GOVERNMENT OF WESTERN AUSTRALIA

HSS health support services

Cloud Service Assessment Form

Health Support Services Security and Risk Management

January 2021

Document control and approval

Version	Date	Author	Comments	File Ref
1.0	23.10.2020	HSS SRM	Initial document	
2.0	20.01.2020	HSS SRM	Transferred to HSS template	
2.1	22/02/2021	HSS SRM	Review and update	

This Cloud Service Assessment Form is intended to assist WA Health System entities who are considering procurement of cloud computing services. As requirements may vary considerably, this document should be regarded as a checklist outlining the baseline requirements in accordance with the MP 0140/20 Cloud Policy and supporting Cloud Service Requirements.

HSS Security & Risk Management (HSS SRM) team are available to advise and support you through completing the assessment via infosec@health.wa.gov.au.

How to complete this form:

- Sections 1 to 4 of this form must be completed for all cloud zones. Sections 5 and 6 are required only for cloud services outside of zone A (HealthNext)
- Identify and assess the risks of engaging with the proposed cloud service using the Risk Assessment Tables for the WA Health System
- Send the completed assessment and supporting documents to infosec@health.wa.gov.au

HSS SRM will:

- Review your assessment to ensure it meets *Cloud Policy* requirements;
- Identify any gaps or inconsistencies and advise where further information is required; and
- Record the details of the cloud service in the Cloud Services Register for reporting and auditing purposes

1. REQUESTOR DETAILS	
Date of Request	2020-11-06
Requestor Name and Title	[redacted]
Health Service Provider / DOH Division	Department of Health

2. CLOUD SERVICE DETAILS	
Cloud Zone	☐ **Zone A (HealthNext)** ☒ **Zone B** ☐ **Zone C**
Service Status	Is the cloud service a new initiative or from an existing operation/project? ☒ **New** ☐ **Existing**
CAR ID (if applicable)	CAR not applicable. Business Case: C19RBC – 108 Implementation of a QR Code Venue Check-In System (Obj Id qA311891)
Name of Cloud Service	SafeWA
Name of Cloud Service Provider	GenVis Pty Ltd / Amazon Web Services (AWS)
Short Description of the Cloud Service	Business need – WA Health is seeking to support the State Government's decision to remove the Hard Border whilst putting in place mechanisms to augment the existing contact tracing system and limit the spread of coronavirus. Functional and Non-Functional requirements are set out in the WA QR Code Implementation Request for Proposal document (Obj. Id fA3924664).
Contract Status	☒ **Active** ☐ **Expired** ☐ **Unknown**
Contract Expiry Date	18/11/2021 Note: This contract is subject to 2x one-year extension options at the discretion of Health Support Services (HSS).

3. CLOUD RISK ASSESSMENT DETAILS

Risk Rating	☐ **Low** ☐ **High** ☒ **Medium** ☐ **Extreme** *Refer to the Risk Acceptance/Tolerance Criteria for the WA Health System*
Risk Assessment Summary	*Provide details that support your risk rating – attach additional pages, if required* Refer to details within documented risk assessments (Obj Id fA3920424).

4. BASELINE REQUIREMENTS

Complete this section if the cloud service is in Zones A, B, or C

Classification of Information

- *Ensure the classification of the information to be stored and processed is clearly identified and communicated, to inform the risk assessment and control process in accordance with the **OD 0537/14 Information Classification Policy***
- *The Classification will inform users of any special handling or control instructions e.g. The Classification may need to be included on login / processing screens and documentation*

Note: Cloud Zone C is not to be used for sensitive information.

What is the classification of the information to be stored and processed via the proposed cloud service?

☐ **Unofficial**

☐ **Official**

☒ **Official: Sensitive**

Refer to the WA Information Classification Policy, released by the Office of Digital Government in June 2020

Provide additional details

Data Steward Approval

- *Ensure the Data Steward and Data Custodian of the information and system are identified and confirm there is full support for implementing the cloud service*
- *The Data Steward and Data Custodian will be the published contact for all queries relating to this service*
- *The Data Steward remains responsible for overall management and authorisations*

A senior controller of the information and service must be identified.
This will be the published contact for all queries relating to this system.

