CAYMAN ISLANDS GOVERNMENT

**Request for Proposals**

**For**

**An E-Procurement Solution**

**Reference No.: EPC-CPO-001**

**Table of Contents**

## PART 1 - INVITATION AND SUBMISSION INSTRUCTIONS

1.1 Invitation to Bidders

This request is an invitation by the Cayman Islands Government ("CIG") to prospective bidders to submit bids for a procurement as further described in Section A of the Procurement Particulars (Appendix A) (the "Deliverables").

1.2 Procurement Contact

For the purposes of this procurement process, the "Procurement Contact" will be: Robert Tatum (procurement@gov.ky)

**Questions and clarification on this procurement must be submitted via email during the question period**. Bidders and their representatives are not permitted to contact any employees, officers, agents, elected or appointed officials or other representatives of CIG, other than the Procurement Contact or the Central Procurement Office, concerning matters regarding this procurement. Failure to adhere to this rule may result in the disqualification of the bidder and the rejection of the bidder's bid.

1.3 Type of Contract for Deliverables

The selected bidder(s) will be requested to enter into contract negotiations to finalize an agreement with CIG for the provision of the Deliverables. The Contractual Terms & Conditions (Appendix D) will form the basis for negotiations between CIG and the selected bidder.

1.4 Procurement Timetable

| | |
|---|---|
| Issue Date | December 18th 2024 |
| Deadline for Questions | January 15th 2025 at 5:00PM EST |
| Deadline for Issuing Answers to Questions | January 17th 2025 |
| Submission Deadline | January 22th 2025 at 5:00PM EST |
| Rectification Period | 5 Business Days |
| Anticipated Outcome Notification Date | February 21st 2025 |
| Contract Negotiation Period | 15 Business Days |
| Anticipated Execution of Agreement | March 14th 2025 |

The timetable is tentative only, and may be changed by CIG at any time. For greater clarity, business days means all days that CIG is open for business.

1.5 Submission of Bids

### 1.5.1 Bids to be Submitted at Prescribed Location

Bids must be submitted at: procurement@gov.ky.

### 1.5.2 Bids to be Submitted on Time

Bids must be submitted at the location set out above on or before the Submission Deadline. Bids submitted to a difference location or after the Submission Deadline will be rejected.

### 1.5.3 Bids to be Submitted in Prescribed Format

Where templates are provided, they must be completed in keeping with the instructions provided. Material modifications to templates may result in elimination. Unless specifically requested in Appendix A, the

content of websites or other external documents referred to in the bidder's submission but not attached will not be considered to form part of its submission.

### 1.5.4 Amendment of Bids

Bidders may amend their bids prior to the Submission Deadline by providing the amendments to the procurement contact.

### 1.5.5 Withdrawal of Bids

At any time throughout the process until the execution of a written agreement for provision of the Deliverables, a bidder may withdraw a submitted bid. To withdraw a bid, a notice of withdrawal must be sent to the Procurement Contact and must be signed by an authorized representative of the bidder. CIG is under no obligation to return withdrawn bids.

## PART 2 – RULES & PROCEDURES OF THE PROCUREMENT PROCESS (WITHOUT DIALOGUE)

The rules and procedures can be found here: https://www.procure.gov.ky/rules-procedures-procurement-without-dialougue

Please ensure that you read and understand these rules and procedure.

**APPENDIX A – PROCUREMENT PARTICULARS**

A. THE DELIVERABLES

## Minimum Required Feature Set

| Module | Required Functionality |
|---|---|
| **Document Development Module** | • Ability to add an unlimited number of "master templates"<br>• Ability to cascade changes from a master template to other areas that they have been assigned<br>• Ability to guide or provide guidance to users completing the templates to ensure high quality outputs<br>• Ability to leverage databases, open source data or historical inputs/data to aid in document completion |
| **Advertising, Bid Collection & Evaluation Module** | • Public facing portal that shows all current and past projects, including related attached documents<br>• Ability to communicate with vendors that have interacted with the project or that have asked a question<br>• Ability to collect submissions from vendors and control access to different parts of the submissions<br>• Ability to add submission reviewers and control their access to submissions<br>• Ability to set criteria and score against those<br>• Ability to produce reports that summarize the project and submission evaluation<br>• Ability to make contract award information publicly available |
| **Contract Management Module** | • Ability to add contracts to a database and give people access to them<br>• Ability for the system to remind users of contract expiry dates prior to expiration and other important contract elements<br>• Ability to track contract modifications<br>• Ability to communicate with contract users on updates |
| **System Administration & Monitoring** | • Multiple levels of permissions, from full administrative privileges to read-only<br>• Ability to assign users to departments or teams<br>• Ability to monitor all projects and contracts in the system<br>• Ability to see submission scoring history<br>• Ability to run reports on system activity, project timelines<br>• Appropriate user log-in security features such as 2-Factor Authentication |

