PARITOR XPERIOS

Data Hosting and NCSC Cloud Security Compliance Report

April 2021

Paritor Ltd

P PARITOR

info@paritor.co.uk

www.paritor.com

Contents

P1. Contents and Report Information

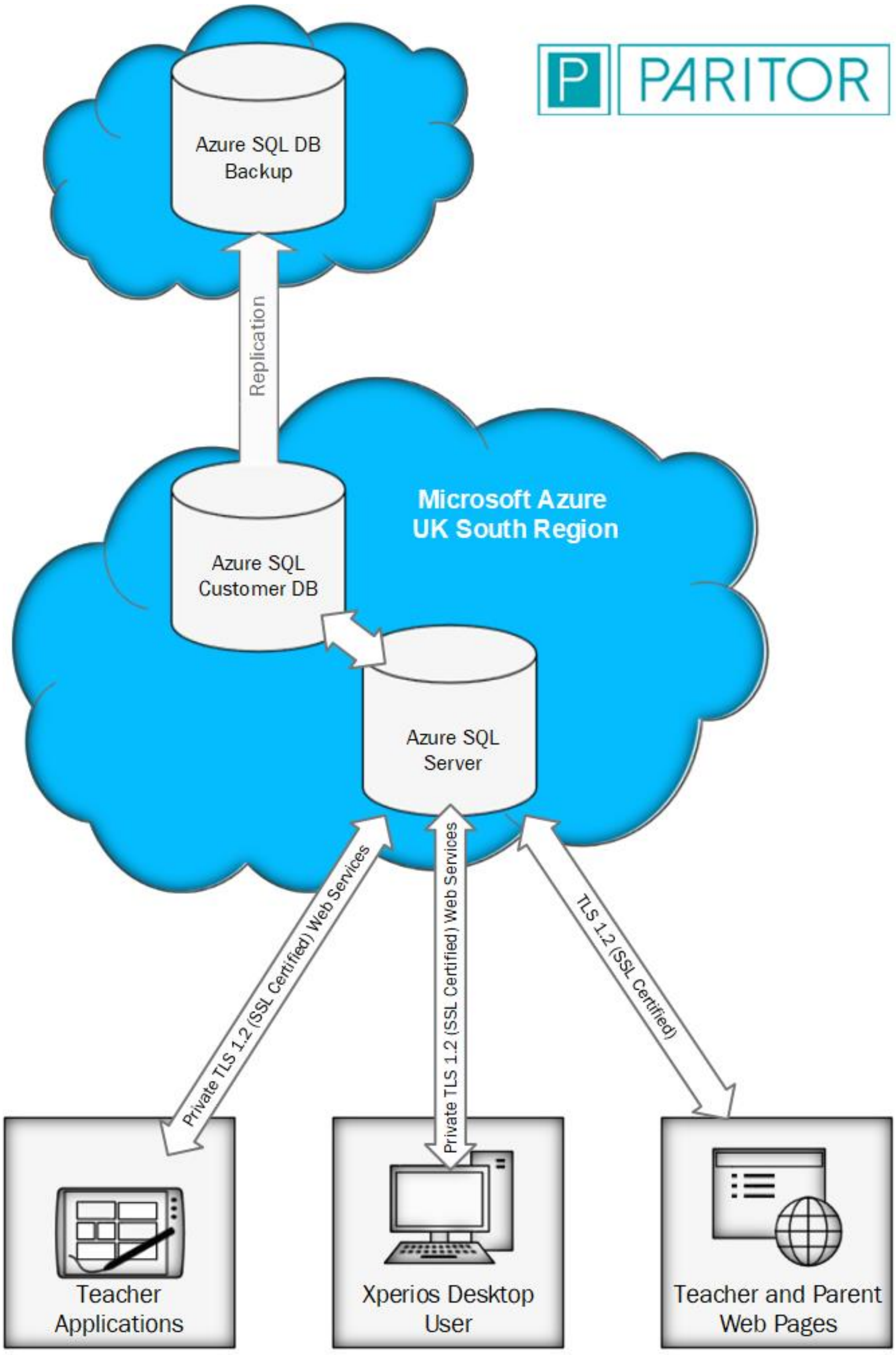
P2. Cloud Security Guidance Principles

Report Description

The UK government requires that councils ensure that suppliers of web applications follow a set of principles to ensure the confidentiality, integrity, and availability of council data. Where the data contains personal data, the supplier will be considered a data processor under the terms of the Data Protection Act 2018.

The principals are named the Cyber Security Principles. Please review these principles and the guidance around how these principles might be met or not. Guidance on these principles is published at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles This document provides the compliance of Paritor Ltd in regard to these security principles.

