|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ECOS Procedure Checklist for Cloud Solution Solicitations and Contracts | | | | |
| Step | Assigned to *(see footer Note 1)* | Where to obtain | Submit to | Supplier proposal action |
| SOLICITATIONS | | | | |
| Obtain Cloud Services Terms and Conditions (agency may not alter these except for adding agency name/acronym) | Procurement lead | [scminfo@vita.virginia.gov](mailto:scminfo@vita.virginia.gov), or [enterpriseservices@vita.virginia.gov](mailto:enterpriseservices@vita.virginia.gov) | NA, include in RFP | Submit any redlines in the document with proposal; must redline the actual document for context review by VITA SCM and Director, ECOS |
| Obtain ECOS Assessment Form | Procurement lead, business owner/project manager | <https://vccc.vita.virginia.gov/vita>  Search ECOS Assessment or search Service Catalog for Cloud Service Assessment, Click Show More, and scroll down to Attachment for 1-003 to access Appendix A, the Security Assessment Form. | NA, include form in RFP | Submit complete and accurate responses with proposal; notify agency of any proprietary responses; this is not evaluated |
| RFP Language | Procurement lead | Add to the end of the Evaluation section of the RFP; but do not add to the Evaluation Criteria list:  If this is a cloud-based procurement (i.e., off-premise hosting), the following will be required: (your agency name) will select the proposal(s) representing the best value to the Commonwealth. Suppliers whose proposals are selected must successfully answer, negotiate, and/or comply with any resulting security exceptions that may arise in order to approve the Supplier’s ECOS Assessment and cloud proposal for further evaluation. Supplier’s failure to do so may result in removal from further consideration. Refer to Appendix X, ECOS Assessment Form, of the RFP.  Add to the Requirements section of the RFP:  If this RFP includes requirements for cloud services (Software as a Service, Platform as a Service or Infrastructure as a Service), in order to be awarded a contract an assessment will have to be conducted by VITA ECOS based on Supplier’s responses to Appendix X of the RFP, ECOS Assessment Form. Supplier should ensure that when submitting its proposal it has provided sufficient and complete responses to reduce the need for additional information.  NOTE: see additional recommended questions immediately below this table to include in the RFP’s Requirements section. | NA, include in RFP. But remember the ECOS Assessment is not evaluated and need not be disclosed to the entire evaluation team, as supplier responses are proprietary/confidential. |  |
| CONTRACTS | | | | |
| ECOS Assessment Form (never include the supplier’s completed version in the contract) | AITR, business owner/project manager/ISO | From supplier’s proposal; each assessment costs agency a flat fee of $1,992.57 so agency will submit the top contender’s ECOS Assessment first | <https://vccc.vita.virginia.gov/>vita  Search *ECOS Assessment* or search *Service Catalog* *for Cloud Service Assessment*, Click *Show More*, scroll down to attach the supplier completed Assessment from the supplier’s proposal. | Supplier may ask agency to sign an NDA or ask VITA to sign one.  ECOS may ask supplier to submit further details or information. |
| ECOS Assessment Approval (never include in the contract, cannot be publicly disclosed) | VITA ECOS, Enterprise Services | From agency AITR, business owner/project manager/ISO | Agency AITR, business owner/project manager/ISO (from the agency role who submitted); submits by email.  Resulting Security Exceptions are never included in the Contract. Resulting Contractual Requirements must be included in the Cloud Terms. | Supplier may have to accept any security exceptions required by ECOS |
| ECOS Assessment approval email notification | AITR, business owner/project manager/ISO | VITA ECOS, Enterprise Services | Agency has 5 days from receipt of VITA’s Assessment approval email to:   * submit any required security exceptions to VITA CSRM * provide any contractual requirements to the agency procurement lead to add to Supplier Responsibilities section of the cloud terms * submit the service request | NA unless to collaborate with agency ISO regarding the security exceptions |
| ECOS Service Request (for SCM Services and ECOS Oversight Service Implementation) | AITR, business owner/project manager/ISO | Go to ServiceNow portal:  <https://vccc.vita.virginia.gov/>vita  Search ECOS Oversight and Select  Cloud Sourcing Specialist for Cloud terms review (FY22 Rate: $123.83 Hourly)  or Cloud Service Oversight (Monthly) for monthly oversight to begin after contract award (Rate: FY 22 Rate: $478.43 Monthly)  Scroll down and complete the relevant form  Hit “Order Now” on right menu. | <https://vccc.vita.virginia.gov/>vita | NA |
| Cloud Services Terms and Conditions (with supplier redlines) | Procurement lead | From supplier’s proposal | Submit supplier redlined version for review to: [sonja.headley@vita.virginia.gov](mailto:sonja.headley@vita.virginia.gov) or [*scminfo@vita.virginia.gov*](mailto:scminfo@vita.virginia.gov)  SCM consultant and ECOS Lead will review and assist in agency negotiations | NA |
| Exceptions to the ECOS Assessment Approval | VITA ECOS, Enterprise Services | From review of the ECOS Assessment responses | To agency AITR/business owner/project manager/ISO who sent the ECOS Assessment to VITA | NA |
| Exception Approval Request | AITR/business owner/project manager/ISO | <https://www.vita.virginia.gov/policy--governance/itrm-policies-standards/>  under Tools and Templates section, 4th bullet | Submit through ARCHER | NA |
| RENEWALS | | | | |
| For existing cloud/SaaS contracts | Procurement Lead/ISO/ project manager/AITR | Confirm with [enterprise.services@vita.virginia.gov](mailto:enterprise.services@vita.virginia.gov) that the supplier/SaaS application is in Active Oversight at the FY 22 rate of $478.43 Monthly. | ECOS Assessments are good for 12 months from the date approved by ECOS unless the supplier/SaaS application goes into Active Oversight within those 12 months via the agency-submitted service request. The ECOS Assessment remains good as long as they are in Active Oversight.  If the supplier/SaaS application is not in Active Oversight, a new ECOS Assessment must be done via the agency-submitted service request. See instructions above.    Once the ECOS Assessment is approved, the agency may also submit a service request for obtaining Active Oversight by ECOS. See instructions above.  If the supplier/SaaS application was approved by the old CIO Exception process prior to ECOS implementation in December 2016, the agency will need to have the supplier complete an ECOS Assessment and agency must submit to ECOS for approval per the email address in the next column. Also, the old SaaS terms will either need to be (1) entirely replaced via contract modification with the current version of Additional Cloud Services Terms and Conditions; or (2) modified to add specific sections of the current version. These may be obtained by request to: [Sonja.headley@vita.virginia.gov](mailto:Sonja.headley@vita.virginia.gov) or [SCMinfo@vita.virginia.gov](mailto:SCMinfo@vita.virginia.gov)  Once the ECOS Assessment is approved, the agency may also submit a work request 1-004 for obtaining Active Oversight by ECOS. This form is also available at the link above. | NA |
| *Note: It is very important that the agency Procurement Lead, ISO and Project Manager read, understand and comply with the final negotiated Cloud Services Terms and Conditions, whether from a VITA Statewide contract or the agency’s own SaaS contract as there are agency obligations to be complied with to avoid any breach situation and to perpetrate knowledge share with all agency Application Users.* | | | | |