B. IMPORTANT PROJECT DISCLOSURES

1. Potential suppliers must be able to supply all of the deliverables to be eligible for contract award. However, CIG reserves the right vary module selection and implementation times.

2. Vendors are encouraged to review the "Requested Information" related to this project and prepare their submissions in line with what is seen in that section. Failure to do this can result in difficulties making your final submission and the potential of missing the submission deadline.

3. All submissions must have an irrevocability period of ninety (90) days from the closing date of the opportunity.

4. For procurements seeking customer-facing technological solutions including software implementations, CIG aligns to the UK Government's Service Standard and Cloud-First Policy. Potential suppliers must acknowledge the standards and mandatory requirements outlined herein if submitting bids for a customer-facing technological solution.

C. MANDATORY REQUIREMENTS

Information requested in this section will be assessed on a **Pass/Fail basis.** If a submission fails to satisfy an **eligibility** requirement, the bidder will be issued a rectification notice identifying the deficiencies and providing the bidder an opportunity to rectify the deficiencies within a given period. **Rectification does not apply to technical requirements.**

| **Evaluation Group 1** | | |
|---|---|---|
| **Requested Information** | **Type of Requirement** | **Criteria for a Pass** |
| Submission Form (Appendix B) | Eligibility | Each submission must include a Submission Form completed and signed by an authorized representative of the bidder. |
| Business License | Eligibility | Submissions must include proof of a Cayman Islands Trade & Business License or a foreign equivalent that covers the provision of the deliverables. |
| Reference Form (Appendix E) | Eligibility | Submissions must include a Reference Form completed according to the instructions in the form. |
| Minimum Feature Set | Technical | Submissions must include be able to demonstrate that the proposed solution is able to provide all of the deliverables above listed as mandatory. |
| CIG eServices Standards (Appendix F) | Eligibility | Submissions must confirm compliance with CIG's eServices Standards for all customer-facing technological solutions. |

| | | |
|---|---|---|
| Vendor Privacy Notice | Eligibility | Submissions must include a copy of the Vendor's Privacy Statement. Where the Vendor will act as a Data Processor, as defined by the Cayman Islands Data Protection Act, this document must include:<br><br>1. Will the Vendor transfer personal data outside of the Cayman Islands in the course of providing the service? If yes, where (geographically) will the personal data be transferred, including for the purposes of storage and backups? If the CIG will have multiple options for data storage/processing locations, provide details of all options available through the Vendor for this specific procurement. If the Vendor engages any sub-processors that will transfer the personal data outside of the Cayman Islands, provide details of these sub-processors and any additional transfer locations.<br><br>2. Will the Vendor use personal data under the control of the CIG for its own purposes and therefore act as a Data Controller as defined by the Data Protection Act? If yes, detail all purpose(s) of processing these personal data where the Vendor is the Data Controller, e.g. analytics and machine learning to improve the service, end-user support, marketing communications, compliance with legal obligations to disclose data. |

D. RATED CRITERIA

The following sets out the information requested in order to rank submissions on a point system as per the criteria laid out below.

