Annex A – Terms of Reference

TERMS OF REFERENCE (TOR) FOR CONSULTANCY SERVICES FOR THE SYSTEMS DEVELOPMENT OF WEBSITE PORTAL FOR ONBOARDING PROCESS OF APPLYING RELYING PARTY ON PHILSYS API-ENABLED SERVICES

1. Project Background and Rationale

The Philippine Identification Systems Act or RA 11055 mandates the Philippine Statistics Authority (PSA) to be the implementing agency for the national ID system or PhilSys. PhilSys is envisioned to make services accessible, promote ease of doing business, enhance integrity of services and reduce fraud, promote participation and trust in digital government and economy, as well as provide Filipinos with greater control over their personal data.

To democratize access to PhilSys services, the PSA intends to partner with private enterprises to act as Relying Parties (RPs) for authentication services. RPs shall go through an onboarding process before they will be granted permission or authority to offer such services to the general public. The PSA shall provide subscription tiers for the different services that RPs could offer. On onboarding, the PSA shall provide RPs a Letter of RP Accreditation and a Subscription Contract.

RPs will not have a direct access to PhilSys services but will course their traffic through PSA-accredited trusted service providers (TSPs). The onboarding process and the onboarding portal will be managed by the Use Case Development Management Service (UCDMS).

2. Project Objectives

2.1. To facilitate this onboarding process, PSA shall launch an onboarding portal to provide:
- 2.1.1. the latest news and information related to
  - 2.1.1.1. the different subscription tiers;
  - 2.1.1.2. the onboarding process for each subscription tier;
- 2.1.2. RPs online access
  - 2.1.2.1. to create and manage their accounts, submit requirements, and follow-up on the onboarding process;
  - 2.1.2.2. view and download their subscription contract;
  - 2.1.2.3. renew or change subscription tier;
- 2.1.3. PSA/UCDMS online access to
  - 2.1.3.1. administer and manage the portal;
  - 2.1.3.2. manage the onboarding process of an RP;
  - 2.1.3.3. manage the renewal or changes in subscription tiers of RPs.

2.2. The portal shall also be designed for easy integration with other PSA systems such as the PhilSys backend and those of TSPs.

3. Scope of Work

3.1. The project seeks to engage a contractor to provide one (1) lot of supply and delivery of services and goods for the development, testing, installation and implementation, configuration, maintenance and support for the Onboarding Portal for Relying Parties.

3.2. The engagement shall require the contractor to provide:

3.2.1. services including project management, business analysis, development, testing, data management, installation or deployment in testing and staging environments, training, and maintenance;
3.2.2. online collaboration tools for project management with Kanban or Scrum capability, document sharing, and code repositories;
3.2.3. the local development environment;
3.2.4. test scenarios, test cases, and test data;
3.2.5. the source and production code, test scripts and deployment scripts;
3.2.6. one (1) year subscription to third-party tools such as analytics, cybersecurity, and other libraries or tools;
3.2.7. thirty (30) analytics reports or templates;
3.2.8. soft and hard copies of documentation including but not limited to project management, business requirements, system requirements specifications, wireframes and media assets, technical designs and diagrams, data management, process orchestration or deployment scripts, training modules, and system administration and end-user manuals;
3.2.9. compliance with the terms to be agreed upon in the project inception report, business requirements specifications and software requirements specifications;
3.2.10. exclusive key personnel for the project; and
3.2.11. one (1) year of maintenance and support services.

4. System Components

4.1. Public-facing Modules

4.1.1. General Information

The portal must:

4.1.1.1. allow site visitors to view information (text, infographics or videos) about the onboarding portal, subscription tiers and benefits, and requirements and process for onboarding.
4.1.1.2. allow site visitors to view a list of FAQs.

4.1.1.3. allow site visitors to do fuzzy search for information on the portal. *Fuzziness rules to be determined during requirements gathering.*
4.1.1.4. allow site visitors to search for RPs (by text or by categories).
4.1.1.5. allow site visitors to view, sort or filter through a list of RPs.
4.1.1.6. allow site visitors to search for TSPs (by text or by categories).
4.1.1.7. allow site visitors to view, sort or filter through a list of TSPs.
4.1.1.8. allow site visitors to chat or send messages for inquiries.
4.1.1.9. provide a link for site visitors to sign-in to their accounts or create accounts for their organization.
4.1.1.10. allow site visitors to view privacy policy and terms and conditions in using the site.
4.1.1.11. allow site visitors to accept or reject cookies selectively.
4.1.1.12. allow site visitors to click subscribe on a preferred subscription tier but, if not authenticated, be redirected to either the login or account creation page.
4.1.1.13. allow registered users to track application status without logging in.