The following questions can be added to the Requirements section of the RFP to better understand supplier business maturity and their solution offering:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Requirements | **A** | **B** |
|  | Is the cloud solution you are proposing a Software as a Service, Platform as a Service or Infrastructure as a Service delivery model? Please describe.  Are you offering public, private, government cloud or a hybrid cloud model? Please describe available models and ensure your pricing includes your offered options.  Also, please describe if your solution allows for onsite hosting. Explain the pros and cons of offsite and onsite hosting that your solution offers. |  |  |
|  | Is the cloud solution you are proposing FedRamp authorized? If yes, please provide a description of your authorization. |  |  |
|  | Does your firm follow and incorporate security and privacy recommendations and best practices from the National Institute Standards and Technology (NIST)? If yes, please describe. |  |  |
|  | Does your cloud solution rely on third-party partners or subcontractors? If yes please describe fully. |  |  |
|  | Have your appropriate staff read the commonwealth’s security policies, standards and guidelines, applicable to your proposed solution, located at the following URL?  <https://www.vita.virginia.gov/it-governance/itrm-policies-standards/>  Please state yes or no. Please explain the top 5 concerns you identify, if any. |  |  |
|  | Does your cloud solution allow a customer to solely manage their own encryption keys or must that function remain with solution provider? Please explain. |  |  |

## Performance Standards Methodology

Please describe the methodology used to develop your firm’s internal performance standards, the processes and tools used to monitor and measure performance against those standards, and the management reporting systems that capture these data.

Indicate your firm’s present customer satisfaction rating, summarize customer satisfaction criteria, and describe the methodology used to measure customer satisfaction. Please include any relevant publication ratings or articles.

## Governance and Compliance Management

Please describe your firm’s management processes that ensure governance and compliance with all federally mandated laws and regulations used by your industry and in provision of your services to your customers. Also, describe how you will provide governance and compliance with any of VITA’s or (your agency name’s) required security and data privacy or other requirements specified in the RFP, not currently managed by your firm, but that you will be willing to do should an award be made to your firm.

## Security Risk Management Overview

Please provide an overview of your firm’s comprehensive security risk management processes including your application, monitoring and management of the controls used. Provide details as to how you establish the context for security risk-based decisions, how you assess the risk, how your respond to the risk once it’s determined, and how you monitor the risk on an ongoing basis using communications and feedback for continuous improvement within your organization.

## Disaster Recovery/Security Plan

Describe in detail your firm’s plans to mitigate against any disaster that would affect the ability to provide (your agency name) with the proposed solution. Provide a detailed plan of your firm’s security infrastructure including facility and information technology security. Provide your firm’s plans of action for the following security incidents, as applicable to the RFP:

* Interruption of service including denial of service attacks
* Vulnerability incidents
* Data loss or compromise
* Insider attacks