| **Requested Information** | **Description & Criteria Scoring System** | **Weight (out of 100%)** |
|---|---|---|
| **Evaluation Group 2** | | |
| Proposal, Demonstration and Value-Add | Each vendor will be required to submit their proposal, detailing their systems features in a written format. As a part of that submission, vendors should answer the following questions:<br><br>1. What processes are automated by your software?<br><br>2. What relationships or partnerships does your company have with other software publishers?<br>3. How does your firm maintain a competitive edge?<br>4. What your planned system upgrades within the next 2 years? | 40 |

| | | |
|---|---|---|
| | Each vendor will be required to present their system in a demonstration that proves that it includes the minimum feature set, and can show any additional features that the vendor considers value-adding.<br><br>Vendor are also asked to show what parts of their system as customizable or configurable to a customer's needs, from branding to specific reports and other technical elements.<br><br>The demonstration will require the vendor to show how they would produce this tender document in their system in the most efficient way.<br><br>Vendors must be prepared to give demonstrations within ten (10) business days of the submission deadline.<br><br>The final pricing must include all modules used in the demonstration to complete the task.<br><br>**Please do not include any pricing information in this document.**<br><br><u>Scoring System</u><br><br>5. **Excellent (9-10 Points)** – Submission demonstrates that the team, in combination with the proposed solution, can provide a level of service beyond expectations, stated requirements and business objectives. The Respondent is offering major enduring benefits in terms of reduced risk and/or a quantifiable value add to the Entity.<br><br>6. **Good (7 – 8 Points)** - Submission demonstrates that the team, in combination with the proposed solution, are able to meet the requirement and business objectives. Adds some major areas of benefit to the Entity with little or no risk and/or increased costs.<br><br>7. **Acceptable (5 - 6 Points)** - Submission demonstrates that the team, in combination with the proposed solution, are able to meet the requirement and business objectives. Adds some minor areas of benefit to the Entity with some risk and/or increased cost.<br><br>Any submissions scoring below "Acceptable" will not be further considered.<br><br>8. **Serious Concerns (3 - 4 Points)** - Submission demonstrates an inability to meet the requirements or business objectives, would require considerable guidance or includes risks that are un-mitigatable.<br><br>9. **Unacceptable (0 – 2 Points)** - Submission does not offer an explanation or ability to meet the Ministry's requirements and business objectives. | |
| Implementation Plan | Each vendor must provide a plan, including a schedule, that shows how long it would take to implement their system, including any new modules that would be required to meet the minimum requirements.<br><br><u>Scoring System</u> | 10 |

| | | |
|---|---|---|
| | 1. **Excellent (9-10 Points)** – Submission demonstrates that the team, in combination with the proposed solution, can provide a level of service beyond expectations, stated requirements and business objectives. The Respondent is offering major enduring benefits in terms of reduced risk and/or a quantifiable value add to the Entity.<br><br>2. **Good (7 – 8 Points)** - Submission demonstrates that the team, in combination with the proposed solution, are able to meet the requirement and business objectives. Adds some major areas of benefit to the Entity with little or no risk and/or increased costs.<br><br>3. **Acceptable (5 - 6 Points)** - Submission demonstrates that the team, in combination with the proposed solution, are able to meet the requirement and business objectives. Adds some minor areas of benefit to the Entity with some risk and/or increased cost.<br><br>Any submissions scoring below "Acceptable" will not be further considered.<br><br>4. **Serious Concerns (3 - 4 Points)** - Submission demonstrates an inability to meet the requirements or business objectives, would require considerable guidance or includes risks that are un-mitigatable.<br><br>5. **Unacceptable (0 – 2 Points)** - Submission does not offer an explanation or ability to meet the Ministry's requirements and business objectives. | |
| Support | Each vendor must provide a support plan that demonstrates how they intend to provide support for their system including initial training, on-going support and self-service options.<br><br><u>Scoring System</u><br><br>1. **Excellent (9-10 Points)** – Submission demonstrates that the team, in combination with the proposed solution, can provide a level of service beyond expectations, stated requirements and business objectives. The Respondent is offering major enduring benefits in terms of reduced risk and/or a quantifiable value add to the Entity.<br><br>2. **Good (7 – 8 Points)** - Submission demonstrates that the team, in combination with the proposed solution, are able to meet the requirement and business objectives. Adds some major areas of benefit to the Entity with little or no risk and/or increased costs.<br><br>3. **Acceptable (5 - 6 Points)** - Submission demonstrates that the team, in combination with the proposed solution, are able to meet the requirement and business objectives. Adds some minor areas of benefit to the Entity with some risk and/or increased cost.<br><br>Any submissions scoring below "Acceptable" will not be further considered.<br><br>4. **Serious Concerns (3 - 4 Points)** - Submission demonstrates an inability to meet the requirements or business objectives, would require considerable guidance or includes risks that are un-mitigatable. | 10 |

