**GovCrate Private Cloud**

GovCrate is an application construction and cloud-hosting solution which is secure, fault tolerant and scalable with a readily programmed data infrastructure build that is regulation compliant. Through GovCrate, government ministries and departments can reduce the time required to develop and build any application (“app”), as the back-end foundational development is provided.

**Features**

* Cloud software government application builder in a box
* Scales up/down automatically with logging/auditing/monitoring built in
* Fault tolerant and high availability
* Single point of contact for your organisation
* Adheres to security best practices of the cloud infrastructure provider
* Intrinsic security from GovCrate and confidentiality
* Fully detailed documentation for security or Information Governance audit
* Handbook with easy-to-use guidelines on implementation

**Benefits**

* Dramatically speeds up time to implementation of new software
* Cost-saving and time-saving, fully interoperable with external cloud services
* Encourages GDPR compliance
* Encourages and incorporates 2-factor authentication for sign-in
* Security-hardened to best practises
* Scalable to changes in user numbers and scale of operations
* Significant cost reductions in development

**Pricing $10,000 per instance**

* Education and Social Services pricing available

**Service documents**

**Framework**

Viviki

**Contact**

**WHUPI LIMITED**

**Service scope**

|  |
| --- |
|  |
| Software add-on or extension | No |
| Cloud deployment model | Public Cloud |
| Service constraints | GovCrate is a one-time purchase product. A maintenance contract can be purchased for a recurring fee. What this maintenance provides is updates to the underlying infrastructure from time to time where we may make improvements or run updates. However once you take the licences you own the output of GovCrate and we do not make any amendments or updates to anything you have built. Further information can be obtained upon request. |
| System requirements | No system requirements |

**User support**

| User support |
| --- |
|  |
| Email or online ticketing support | Email or online ticketing |
| Support response times | Support is 9-5 GMT Mondays to Fridays by email.   No ticketing is available at this time |
| User can manage status and priority of support tickets | No |
| Phone support | No |
| Web chat support | No |
| Onsite support | No |
| Support levels | We provide you with detailed technical documentation and a simple training document, complete with examples. However the infrastructure is created in your own accounts to which we will not have access. Support is available by email and we can escalate to phone or onsite support if required on a case-by-case basis. |
| Support available to third parties | Yes |

**Onboarding and offboarding**

|  |
| --- |
|  |
| Getting started | We provide both a simple and intuitive user document, and detailed technical documentation. Any further questions that the client has can be raised by email with our tech team and will be addressed on a case-by-case basis. The sample application itself forms part of a 'how-to-use' guide for the created stack. |
| Service documentation | Yes |
| Documentation formats | * HTML * PDF |
| End-of-contract data extraction | Because the infrastructure is created in the client's own Cloud accounts, then they own the configuration right from the start with no lock-in. |
| End-of-contract process | We cease to provide security updates and fixes to infrastructure provisioned by the solution. On a case-by-case basis we can provide additional updates for security and infrastructure at a cost.  The product the client buys is a fully provisioned tech stack and app with supporting documentation. |

**Using the service**

|  |
| --- |
|  |
| Web browser interface | No |
| Application to install | No |
| Designed for use on mobile devices | Yes |
| Differences between the mobile and desktop service | The sample application that we provide is designed as a responsive web-app and can run on mobile and desktop. |
| Accessibility standards | None or don’t know |
| Description of accessibility | This is the client's responsibility to ensure that applications written on top of our stack comply with any and all accessibility requirements that they have. |
| Accessibility testing | N/A |
| API | No |
| Customisation available | Yes |
| Description of customisation | The client can customise the sample application with any features they require. In addition, the stack is application agnostic and will work with any solution that can be placed in a Docker container. |

**Scaling**

| Scaling |
| --- |
|  |
| Independence of resources | All applications are run in multiple availability zone deployments that take full advantage of Amazon's auto-scale abilities. We also provide the ability to do hot-deployments to eliminate system downtime. Multiple load balances are also incorporated into the system design to allow for vertical and horizontal scalability. |

**Analytics**

| Analytics |
| --- |
|  |
| Service usage metrics | Yes |
| Metrics types | This is provided by AWS CloudWatch. |
| Reporting types | * API access * Real-time dashboards * Regular reports * Reports on request |

**Resellers**

| Resellers |
| --- |
|  |
| Supplier type | Not a reseller |

**Staff security**

| Staff security |
| --- |
|  |
| Staff security clearance | Staff screening not performed |
| Government security clearance | Up to Developed Vetting (DV) |