ACCESS AND SECURITY COMPLIANCE The following 14 questions relate directly to the 14 Cloud Security Principles published on the National Cyber Security Centre website. The starting page for these can be found here.	
	PRINCIPLE 1: **Explain** how your solution will provide protection for data in transit. Ensure you provide specific details of all the mechanisms in your solution that address this principle.
	All data transferred between the hosted data and the operational PCs is encrypted and provided via private web services using TLS 1.2. Access to these web services is limited to the software and must first be authenticated as a valid client and client member. **The transfer of data between Azure storage centres (for backup) is managed via dedicated private networks encrypted with a 2048 bit SSL certificate.**
	PRINCIPLE 2: Explain how your solution will provide asset protection and resilience. Ensure you provide specific details of all the mechanisms in your solution that address this principle. *User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage, or seizure.*
	PRINCIPLE 2: 1 Physical location and legal jurisdiction *The supplier must clearly state in which countries council data will be stored, processed and managed.*
	All customer data is stored, processed, and managed within the United Kingdom. The specific location used for data storage is London (UK South datacentre location on Azure). Please see the below Infrastructure diagram for more detail.

	 PARITOR Azure SQL DB Backup Replication Microsoft Azure UK South Region Azure SQL Customer DB Azure SQL Server Private TLS 1.2 (SSL Certified) Web Services Private TLS 1.2 (SSL Certified) Web Services TLS 1.2 (SSL Certified) Teacher Applications Xperios Desktop User Teacher and Parent Web Pages Copyright © Paritor Ltd 2021
	PRINCIPLE 2: 2 Data centre security *The supplier must describe the physical security measures employed at any data centre where council data will be stored, processed and managed.*

Our data is stored in Microsoft’s globally distributed datacentre infrastructure via Azure. Datacentres managed by Microsoft have extensive layers of protection: access approval at the facility’s perimeter, at the building’s perimeter, inside the building, and on the datacentre floor. The specific layers of physical security are:

- **Access request and approval. You must request access prior to arriving at the datacentre. You are required to provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the datacenters to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the datacenter required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.**

- **Facility’s perimeter. When you arrive at a datacentre, you're required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacenters, with a security team monitoring their videos at all times.**

- **Building entrance. The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter, and monitor the videos of cameras inside the datacenter at all times.**

- **Inside the building. After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the datacenter. If your identity is validated, you can enter only the portion of the datacenter that you have approved access to. You can stay there only for the duration of the time approved.**

- **Datacenter floor. You are only allowed onto the floor that you're approved to enter. You are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the datacenter floor, you again must pass through full body metal detection screening. To leave the datacenter, you're required to pass through an additional security scan.**

Source: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

PRINCIPLE 2: 3 Data at rest protection

You supplier must describe the physical and technical measures in place to ensure storage media containing council data are protected from unauthorised access.

All our data stored within Azure is encrypted at rest with 256 Bit AES Encryption. This includes data stored on our Azure Virtual Machines and VHD using Azure Disk Encryption. All client data is stored within Microsoft Azure SQL databases, with one unique database per client.

PRINCIPLE 2: 4 Data sanitisation

The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data.

	The supplier must describe what processes they have in place to ensure council data is erased when resources are moved or re-provisioned, when the council ceases to use the service or the council requests its data to be erased. *The supplier must decscribe what processes they have to ensure that storage media which has held council data is sanitised or securely destroyed at the end of its life.*
	Should the data hosting agreement be cancelled then the client, once satisfying itself that it has taken a local copy of the data, can request in writing that the company disposes of all hosted copies of the data. Should such instructions not be received within a period of three months from any cancellation of service the company will destroy all copies of the data, such as the data held within the SQL databases. If a council requests specific data to be erased, all copies of select records will be securely destroyed.
	PRINCIPLE 2: 5 Equipment disposal Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or council data stored in the service. *The supplier ,must describe what processes they have in place to ensure that all equipment potentially containing council data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled); that any components containing sensitive data are sanitised, removed or destroyed as appropriate; and that accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.*
	If a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before it is returned to the manufacturer for replacement or repair. The data on the drive is completely overwritten to ensure the data cannot be recovered by any means. **When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.**
	PRINCIPLE 2: 6 Physical resilience and availability *The supplier must state a minimum level of service availability which they will guarantee and describe the processes they have in place to ensure that level of service is maintained.*
	The services hosted within Azure are being constantly monitored, to ensure the availability of the Data Hosting is at least 99% during the hours of 9am to 5.00pm on Business Days (Normal Business Hours). This availability does not include customer-caused or third party-caused outages or disruptions.
	PRINCIPLE 3: Explain how your solution will provide separation between consumers. Ensure you provide specific details of all the mechanisms in your solution that address this principle. *A malicious or compromised user of the service should not be able to affect the service or data of another.*