| | | |
|---|---|---|
| | 5. **Unacceptable (0 – 2 Points)** - Submission does not offer an explanation or ability to meet the Ministry's requirements and business objectives. | |
| **Evaluation Group 3** | | |
| Pricing Form (Appendix C) | Each submission must include a Pricing Form (Appendix C) completed according to the instructions in the form.<br><br>Pricing will be requested **after** the evaluation of groups 1 and 2 is completed. Please **do not** include pricing in the initial submission required by the submission deadline but please have it ready to provide within 2 business days of notice following your demonstration.<br><br><u>Scoring System</u><br><br>See Appendix C | 40 |
| | Total | 100 |

E. PRE-CONDITIONS OF CONTRACT AWARD

The following sets out the information that will need to be **provided by the successful bidder only.** This information is provided so that all potential bidders can account for these requirements in their pricing submissions. The items listed in the table **DO NOT** need to be provided until a bidder receives a letter of intent to award.

| Pre-Condition of Award | Criteria for a Acceptance |
|---|---|
| Declarations | A declaration that the bidder (and its proposed subcontractors) are not subject to any winding up proceedings and is not aware of any ongoing or impending litigation being brought against it that may materially impact its ability to deliver the proposed solution or commitments in this submission. |
| Cayman Islands Government Security Assurance Attestation Questionnaire | Questionnaire must be completed and agreed with the procuring entity. Questionnaire is included as Appendix G. |
| Cyber Liability Insurance | USD$5,000,000 Per Occurrence |
| Data Protection Compliance | Agree to either:<br><br>1. Hosting of the E-Procurement System in the UK or European Jurisdiction or; |

| | |
|---|---|
| | 2. Signing of Data Transfer Agreements based on Standard Contractual Clauses published by the Ombudsman of the Cayman Islands |

## APPENDIX B – SUBMISSION FORM

### 1. Bidder Information

| Please fill out the following form, naming one person to be the bidder's contact for the process and for any clarifications or communication that might be necessary. | |
|---|---|
| Full Legal Name Under which Bidder Carries on Business: | |
| Street Address: | |
| City, Country/Province/State: | |
| Postal Code: | |
| Phone Number: | |
| Company Website (if any): | |
| Bidder Contact Name and Title: | |
| Bidder Contact Phone: | |
| Bidder Contact Email: | |

### 2. Acknowledgment of Procedures & Rules of Procurement Process

The bidder acknowledges that they have reviewed, fully understand and will be governed by the procedures and rules of the procurement process seen in Part 2. The bidder declares that it has not engaged in any conduct prohibited by this procurement. Among other things, such rules and procedures confirm that this procurement process does not constitute a formal, legally binding bidding process and does not give rise to a contract, and that no legal relationship or obligation regarding the procurement of any good or service will be created between CIG and the bidder unless and until CIG and the bidder execute a written agreement for the Deliverables.

### 3. Addenda

The bidder is deemed to have read and taken into account all addenda issued by CIG prior to the Deadline for Issuing Addenda.

### 4. Conflict of Interest

For the purposes of this procurement, the term "Conflict of Interest" includes, but is not limited to, any situation or circumstance where:

(a) in relation to the procurement process, the bidder has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to (i) having, or having access to, confidential information of CIG in the preparation of its bid that is not available to other bidders, (ii) communicating with any person with a view to influencing preferred treatment in the procurement process (including but not limited to the lobbying of decision makers involved in the procurement process), or (iii) engaging in conduct that compromises, or could be seen to compromise, the integrity of the open and competitive procurement process or render that process non-competitive or unfair; or

(b) in relation to the performance of its contractual obligations under a contract for the Deliverables, the bidder's other commitments, relationships or financial interests (i) could, or could be seen to, exercise an improper influence over the objective, unbiased and impartial exercise of its independent judgement, or (ii) could, or could be seen to, compromise, impair or be incompatible with the effective performance of its contractual obligations.