4.1.2. Account Management

4.1.2.1. To create an account, public users must provide the following fields (*final field list to be disclosed to the winning contractor*):
4.1.2.1.1. Business Email address
4.1.2.1.2. Password
4.1.2.1.3. First Name
4.1.2.1.4. Last Name
4.1.2.1.5. Organization
4.1.2.1.6. Captcha
4.1.2.2. To create an account, public users must agree to the Terms and Conditions and Privacy Policy of the portal.
4.1.2.3. Public users must verify the provided email address before the portal activates the account.
4.1.2.4. A logged-in account must complete their personal profile information before being allowed to access other capabilities. *Personal profile field list to be disclosed to the winning contractor.*
4.1.2.5. A logged-in account must complete the organization profile before being allowed to access the onboarding application modules or other portal capabilities. *Organization profile field list to be disclosed to the winning contractor.*
4.1.2.6. Allow logged-in account users to fill in organization profile fields and upload supporting documents for an onboarding application.
4.1.2.7. Allow logged-in account users to add other users to the organization.

4.1.3. Onboarding Application Module

4.1.3.1. Allow a logged-in account to create an application based on the chosen subscription tier and subscription class.
4.1.3.2. The portal must provide a guided process (e.g. visualized steps or percentage of fulfilled tasks) for the onboarding application.
4.1.3.3. The portal must provide estimated time of processing for each step in compliance with RA 11032.
4.1.3.4. Onboarding application form fields must be auto-populated from the pre-filled personal or organizational profile fields.
4.1.3.5. Allow a logged-in account to partially fill-up or upload supporting documents and save the application as a draft.
4.1.3.6. Allow a logged-in account to continue working on a draft.
4.1.3.7. Allow a logged-in account to review the application prior to submitting the application.
4.1.3.8. Allow a logged-in account to submit an application.
4.1.3.9. Allow a logged-in account to track the status of the application. *Application status types to be disclosed to the winning contractor.*
4.1.3.10. Allow a logged-in user to update the application submission (modifying fields or uploading new documents).
4.1.3.11. Allow a logged-in primary account to abandon or cancel an application.

4.1.4. Subscription Management

4.1.4.1. Allow a logged-in user to view, download or print subscription contract and associated terms.
4.1.4.2. In-app or email alerts for contracts nearing expiry should contain links to the subscription renewal page.
4.1.4.3. Allow a logged-in user to
4.1.4.3.1. renew a current subscription;
4.1.4.3.2. upgrade to a higher subscription tier;
4.1.4.3.3. downgrade to lower subscription tier;
4.1.4.3.4. change the subscription class.
4.1.4.4. Renewal, upgrade and downgrade or tier, or change in class will trigger the application process. The application form fields will be auto-populated from the pre-filled organizational profile fields.

4.2. Administration Dashboards

4.2.1. Content Administration

4.2.1.1. Content management is accessible only to administration users with content writing or editing capability or higher access rights.
4.2.1.2. Capability for some drag-and-drop functionality to change the layout of the informational content area of the portal OR the capability to easily update page or section templates.
4.2.1.3. Allow content writers to add, modify or delete content.

4.2.1.4. Capability of the system to automatically populate content in the subscription section or page based on tier information provided in the Subscription Tier Administration module.
4.2.1.5. Capability to provide page layouts or templates compatible with PSA themes and incorporate official Philippine Standard Time maintained by DOST-PAGASA.
4.2.1.6. Allow content writers to update TSP list entries.

4.2.2. RP Accounts Administration
4.2.2.1. Allow account administrators to view, download or print a list of RP accounts.
4.2.2.2. Allow account administrators to filter or sort through a list of RP accounts.
4.2.2.3. Allow account administrators to view, download or print the profile of a RP organization and all primary and secondary accounts associated with the organization
4.2.2.4. Allow account administrators to view the transaction history of an RP account user (e.g. time stamp, actions taken, MAC and IP address, etc).
4.2.2.5. Allow account administrators to suspend or unsuspend an account. This will trigger the sending of an in-app and email notification to Portal Administrators. Suspension shall require a separate confirmation by a Portal Administrator.
4.2.2.6. Allow account administrators to suspend or unsuspend the subscription of an account. This will trigger the sending of an in-app and email notification to the Portal Administrators. Suspension shall require a separate confirmation by a Portal Administrator.