	You should describe the types of user you share the service or platform with; describe how your service is separated between different users of the service; and describe how the management of your service is kept separate from other users (covered separately as part of Principle 9)
	Each consumer is provided with a unique database stored on Microsoft's Azure SQL server. This database has a unique identification number and password; however, these are only used by Paritor's Internal API. An initial 'super-user' is associated with the database, who can then grant further users access from within the system. Each database is stored in its own unique Azure database, making it impossible for a malicious consumer to access an unknown database.
	PRINCIPLE 4: Explain how your solution will provide a governance framework. Ensure you provide specific details of all the mechanisms in your solution that address this principle. *The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Having an effective governance framework will ensure that procedure, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments and the appearance of new threats. You should provide sufficient information to give confidence that the service has a governance framework and processes which are appropriate for its intended use.*
	Paritor have a dedicated chief technical officer, who works closely with select few individuals to ensure that any changes being made to the physical and technical security procedures are in line with constantly developing threats. The datacentre we use is fully compliant with ISO 27001 which is an international standard outlined by the International Organization for Standardization (ISO).
	PRINCIPLE 5: 1 Configuration and change management *The supplier must provide details of the the status, location and configuration of service components (both hardware and software) and how they are are tracked throughout their lifetime.* *The supplier must provide details of how changes to the service are authorised and managed.* *The supplier must provide details of the processes employed to ensure changes to the service are assessed for potential security impact and how these are then managed and tracked through to completion.*
	An infrastructure engineer is employed to ensure the correct location, configuration and status of service products hosted through Azure. Azure provides comprehensive details on its services – allowing for constant health monitoring of crucial components and ensuring a high level of availability. Paritor have a change management board in place, and any changes to the service require review and approval from this board before implementation can occur.
	PRINCIPLE 5: 2 Vulnerability management *Suppliers must describe the management processes they have in place to identify, triage and mitigate vulnerabilities.*

	You should detail how potential new threats, vulnerabilities or exploitation techniques which could affect your service are assessed and corrective action is taken; how you monitor relevant sources of information relating to threat, vulnerability and exploitation techniques; how the severity of threats and vulnerabilities is considered within the context of the service and this information is used to prioritise the implementation of mitigations and how you use a suitable change management process, known vulnerabilities are tracked until mitigations have been deployed and what your timescales are for implementing mitigations.
	Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run OS, web application, and database scans of the Azure environment. All office computers are installed with the latest security updates via Windows update centre, with Windows Defender and Malwarebytes installed. We use outlook for mail exchange, with MFA enabled across all our O365 logins. We use a service known as Server Scan, a PCI scanning tool to provide us with vulnerability recommendations. We test and migrate in our own environment before uploading to Azure.
	PRINCIPLE 5: 3 Protective monitoring *The supplier must give details of how they monitor their service to detect malicious activity, how they detect security incidents and how they take action to address identified incidents.*
	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 non-malicious. 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.**
	PRINCIPLE 5: 4 Incident management *The supplier must describe the incident management processes they have in place including pre-defined processes for responding to common incidents; what processes you have in place for the reporting of security incidents by the council or other external entities; and how you will report on security incidents which are relevant to the council including your timescales for reporting.*
	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.

	PRINCIPLE 6: Explain how you ensure personnel security. Provide specific details of all the mechanisms in your solution that address this principle. *Where service provider personnel have access to council data and systems the council needs a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.* *The service provider should subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities. Providers should make clear how they screen and manage personnel within privileged roles.* *You should provide information on how you ensure that the level of security screening conducted on service provider staff with access to your information, or with ability to affect your service, is appropriate and that the minimum number of people necessary have access to your information or could affect your service.*
	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.
	PRINCIPLE 7: Explain how you ensure secure development. Provide specific details of all the mechanisms in your solution that address this principle. *Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.* *You should provide details about how new and evolving threats are reviewed and the service improved in line with them; development is carried out in line with industry good practice regarding secure design, coding, testing and deployment; and configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.*
	We use Microsoft DevOps, with only authorised users permitted access to the coding repositories. All changes are logged using the Git management system. Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan. In addition, Microsoft provides native antimalware on all Azure VMs. Our development team adhere to the most recent security risks via the OWASP Top 10 Critical Web Application guidelines, version 2017.
	PRINCIPLE 8: Explain how you ensure supply chain security. Provide specific details of all the mechanisms in your solution that address this principle. *The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.* *You should detail: how council information is shared with, or accessible to, third party suppliers and their supply chains; how your procurement processes place security requirements on third party suppliers; how you manage security risks from third party suppliers; how you manage the conformance of their suppliers with security requirements; and how you verify that hardware and software used in the service is genuine and has not been tampered with.*