Data Steward: [redacted]

Data Custodian: [redacted]

☒ **Confirmed full support for implementing the cloud service**

Provide additional details

From Genvis:
Full Name: [redacted]
Position: Chief Technology Officer at Genvis
Email: [redacted]@genvis.co
Contact Number: [redacted]

	Business Continuity Plans	• *Once the service is operational, ensure business continuity plans are established to prevent/minimise service disruption, in the event of an internet outage, natural disaster or cyber-attack:*
		  - *Vendor: will need backup and recovery plans*
		  - *HSP: will need local business continuity plans*
		• *Requirements for business continuity plans are outlined in **OD 0595/15 Business Continuity Management***
		• *Consult with the local site or application/information business continuity manager for details (if unsure request details from infosec@health.wa.gov.au).*

		Provide details of backup and recovery plans from cloud service provider *Develop local business continuity plans as appropriate - consult with your local business continuity manager for details* Database and application servers are deployed across multiple availability zones within Australia to allow for system redundancy. Data is backed up during specified maintenance windows and persisted for ease of restoration for a 2-month period. There is no observable user impact for system failover.
	Other Risks	*Ensure any other specific legislative requirements (e.g. mental health, HIV, juvenile etc.) and risks relevant to this information are addressed* *Note: The Data Steward must identify and satisfy legislative requirements in addition to the baseline requirements.*
		Are there specific legislative requirements and risks that impact on this service? ☐ **No** ☒ **Yes** *Provide additional details – attach a separate risk analysis, if required* The targeted number of users and expected daily load of check ins is high. To ensure service delivery, HSS will undertake load testing on the system prior to the go live date to ensure the system has sufficient capacity to perform efficiently under load. Further Genvis solution is cloud native which allows the real-time autoscaling of the database horizontally and vertically as well as the API service layers. A penetration and security test will be performedon the system by a reputable third party, Riot Solutions prior to go live to ensure data security. Continuous vulnerability assessment tooling provides intrusion detection alerts, which are subsequently blocked using AWS Web Application Firewall configurations. This consists of, but is not limited to; • Known malicious IP addresses • Common Linux attack prevention • Unix request attack prevention • SQL injection attack prevention In addition, HSS will undertake independent vulnerability testing to provide further assurance around data security.

5. BASELINE REQUIREMENTS

Additionally, complete this section if the cloud service is in Zones B or C

Evaluation Due Diligence	*Outline the reasons why Zone A is not suitable. The Data Steward needs to be satisfied that an assessment of Zone A services has been completed and it has been found to be not suitable.*
	Provide additional details This is a fully managed, comprehensive and extensible SaaS platform delivered to WA Health by GenVis and already in use by WA Police since March 2020 where it has been the underlying technology that they have relied on to enforce and manage travel restrictions across the state. Genvis platform is built specifically for public safety teams and is a fully featured modular solution that allows for the quick development of new features and modules that support customer needs. Each module can interact with each other based on roles and permissions. Genvis as a company only works with public safety/government agencies and takes a partnering approach whereby the customer requirements and workflows are fully understood and appreciated by the product and engineering teams allowing them to open up new workflow enhancements.

Privacy	*Ensure privacy obligations can be met for the term of the contractual arrangement. These obligations include:*
	
	• *understanding how privacy of patients and staff could be jeopardised by the information being stored within the cloud service*
	• *obtaining assurance from the cloud service provider on the security and accessibility of information including:*
	  - *where it will be stored/backed-up*
	  - *who will have access to the information and how will this access be controlled*
	  - *how will security be managed within the cloud service*
	  - *whether the WA health system need to give up control of the information*
	• *obtaining confirmation from the cloud service provider regarding their compliance with Australian Privacy Principles, including how they address privacy breaches and any cross-border disclosure of personal information requests*
	• *confirming that all information disclosure requirements, as outlined in **MP 0015/16 Information Access, Use and Disclosure Policy** and **MP 0010/16 Patient Confidentiality Policy** will be implemented*

	Have you addressed the privacy requirements outlined in the Cloud Policy and Cloud Service Requirements? ☐ **No** ☒ **Yes** *Provide additional details, including privacy risk assurance from cloud service provider as well as details of compliance to APP and disclosure requirements outlined in the policies – attach any documents/records to reference (if available)* Genvis works closely with its customers and relevant regulatory bodies, including SSO to ensure all our services comply with each customer's specific privacy requirements including what data can be captured and for what purpose, who can access it and how long it is stored.