For the purposes of section (a)(i) above, bidders should disclose the names and all pertinent details of all individuals (employees, advisers, or individuals acting in any other capacity) who (a) participated in the preparation of the bid; **AND** (b) were employees of CIG within twelve (12) months prior to the Submission Deadline.

| Name(s) of Individual Involved in Bid Preparation | Previous Position/Capacity within CIG |
|---|---|
| | |

If the box below is left blank, the bidder will be deemed to declare that (a) there was no Conflict of Interest in preparing its bid; and (b) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the procurement. Otherwise, if the statement below applies, check the box.

- The bidder declares that there is an actual or potential Conflict of Interest relating to the preparation of its bid, and/or the bidder foresees an actual or potential Conflict of Interest in performing the contractual obligations if they are awarded the contract. Details are provided below:

**5. Disclosure of Information**

The bidder hereby acknowledges that any information provided in this bid, even if it is identified as being supplied in confidence, is subject to the provisions of the Freedom of Information Law (2015 Revision), and may be disclosed where required by law or by order of a court. The bidder hereby consents to the disclosure, on a confidential basis, of this bid by CIG to the advisers retained by CIG to advise or assist with the procurement process, including with respect to the evaluation this bid.

Signature of Bidder Representative

Name of Bidder Representative

Title of Bidder Representative

Date

I have the authority to bind the bidder.

## APPENDIX C – PRICING FORM

### 1. Instructions on How to Complete Pricing Form

(a) Rates must be provided in Caymanian Dollars (KYD). Please note that when converting from US Dollars to Cayman Islands Dollars, bidders shall use a conversion rate of $1 USD = $0.8375 KYD.

(b) Rates quoted by the bidder must be all-inclusive and must include all bonding costs, all labour and material costs, all travel and carriage costs, all insurance costs, all costs of delivery, all costs of installation and set-up, including any pre-delivery inspection charges, and all other overhead, including any fees or other charges required by law.

(c) Pricing should be exclusive of duties levied by Customs & Border Control. A duty waiver will be provided.

### 2. Evaluation of Pricing

The pricing of bidders that have not met the mandatory or minimum criteria laid out in Appendix A will not be included in the pricing evaluation. *The value of the "total pricing points" can be found in the rated criteria section in Appendix A.*

**Pricing will be evaluated with the following formula:**

*(lowest price ÷ bidder' s price) × total pricing points = bidder' s pricing points*

### 3. Pricing Form

| Pricing Component | Pricing Structure | (A) Number of Years | (B) Annual Price | (AxB) Total Price (KYD$) |
|---|---|---|---|---|
| Implementation | One-Time Cost | N/A | N/A | $ |
| Document Development Module | Annual Licence | 3 | $ | $ |
| Advertising, Bid Collection & Evaluation Module | Annual Licence | 3 | $ | $ |
| Contract Management Module | Annual Licence | 3 | $ | $ |
| | | | **Sub-total** | $ |
| | | | **Discount (%)** | |
| | | | **Total:** | **$** |

## APPENDIX D – CONTRACTUAL TERMS & CONDITIONS

The contractual terms & conditions found here:

- **Contract for Services**

This will form the basis of any eventual Agreement between the CIG and the Successful Bidder. Although the final wording of the provisions may be subject to limited negotiation, bidders should be prepared to enter into an agreement with minimal changes. Below are key contract considerations related to this project. Vendors should include any objections to the below terms as a part of their submission for consideration.

| Key Contract Elements | Details |
|---|---|
| Expected Execution Date | See "Procurement Timetable". |
| Expected Initial Contract Length | |
| Contract Extension Clause | |
| Goods Delivery Location | |
| Payment Terms | **Goods:** Payment upon on delivery and acceptance<br><br>**Services:** Upon Completion of Agreed Project Milestones<br><br>**Days from Invoicing by Supplier to Payment:** 30 Days |
| Period for which Insurance must remain in force | During the term of this Agreement and for a period of six years thereafter. |
| Termination by Customer | Allowed with three months' written notice |
| Material Breach Termination by Either Party | Allowed with immediate effect if a material breach occurs that is irremediable or if such breach is remediable, is not remedied within 30 Days of written notice. |
| Force Majeure | If the period of delay or non-performance continues for [#] [weeks OR months], the party not affected may terminate this Agreement by giving [#] [days'] written notice to the affected party. |

## APPENDIX E – REFERENCE FORM

Each bidder is required to provide three (3) references from three (3) different companies who procured similar goods and services from the bidder in the last 5 years. References will only be counted as valid if the work for that reference was undertaken by a member of the project team assigned to this procurement. The contact person must agree to be listed prior to submission for the reference to be counted as valid. The CIG reserves the right to contact any or all references.