**Asset protection**

| Asset protection |
| --- |
|  |
| Knowledge of data storage and processing locations | Yes |
| Data storage and processing locations | * United Kingdom * European Economic Area (EEA) * EU-US Privacy Shield agreement locations * Other locations |
| User control over data storage and processing locations | Yes |
| Datacentre security standards | Managed by a third party |
| Penetration testing frequency | Never |
| Protecting data at rest | * Physical access control, complying with SSAE-16 / ISAE 3402 * Encryption of all physical media * Scale, obfuscating techniques, or data storage sharding |
| Data sanitisation process | No |
| Equipment disposal approach | Complying with a recognised standard, for example CSA CCM v.30, CAS (Sanitisation) or ISO/IEC 27001 |

**Data importing and exporting**

| Data importing and exporting |
| --- |
|  |
| Data export approach | As outlined above - there is no lock-in since all data is held in the client's own accounts and not held by PUBLIC. |
| Data export formats | Other |
| Other data export formats | No need to export data as it resides Users' system |
| Data import formats | Other |
| Other data import formats | Users own the system to upload to |

**Data-in-transit protection**

| Data-in-transit protection |
| --- |
|  |
| Data protection between buyer and supplier networks | Other |
| Other protection between networks | Not applicable, the solution is run entirely within clients' own network |
| Data protection within supplier network | Other |
| Other protection within supplier network | Data protection requirements are responsibility of the client when writing their solution upon the infrastructure we provide. However all end-points within our stack are connected over SSL. All application resources are contained within private subnets and protected by minimum route tables. All processes run within their own security profiles and adhere to least responsibility principles. |

**Availability and resilience**

| Availability and resilience |
| --- |
|  |
| Guaranteed availability | We don't provide an SLA however the stack is designed to help provide maximum up-time requirements |
| Approach to resilience | All application tiers are multiple availability zones and can therefore withstand data centres becoming inoperable. All applications are deployed to auto-scaling clusters to provide resilience. All data storage is provided in clustered solutions. Management stage and production environments are in separate VPCs. All infrastructure is security hardened with no public IP access other than a single Bastion host which is protected VPN access. |
| Outage reporting | Full CloudWatch and alerting integration is provided. |

**Identity and authentication**

| Identity and authentication |
| --- |
|  |
| User authentication needed | No |
| Access restrictions in management interfaces and support channels | It should be noted that the components created by our solution are the responsibility of the client and can conform to whatever change management process they currently employ. |
| Access restriction testing frequency | Never |
| Management access authentication | Dedicated link (for example VPN) |

**Audit information for users**

| Audit information for users |
| --- |
|  |
| Access to user activity audit information | Users have access to real-time audit information |
| How long user audit data is stored for | User-defined |
| Access to supplier activity audit information | Users have access to real-time audit information |
| How long supplier audit data is stored for | User-defined |
| How long system logs are stored for | User-defined |

**Standards and certifications**

| Standards and certifications |
| --- |
|  |
| ISO/IEC 27001 certification | Yes |
| Who accredited the ISO/IEC 27001 | As per AWS Certification |
| ISO/IEC 27001 accreditation date | As per AWS Certification |
| What the ISO/IEC 27001 doesn’t cover | As per AWS Certification |
| ISO 28000:2007 certification | No |
| CSA STAR certification | No |
| PCI certification | No |
| Other security certifications | Yes |
| Any other security certifications | As per cloud provider |

**Security governance**

| Security governance |
| --- |
|  |
| Named board-level person responsible for service security | Yes |
| Security governance certified | No |
| Security governance approach | We are Cyber Essentials certified and while we are not ISO27001 certified we approach security incredibly seriously and we aim to work towards ISO27001 level information governance and security levels. |
| Information security policies and processes | As per Cloud Provider e.g. AWS security best practises AWS. |

**Operational security**

| Operational security |
| --- |
|  |
| Configuration and change management standard | Supplier-defined controls |
| Configuration and change management approach | It should be noted that the components created by our solution are the responsibility of the client and can conform to whatever change management process they currently employ. |
| Vulnerability management type | Supplier-defined controls |
| Vulnerability management approach | It should be noted that the components created by our solution are the responsibility of the client and can conform to whatever change management process they currently employ. |
| Protective monitoring type | Supplier-defined controls |
| Protective monitoring approach | It should be noted that the components created by our solution are the responsibility of the client and can conform to whatever change management process they currently employ. |
| Incident management type | Supplier-defined controls |
| Incident management approach | It should be noted that the components created by our solution are the responsibility of the client and can conform to whatever change management process they currently employ. |

**Secure development**

| Secure development |
| --- |
|  |
| Approach to secure software development best practice | Conforms to a recognised standard, but self-assessed |

**Public sector networks**

| Public sector networks |
| --- |
|  |
| Connection to public sector networks | No |

**Pricing**

| Pricing |
| --- |
|  |
| Price | $USD 10,000 per instance |
| Discount for educational organisations | Yes |
| Free trial available | Yes |