	The only third-party supplier used is Microsoft Azure, with a Microsoft Online Subscription agreement in place (https://azure.microsoft.com/en-gb/support/legal/). Microsoft are used only for the purpose of server and data hosting and do not have access to council data.
	PRINCIPLE 9: Explain how you ensure secure consumer management. Provide specific details of all the mechanisms in your solution that address this principle.
	PRINCIPLE 9: 1 Authentication of users The supplier must detail how users of the service are authenticated over each of the channels – e.g. web portal, Email, telephone – used in providing the service and how any management services which could have a security impact are performed over secure and authenticated channels. The suppler must describe all of the mechanisms by which they provider would accept management or support requests from the council and ensure that only authorised individuals from the council can use those mechanisms to affect your use of the service. The supplier must ensure that the strength of the identity and authentication processes is commensurate with the security of the council data processed.

	PRINCIPLE 9: 2 Separation and access control within management interfaces. The supplier must provide details of how use access to council data and service is contrained appropriately so that users from other organisations cannot access, modify or otherwise affect the council's service management; how council users are provided access based on the principle of least privilege; and how management interfaces are protected and what functionality they expose.
	Each client administrator is provided with an individual database specific to their service, with an initial association between their user email and database. In the system, access to this database is controlled by the client administrator. Administrators can set which data each user of the system can access, and how they can manipulate such data (no access/read only/write).
	PRINCIPLE 10: Explain how your solution will provide identity and authentication. Ensure you provide specific details of all the mechanisms in your solution that address this principle. *All access to service interfaces should be constrained to authenticated and authorised individuals. Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service. Importantly, authentication should occur over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering attacks.*
	Comprehensive security is built into Xperios, with access to the data and functions within the system controlled via user groups and user accounts. A user must be invited to the database from an administrator to gain access. The user then signs into their Schooble account and only once signed in will be able to access the database associated with that login.
	PRINCIPLE 11: Explain how your solution will provide external interface protection. Ensure you provide specific details of all the mechanisms in your solution that address this principle. *All external or less trusted interfaces of the service should be identified and appropriately defended.* *You must provide information which clearly shows what physical and logical interfaces council information processed in your solution is available from, and how access to your is controlled and show how your solution identifies and authenticates users to an appropriate level over those interfaces (see Principle 10)*
	API Keys can be generated from within Xperios. These API's can be used to retrieve data into external software, such as BI applications. In the event an API key is compromised, they can be deactivated and regenerated from within the software.
	PRINCIPLE 12: Explain how your solution will provide secure service administration. Ensure you provide specific details of all the mechanisms in your solution that address this principle. *Systems used for administration of a ervice will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.* *The design, implementation and management of administration systems should follow enterprise good practice, whilst recognising their high value to attackers.*

	You should provide information which clearly shows the service administration model being used in your solution to manage the service.
	A single client administrator is granted initial access to the system. From here access is controlled by user groups and associations. Moreover, frequent audits and logging are available to identify suspicious internal behaviour.
	PRINCIPLE 13: Explain how your solution will provide audit information. Ensure you provide specific details of all the mechanisms in your solution that address this principle. *You should provided with audit records sufficient to monitor access to your service and the data held within it.* *You should provide details of the audit information that will be provided to in your solution, how and when it will be made available, the format of the data, and the retention period associated with it.*
	Usage of any function within the system is logged together with any changes made providing users with full audit trails of all access and modifications to their data. This log includes the date, user, source, record type and records modified. These logs are only available to those with administrator rights and are available through the software.
	PRINCIPLE 14: Explain how your solution will ensure secure use of service by the consumer. Provide specific details of all the mechanisms in your solution that address this principle. *The security of ICT solutions and the data held within them can be undermined if the service is not used well. You must supply sufficient information to enable us to ensure that we are using the solution properly.* *You must give details of any service configuration options available to the council and the security implications of the choices which have to made in using the solution. You must also provide detailed information of the security requirements for our use of the solution.*
	The service is only available on local, enterprise managed devices. Therefore, the security of the service relies on an appropriate security policy and procedures to be in place by the consumers. It is not possible to access Ensemble via non-authorised devices.

Legal Disclaimer

The information contained in this document represents the current view of Paritor Ltd on the issues discussed as of the date of publication. Paritor Ltd must respond to changing market conditions, therefore it should not be interpreted to be a commitment on the part of Paritor Ltd, and Paritor Ltd cannot guarantee the accuracy of any information presented after the date of publication. This Conformance Report is for informational purposes only. PARITOR LTD MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.