**Reference #1**

| | |
|---|---|
| Company Name: | |
| Company Address: | |
| Contact Name: | |
| Contact Telephone Number: | |
| Contact E-mail: | |
| Date Work Undertaken: | |
| Project Team Member Assigned: | |
| Nature of Assignment: | |

**Reference #2**

| | |
|---|---|
| Company Name: | |
| Company Address: | |
| Contact Name: | |
| Contact Telephone Number: | |
| Contact E-mail: | |
| Date Work Undertaken: | |
| Project Team Member Assigned: | |
| Nature of Assignment: | |

**Reference #3**

| | |
|---|---|
| Company Name: | |
| Company Address: | |
| Contact Name: | |
| Contact Telephone Number: | |
| Contact E-mail: | |
| Date Work Undertaken: | |
| Project Team Member Assigned: | |
| Nature of Assignment: | |

## APPENDIX F – CIG ESERVICES STANDARDS

Each bidder is required to provide submissions evidencing how the proposed solution will meet the requirements detailed below. Bidders are not permitted to alter the standards or technical requirements.

| # | eService Standard | Requirement(s) |
|---|---|---|
| **1** | Understand users and their needs | a. CIG is required to balance the optimal mix of functional and non-functional requirements, with the minimum financial outlay over the period that the eService is intended to be delivered. State how your submission is likely to achieve this balance.<br>b. Where CIG does not have access to a business analyst resource, the proponent should participate in refining the business requirements. |
| **2** | Solve a **whole** problem for users | a. The solution will be structured and present services as they are viewed by CIG's customers, at the time that the customers need them, rather than structuring services based on CIG internal processes and operations. |
| **3** | Provide a joined up experience across all appropriate CIG channels | a. Deliver a solution that is responsive on web and mobile devices.<br>b. Functionality available on web and/or desktop should be equally accessible on mobile devices. |
| **4** | Make the eService simple to use | a. Support modern authentication standards, and in particular leverage convenient biometric authentication (FaceID facial or fingerprint identification) when delivered on mobile devices.<br>b. Deliver a solution that meets UI/UX best practices and standards such as ISO 9241 or similar. |
| **5** | Make sure everyone can use the eService | a. For web-based services, adhere to the latest version of Web Content Accessibility Guidelines.<br>b. Deliver a solution that considers multiple user journeys, catering to the varying demographics of the Cayman Islands population. |
| **6** | Have a multidisciplinary team | a. Support CIG by providing access to a primary point of contact during the course of the project.<br>b. Support CIG by providing access to a business and/or data analytical resource to support requirements and design phases.<br>c. Support CIG by providing access to necessary technical experts with experience in delivering the desired solution. |
| **7** | Use agile ways of working | a. Institute a project methodology that supports gathering sufficient requirements upfront while remaining agile to respond to change in requirements or user feedback once within the project scope.<br>b. Provide adequate documentation of configurations and/or customisations made to the solution to meet CIG's requirements.<br>c. Provide regular progress updates that are visible and easily accessed by CIG stakeholders. |
| **8** | Iterate and improve frequently | a. Offer frequent evolutions that track changes in the applicable industry segment,<br>b. Provide consultation on the prioritisation tasks so that maximum value is delivered with each iteration.<br>c. Disclose to CIG any intentional technical debt incurred by development changes. |

