to ensure that they are still appropriate and following the concepts of 'least privilege'. A) Describe the process for privilege review / audit and its frequency. B) Confirm the coverage of the process (e.g. Operating System, web application admin functions etc.). C) Outline how privileges can be managed by the Provider or by GCC as part of this contract, e.g. the provision of a web-based Role-based Access Control interface for user account administration.	*Employees only have access to the data required for them to perform their daily job requirements (.e.g support members have access to the support system functionality). This is on a least privelege basis. We have replicated this functionality in Xperios, and users with administrators rights can set the access control level to other users. Paritor aim to conduct an internal privelege audit/review yearly.*	*Employees only have access to the data required for them to perform their daily job requirements (.e.g support members have access to the support system functionality). This is on a least privelege basis. We have replicated this functionality in Xperios, and users with administrators rights can set the access control level to other users. Paritor aim to conduct an internal privelege audit/review yearly.*

34	ISO27001 / NCSC Cloud Security Principle 9: Secure user management	11.2.3 / 11.5.3	Access Control / User Password Management & Password Management System (Management & Support)	**MUST**	**PASSWORD & ACCOUNT MANAGEMENT** All passwords must be managed securely. Strong passwords must be used for administration of the data handling solution. Strong passwords must be of 8 characters or more, with the use of mixed case alphanumerics with other symbols and not be based on a dictionary word. Account protection mechanisms must also be implemented where supported by hardware and software, including account lockouts, password change intervals, password complexity rules etc. A) Detail the password and account management controls that are in place with regard to all aspects of the management and support of the data handling solution. Examples include local administrator / root accounts, Operating System users, domain users and admins. Strong passwords should also be set for database accounts and web management interfaces. B) Explain how multiple passwords pertaining to system and network components are managed and stored.	*Passwords, both internally and for customers/parents accounts are stored using Microsoft Active Directory - Paritor do not have access to password data - just the ability to reset such data. All passwords are required to conform to strong complexity. For more information on Microsoft's AD password protection, see https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad.*	*Passwords, both internally and for customers/parents accounts are stored using Microsoft Active Directory - Paritor do not have access to password data - just the ability to reset such data. All passwords are required to conform to strong complexity. For more information on Microsoft's AD password protection, see https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad.*
35	ISO27001 / NCSC Cloud Security Principle 9: Secure user management	11.2.4	Access Control / Review of user access rights	**MUST**	**PROVIDER ACCESS & ACCOUNT REVIEW** Accounts associated with the management of and support of all aspects of the data handling solution must be immediately revoked based on a member of staff's employment being terminated or when their role changes. Periodic reviews must also be conducted of Provider access rights. A) Outline the processes that are in place with regard to the review and revocation of Provider user accounts, including review intervals.	*All access to our system is managed by microsoft active directory and microsoft 365. When an emplyee leaves the company access to these accounts is removed. Any equipment held by the employee is returned.*	*All access to our system is managed by microsoft active directory and microsoft 365. When an emplyee leaves the company access to these accounts is removed. Any equipment held by the employee is returned.*
36	ISO27001 / NCSC Cloud Security Principle 12: Secure service administration	11.4.4	Access Control / Remote Diagnostic and Configuration Port Protection	**MUST**	**EXTERNAL INTERFACE PROTECTION** Any external interface for remote diagnostics and support must be suitably protected from unauthorised access. A) Define any remote management, diagnostic or administrative interfaces that exist within the data handling solution B) Describe the protective measures implemented (e.g. encryption, access control lists etc.).	*API Keys can be generated from within Xperios - if the user generating has the correct access control. These API's can be used to retrieve data into external software, in an encrypted manner, such as BI applications. In the event an API key is compromised, they can be deactivated and regenerated from within the software.*	*API Keys can be generated from within Xperios - if the user generating has the correct access control. These API's can be used to retrieve data into external software, in an encrypted manner, such as BI applications. In the event an API key is compromised, they can be deactivated and regenerated from within the software.*
37	ISO27001 / NCSC Cloud Security Principle 5: Operational security	11.5.4	Access Control / Operating System Access Control / Use of System Utilities	**SHOULD**	**SYSTEM UTILITIES CONTROL** Unnecessary system utilities should not be deployed on production servers associated with the data handling solution, unless there is a specific requirement and as agreed. Example include compilers, network sniffers, network utilities and penetration testing tools. A) Detail measures the Provider will take to ensure that such tools are not installed on production servers and any envisaged exceptions.	*No unecessary system utilised are deployed in a production environment.*	*No unecessary system utilised are deployed in a production environment.*