	Information Breach Notification	*Ensure that there is a clearly documented information breach management and notification process, including:* • *who will receive notifications and when* - *listing of any external parties to the contract who need to be notified* - *how the vendor will respond if information is lost or accessed in the event of an accidental or malicious incident by an:* ▪ *internal attack* ▪ *external attack*
		Is there a documented information breach management and notification process? ☐ **No** ☒ **Yes** *Provide additional details – attach documented information breach management and notification process from cloud service provider (if available)* Our Services comprise network level firewalls to protect the perimeter and segregate the cloud services appropriately. Vulnerability scanning and intrusion detection systems constantly monitor and alert whenever anomalies are detected. All security information events are stored and Genvis is able to search this information for investigation purposes. These measures ensure we can rapidly respond to any issues that arise and in the unlikely event of a security breach, Genvis will promptly notify WA Health of any unauthorized access to, or loss of data. In the unlikely event of a data breach Genvis will work closely with WA Health to determine what obligations we have under the Notifiable Data Breaches scheme and what information, if any, needs to be disclosed to the OIAC.
	Security Standards	• *Ensure security standards comply with the WA health system* ***MP 0067/17 Information Security Policy*** • *Assess what security measures are available including the suitability of password complexity rules and use two-factor authentication (e.g. biometrics, SMS verification, or authenticator app) wherever possible*
		In compliance with Information Security Policy, are there appropriate controls in place to protect health information and systems from theft, fraud, malicious or accidental damage, and privacy or confidential breaches? ☐ **No** ☒ **Yes** *Provide additional details, including available security measures – attach information security documentation from cloud service provider (if available)* App users must verify their accounts by entering a PIN sent to them by SMS at the time of creating their account. All passwords must be a minimum of 10 characters in length. AWS offers two-factor authentication for their services. Access to production AWS accounts is limited to the absolute minimum number of people necessary. All Genvis access control decisions are guided by the principles of Need to Know basis and Least Privileges in order to limit risk.

	Identity Management	*Assess whether there are any risks posed by the types of user accounts to be registered with the vendor. For example:* • *What login identities and passwords will be used?* • *Who will have management responsibility?* • *What WA health system details will be registered with the cloud service provider (and how can these be minimised)?* ***Any external registration must NEVER re-use WA health system user passwords.***
		Provide details Any credentials given to Genvis in order to deliver the services and in particular API integrations will never be reused. The data controllers from both WA Health and Genvis will have full identity management responsibility. End users are required to provide name and phone number and must create a password at account creation.In addition, business users and administrators must provide an email address.
	Intended Users	• *Understand who the intended users of the cloud service are (internal to the WA health system or public)* • *Assess any risks or issues posed via users accessing the service, for example, will the system be accessed by the public and how will access be managed* • *Understand how access will be disabled when no longer required, for example, staff movement or departures.*
		Who are the intended users of the cloud service? ☐ **Internal to the WA Health System** ☒ **Public** *Provide additional details, including risks and account management* 1. Primary contacts from the Business or Organisation 2. Members of the Public 3. Public Health Operations (PHOps) Representatives

	Administrative Access	• *Understand who will have full administrative access to the cloud service and the stored information* • *If full control does not remain with the WA health system, ensure protection measures for stored information & information being transmitted are included (i.e., encryption)*
		Does full administrative access remain with the WA Health System? ☒ **No** ☐ **Yes** *Provide additional details, including protection measures for information* Key Genvis staff will have full administrative access to the service and stored data in order to deliver the services. This access must first be granted in writing by WA Health with each request specifying the reason and the length of time the access is required. Genvis staff seeking to access the service and data are based in Australia, the majority in Perth and all have undergone integrity checks by WA Police in order to deliver G2G PASS and G2G Now. Genvis employs strict data protection measures to ensure all data is stored safely, backed up and is encrypted in transit and at rest.
	Information Ownership and Retrieval	*Ensure that contract documentation:* • *stipulates the WA health system retains ownership of all information and/or intellectual capital (IP) - the vendor is not permitted to extract subsets or metadata for their own purposes, for example, marketing or service analysis* • *detail what happens to WA health system information if the cloud service provider is purchased by another company or the contract is terminated* • *clearly defines cloud service ownership and partnerships used to deliver the service (i.e., trusted third parties)* • *If the vendor is not independent, i.e. owned by a parent company, the contract documentation should also ensure that the WA health system entity's information cannot be accessed by the parent entity*
		Does WA Health System retain ownership of information? ☐ **No** ☒ **Yes** *Provide additional details including contract documentation from cloud service provider* All data is owned by WA Health and accessed by Genvis in order to provide the services. Genvis agrees to not extract subsets or metadata for their own marketing or analysis purposes. The vendor is an independent, Western Australian company. If the vendor is purchased by another company no changes to data ownership will occur. Data remains at all times owned by WA Health.