| # | eService Standard | Requirement(s) |
|---|---|---|
| **9** | Create a secure eService which protects users' privacy | a. Adhere to current security policies as published by the office of the CISO, and/or the NIST Cybersecurity Framework.<br>b. For cloud-based services, align with Cloud Security Guidelines issued by the UK government's National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/collection/cloud-security).<br>c. Comply with the principles of the Cayman Islands Data Protection legislation.<br>d. Comply with GDPR, particularly the right to erasure of personal data.<br>e. Ensure that CIG remains the controller of all personal and private customer data. There must be a clear definition of which party owns the data within the service.<br>f. Permit repatriation of data at end-of-contract.<br>g. Comply with any findings or requirements of an applicable Data Privacy Impact Assessment issued by CIG. |
| **10** | Define what success looks like and publish performance data | a. Solutions must provide access to performance data and/or reports.<br>b. Solutions must be implemented with adequate key performance indicators that can be easily measured throughout the course of the project. |
| **11** | Choose the right tools and technology | a. CIG's preference is for capturing and managing data as opposed to documents. Where documents are necessary, the records management component must interact and store records with an API for an existing CIG records management platform.<br>b. Comply with a cloud-first philosophy: if the proposed solution is not in the public cloud, justification must be provided if the lifetime cost exceeds that of the proposed on-premises solution.<br>c. If the proposed solution is on premise, it must be hosted on existing CIG infrastructure.<br>d. Tools and technologies proposed must meet the technical requirements defined in eService Standard #13. |
| **12** | Make new source code open and comprehensible | For any bespoke software development for CIG:<br>a. Proposed project team must adhere to best coding practices including adequate and comprehensible developer comments within the source code.<br>b. Source code updates is to be provided to CIG as they occur.<br>c. Source code must be stored in a shared source code repository that CIG and the successful proponent have access to. |
| **13** | Use and contribute to open standards, common components and patterns | a. Solutions will be developed first within a development ("dev") environment. Once adequately tested, changes should be progressed to a UAT environment for CIG testing, feedback and approval before promotion to a live/production environment.<br>b. For internal CIG user access and authentication, the solution will need to integrate with Microsoft Active Directory and/or Oracle OID.<br>c. For external user access and authentication, the solution must be compatible with federation standards such as SAML 2.0 (or later), OpenID Connect, or OAuth.<br>d. Ensure interoperability by leveraging SOAP/XML web services that are compatible with the eGOV Connect solution (i.e. conform to X-Road message protocol v4.0 or later). |
| **14** | Operate a reliable eService | a. Solutions should be deployed on a high-availability network infrastructure, to be agreed by CIG and the successful proponent. |

**APPENDIX G - CAYMAN ISLANDS GOVERNMENT SECURITY ASSURANCE QUESTIONNAIRE FOR THIRD-PARTY HOSTING SERVICE PROVIDER**

| DATA AND SECURITY ASSURANCES | (Service Provider) RESPONSE |
|---|---|
| 1. The Service Provider must only store and otherwise process any personal data that have been disclosed to the Service Provider by the Cayman Islands Government in a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Cayman Islands Government shall be the only person with authority to determine whether a specific jurisdiction provides adequate protection. If the Service Provider must, as a condition of providing its services, transfer personal data disclosed by the Cayman Islands Government to a jurisdiction that does not provide such adequate protection, the Cayman Islands Government must first confirm there is a relevant exemption from or exception to the Eighth Data Protection Principle and explicitly authorise the specific transfer. | |
| 2. Any and all disclosures, to any third parties (including unauthorised disclosures), of Sensitive or personal data (as defined under the Cayman Islands Data Protection Act) or any other data deemed by the Cayman Islands Government to be confidential, must be recorded and notified to the Cayman Islands Government authorised contact as per the contract/agreement. The notification must include specific information on the nature of the data and extent of the disclosure, to whom and at what date and time. The Service Provider, as a Data Processor, will bear the responsibility for providing notifications of disclosure related to their Sub-Processors. | |
| 3. The Service Provider should inform the Cayman Islands Government, at least 20 (twenty) business days in advance, of any intended material changes to the agreements (whether contractual or otherwise) that have the potential to impact Data Governance or Ownership Structure, such as a change to their data center hosting location/jurisdiction, mergers, acquisition, buy-out and the like, so that the Cayman Islands Government has the ability to object to such changes or to terminate the contract. | |
| 4. The Service Provider must promptly notify the Cayman Islands Government in the event of a breach of security and/or a personal data breach (as defined in the Cayman Islands Data Protection Act) related to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or, access to, personal data transmitted, stored or otherwise processed by the Service Provider. The Service Provider must notify the Cayman Islands Government's authorised contact as per the contract/agreement, of any such security and/or personal data breach within no more than 24 hours of becoming aware of it. | |
| 5. In the event of an actual or suspected personal data breach, the Service Provider must maintain a record with a description of the incident, the nature of the breach (including a description of the personal data that were compromised, if any), the time | |