38	ISO27001 / NCSC Cloud Security Principle 12: Secure service administration	11.6.2	Access Control / Application and information access control / Sensitive System Isolation	**SHOULD**	**SENSITIVE SYSTEM PROTECTION** Sensitive systems and interfaces (e.g. virtualisation physical server interfaces, protective monitoring stations, firewall management stations, AV controllers, backup controllers etc...) should not be hosted on production networks. A) Confirm the Providers compliance with this requirement. B) Outline whether management networks will form part of the data handling solution and how the Provider will control access to sensitive systems.	*No sensitive systems are hosted on production networks.*	*No sensitive systems are hosted on production networks.*
39	ISO27001 / NCSC Cloud Security Principle 10: Identity and authentication	11.7.1 - 11.7.2	Access Control / Mobile computing and teleworking	**MUST**	**REMOTE WORKING SECURITY** If support of the data handling solution will at any time be delivered by remote support personnel then this must be delivered securely. The Provider must have encryption (e.g. VPN) and authentication (e.g. 2 factor) in place that will protect remote support mechanisms. The Provider must also have further protective measures in place including remote working policies and data at rest encryption. A) Provide detailed information of how remote support will be provided, including the devices used and mechanisms by which remote support staff will gain access to the infrastructure to deliver support. B) Provide details on any further protective measures that will be implemented.	*Multi-factor authentication and IP-based access control are enabled on all accounts dealing with sensitive data, for the purpose of remote working security. In the event of a compromised account whilst working remotely, the account will be disabled via Azure until appropriate remediation actions have been tkaen.*	*Multi-factor authentication and IP-based access control are enabled on all accounts dealing with sensitive data, for the purpose of remote working security. In the event of a compromised account whilst working remotely, the account will be disabled via Azure until appropriate remediation actions have been tkaen.*
40	ISO27001 / NCSC Cloud Security Principle 5: Operational security	12.3.1 - 12.3.2	Security requirements of information systems / Security of system files / Control of operational software	**MUST**	**SERVER LOCKDOWN** A secure locked down environment must be implemented with regard to servers and workstations that are associated with the support and management of the data handling solution. A) Explain the techniques and any best practice guidelines (for example, CIS and NIST) that the Provider follows with regard to the lockdown of servers and workstations.	*We use the latest version of Microsoft SQL server 2019 - which automatically recieves any crucial security updates as they are available. This server is locked down to a network which only Paritor employee's can access via IP-based access control.*	*We use the latest version of Microsoft SQL server 2019 - which automatically recieves any crucial security updates as they are available. This server is locked down to a network which only Paritor employee's can access via IP-based access control.*
41	ISO27001 / NCSC Cloud Security Principle 5: Operational security	12.5.2	Security requirements of information systems / Security in development and support processes / Technical review of applications after Operating System changes	**SHOULD**	**OPERATING SYSTEM UPDATES** Following Operating System updates, the data handling solution should be tested for continued operation. A) Define the Operating System update process within the Provider organisation B) Explain how the Provider will ensure that GCC's service shall be unaffected by the need to ensure security patches and updates are applied to the underlying Operating System.	*Any OS security updates are automatically managed and applied by Microsoft. In terms of local devices, we use Azure AD to ensure that auto-update is enabled on any company machines.*	*Any OS security updates are automatically managed and applied by Microsoft. In terms of local devices, we use Azure AD to ensure that auto-update is enabled on any company machines.*

42	ISO27001 / NCSC Cloud Security Principle 5: Operational security	13.2.1 - 13.2.3	Information Security Incident Management / Management of Information Security Incidents and improvements	**SHOULD**	**INCIDENT MANAGEMENT PLANS** A plan should be in place for the management of incidents and how to handle the collection of evidence. Typically these are known as Security Incident Management (SIM) plans and a Forensic Readiness Plan (FRP). A) Provide details of any such plans that exist within the Provider organisation and provide copies where available. B) If they do not currently exist, provide a target date for implementation.	*Paritor take daily, weekly, and monthly backups of all databases – which are encrypted at rest. We run a support ticket facility and tickets are classified according to criticality. The user can set this to high, medium or low. This gives a method of direct communication between consumers* *and clients about security related incidents. Paritor has an incident management policy in place, which governs what to do in the event of internal software incidents (unauthorised access, malicious activity, system alerted activity, loss of data, virus, spyware) and external hardware incidents (fire incidents, physical office incidents etc). We aim to test this policy every 6 months.*	*Paritor take daily, weekly, and monthly backups of all databases – which are encrypted at rest. We run a support ticket facility and tickets are classified according to criticality. The user can set this to high, medium or low. This gives a method of direct communication between consumers and clients about security related incidents. Paritor has an incident management policy in place, which governs what to do in the event of internal software incidents (unauthorised access, malicious activity, system alerted activity, loss of data, virus, spyware) and external hardware incidents (fire incidents, physical office incidents etc). We aim to test this policy every 6 months.*