	Compliance with WA Health System Retention, Destruction and Disposal Policies	• *The WA health system's record retention requirements are as specified in the following schedules:*
		  - ***MP 0002/16 Patient Information Retention and Disposal Schedule***
		  - *Retention and Disposal Schedule for Administrative and Functional Records*
		• *The cloud service provider should return information to the WA health system on request, and at the conclusion of the contract, in a usable format*
		• *Information which may need to be used as evidence should be proven as authentic, reliable, and not altered or tampered with in any way*
		
		Note: *MP 0002/16 Patient Information Retention and Disposal Schedule is no longer applicable – superseded by* ***MP0144/20 Information Retention and Disposal Policy*** *(1 December 2020)*

		Provide details The vendor agrees to comply with WA Health privacy and data policies. As required in QR0012 all data collected via the QR Code solution will be stored for 28 days and then deleted on the 29th day in line with the Emergency Management Act. Data and security logs are stored for a period of 2 months before deletion. This time window can be adjusted as per WA Health's requirements. **Exit strategy** At the expiry of the contract Genvis will require written confirmation of the WA Health's intention to close down the G2G Go system. A statement of work will be agreed and issued with engineering charges to be quoted per the rate card shown with pricing information attached. All data stored and processed by the system can be exported in a prescribed format and made available to WA Health on contract expiry. This data is then permanently deleted from the system. Any cloud services and/or machine instances utilised for provisioning of the solution to WA Health will be shut down. All user access will be revoked.
	Service Level Agreement (SLA)	*If a Service Level Agreement can be established for this arrangement, it must address the following:* • *Where, when, and how fast the service needs to be consumed* • *Acceptable service downtime arrangements for patch or maintenance activities*
		Is there an SLA established? ☐ **No** ☒ **Yes**

		Provide details – attach documentation, if available The GenVis SLA and related documentation is available in Objective (Id fA3924661). AWS cloud service SLA's are sufficient to support Genvis in delivering on these SLA's. More information about AWS SLA's can be found here: https://aws.amazon.com/compute/sla/
	Certification	*Information Security Registered Assessors Program (IRAP) or Service Organisation Control 2 (SOC 2) certification is considered highly desirable.*
		Identify vendor certification, if available ☐ **IRAP** ☐ **SOC 2** ☐ **None** ☐ **Others, please specify below** *Provide details – include link and/or documentation of vendor's certifications* None provided
	Penetration Test	*An independent penetration test of the proposed cloud service is considered highly desirable. It will provide information on whether there is any security:* • *vulnerabilities that an attacker could exploit, and/or* • *weaknesses that need to be addressed*
		Is there an independent penetration test done on the cloud service? ☐ **No** ☒ **Yes** *Provide additional details*
	Costs	• *Ensure a total cost of operation comparison has been undertaken.* • *Verify the full tenure of the proposed cloud service – is there a contract/minimum term?* • *Verify the full financial costs of the proposed service during its lifetime – how will these be met, and by whom* • *Verify cloud service capacity to meet the required needs?*

		Provide details As at the date of this submission, the full price of a fixed 12-month contract is $1,086,800 including development and implementation fees with the option to renew for a further 24 months. The fees for the second and third years are both The fixed fee for year 2 and year 3 is $990,000p.a. Lifecycle - The initial contract period will be 12 months with the option to renew for a further 24 months.

6. BASELINE REQUIREMENTS

Additionally, complete this section if the cloud service is in Zone C

Geographic Location(s)	• *Ensure the classification of the information is suitable for being offshored* • *Ensure the country or countries in which the information will be stored are identified* • *Ensure the contractual and legislative environment does not contravene the WA health system legal obligations for information protection, performance management, contract termination, contract management*
	List countries in which the information will be stored – provide additional details
Executive Approval	*Prior to the final deployment of any service into Zone C, written approval must be granted by the Data Steward (as per the Delegation Schedule – Health Information) and recorded in the Cloud Services Register.*
	☐ **Confirmed – written approval must be obtained prior to deployment of cloud service** *Provide additional details*

This document can be made available in alternative formats on request for a person with disability.