| | | |
|---|---|---|
| | period, the consequences of the incident, the name of the reporter (if known), to whom the incident was reported, and the steps taken to resolve the incident (including the person in charge and the data recovered, if relevant). | |
| 6. | In the event of an actual data breach involving Sensitive and personal data, the record should also include a description of the exact data records which have been compromised, if known; and if any notifications were performed, the Service Provider must notify the Cayman Islands Government, the Data Controller, within no more than 24 hours. | |
| 7. | The Service Provider must retain historic copies of the various policies 'As Was' versions of their security policies and operating procedures, going back for a minimum period of up to 7 years. The Service Provider must make the historic policies and operating procedures available to the Cayman Islands Government upon request, within no later than 5 days. The reason for this, is that a review of current and historical policies and procedures can be required by the Cayman Islands Government for sharing with a third-party, e.g. in the cases of customer dispute resolution and investigation by a Local Supervisory Authority and or other International Supervisory Authority or Agency. | |
| 8. | The Service Provider must have a policy in respect of the return, transfer and/or permanent disposal of any and all of the data, across any and all of the Service Providers (or their sub-processors) assets (including but not limited to production environment, support environments, backups and their disaster recovery / business continuity environments). The Service Provider must make the policy available to the Cayman Islands Government upon request, within no later than 5 days. The Service Providers must provide written attestation, in respect of the above being carried out, and the attestation will be legally relied upon by the Cayman Islands Government. | |
| 9. | At the termination of the contract or agreement, the Cayman Islands Government has the right to request for any and all data to be transferred to another Cloud Service Provider. Alternatively, the Cayman Islands Government may request that any and all data processed by the Service Provider be securely deleted or otherwise destroyed or anonymised. | |
| 10. | Persons or entities under the Service Provider's control (including but not limited, to employees, agents or sub-contractors), who have access to the Cayman Islands Government's data or assets storing the Cayman Islands Government's data, should be subject to appropriate/regular vetting, non-disclosure and confidentiality obligation, as part of the relevant contract or agreement. The obligations of the non-disclosure and confidentiality agreement must survive termination of any relevant contract. | |
| 11. | The Service Provider must implement stringent measures and controls to guarantee that their employees or sub-contractors cannot copy any Cayman Islands Government's data onto portable physical media or other devices/media which can be used for the purpose of exfiltrating the Cayman Islands Government's data. | |

| | |
|---|---|
| 12. The Service Provider must maintain up-to-date record of employees, agents and sub-contractors who have authorised access to the information system(s) storing Cayman Islands Government's data. | |
| 13. The Service Provider must have protocols and procedures in place to provide employees, agents and sub-contractors of the Cayman Islands Government with access to the facility should this be required. | |
| 14. The Service Provider must have measures in place to de-activated or disable access privileges to physical premises and information systems. | |
| 15. The Service Provider must implement security measures to ensure that the any and all Cayman Islands Government's data, whilst stored or transmitted across the Service Provider's infrastructure or across the internet, is encrypted end-to-end and always kept secure from unauthorised access. | |
| 16. The Service Provider must implement appropriate security measures, controls and systems to maintain the security of the service provided to the Cayman Islands Government – this includes the capability to identify, detect and prevent a range of cyber security threats, such as unauthorised access, insider threats, ransomware, data theft, denial of services and the like. | |
| 17. The Service Provider must have information security incident management procedures in place, which shall include detection, containment, eradication and recovery and these must be tested on a regular basis. | |
| 18. The Service Provider must have business continuity and disaster recovery plans in place to meet the agreed contractual service levels and these plans must be tested on a regular basis. | |
| 19. The Service Provider facility must be either Tier 3 or Tier 4 rated standard. | |
| 20. The Service Provider must achieve (or have plans in place to achieve) at least one international recognized accreditation / certification, such as SOC 2 compliance, ISO27001 certification. | |
| 21. The Service Provider to advise whether they or their sub-processors, have ever suffered a cyber-attack or data compromise. | |
| 22. The Service Provider to advise whether they have a valid Professional Liability Insurance in place and if so, please can you provide details of the Policy Schedule. | |
| 23. The Service Provider to advise whether they have a valid Cyber Security Insurance in place and if so, please can you provide details of the Policy Schedule. | |

END OF DOCUMENT