4.2.3. Application Processing
4.2.3.1. *This section provides an overview of the process. Processing steps to be disclosed to the winning contractor*.
4.2.3.2. System must ensure a FIFO processing of applications and a round-robin policy of assigning applications to application reviewers.
4.2.3.3. System must ensure anonymity of an application prior to an application reviewer viewing the contents of the application. *Viewable fields to be disclosed to the winning contractor.*
4.2.3.4. Allow application reviewers to view, download or print an onboarding application.
4.2.3.5. Allow application reviewers to transfer an application to another reviewer class.
4.2.3.6. Capability of the system to automatically set the application status to “Under review” once the application reviewer opens the application form.

4.2.3.7. Capability of the system to update the status of the application based on the action of the application reviewer. *Status types to be disclosed to the winning contractor.*

4.2.3.8. While “Under review”, allow application reviewers to annotate applications deemed deficient or requiring clarifications. The portal shall automatically send an email message to the applying organizations users. Annotations or comments that have been sent to the applicant can not be modified or deleted by the application reviewer.

4.2.3.9. Allow application approvers to review the application and annotation history made by the application reviewer. Annotations or comments that have been sent to the reviewer can not be modified or deleted by the application approver.

4.2.3.10. Allow application approvers to deny or approve the application. The portal automatically notifies the applicant and reviewer, in-app and via email, of the approval. If denied, the application approver must provide a reason.

4.2.3.11. Once approved, the portal shall automatically generate the letter of RP accreditation and subscription contract.

4.2.3.12. The portal must log all actions of the application reviewer, application approver and those by the portal itself.

4.2.4. Catalog Administration

4.2.4.1. Allow catalog administrators to dynamically update categories, drop down lists, statuses, select options, and other data fields. *Data categories or lists to be disclosed to the winning contractor.*

4.2.4.2. Allow catalog administrators to lock or unlock fields for editing or use by other users.

4.2.5. Subscription Administration

4.2.5.1. Allow subscription administrators to create subscription tiers. Subscription tier field list includes (*full list to be disclosed to the winning contractor*):

4.2.5.1.1. Tier name

4.2.5.1.2. Tier description

4.2.5.1.3. Tier capability list

4.2.5.1.4. Tier annual cost

4.2.5.1.5. Minimum subscription duration

4.2.5.2. Allow subscription administrators to create subscription classes. Subscription class field list includes (*full list to be disclosed to the winning contractor*):

4.2.5.2.1. Class name

4.2.5.2.2. Class description

4.2.5.3. Allow subscription administrators to dynamically adjust required supporting documents or fields for each tier type and/or for each class type via a simple UI interface.

4.2.5.4. Allow subscription administrators to set the permissible document MIME type.
4.2.5.5. Allow subscription administrators to mark a subscription tier or class as 'retired'. However, all existing subscription contracts of the retired tier or class will be honored.
4.2.5.6. Retired subscription tiers or classes will not be displayed on the content section.
4.2.5.7. Allow subscription administrators to set the alert schedule that is issued to remind RP account users before their subscription contracts expire. *System default alert schedule will be provided to the winning contractor*.
4.2.5.8. Allow subscription administrators to upload or create and modify the content of the letter of accreditation and subscription contract templates.
4.2.5.9. The portal has the capability to generate a QR code imprinted on the letter of accreditation. The QR code links back to a publicly available profile RP page providing organizational information and subscription status.

4.2.6. User Administration
4.2.6.1. Shall have access privileges of RP Accounts administrators.
4.2.6.2. Allow user administrators to create user groups and assign read, write, update or delete privileges over resources. Example of such user groups are (*final list to be disclosed to the winning contractor*):
4.2.6.2.1. Content managers
4.2.6.2.2. RP accounts managers
4.2.6.2.3. Application reviewers
4.2.6.2.4. Application approvers
4.2.6.2.5. Reports/Data analyst
4.2.6.2.6. Subscription tier administrators
4.2.6.2.7. Portal administrators
4.2.6.2.8. Auditors
4.2.6.3. Allow user administrators to create administration user accounts and assign the user to one or more user groups.
4.2.6.4. On creation, the default group of a user is the group with the least amount of granted privileges.
4.2.6.5. On the addition of an administration user, email addresses must be limited to the PSA domain. However, this capability must be configurable from the portal administration dashboard.

4.2.7. Portal Administration
4.2.7.1. Portal administrators shall have access privileges of all previous user groups.
4.2.7.2. Allow portal administrators to configure capabilities, thresholds, access to resources, lock/unlock content or fields, among others using a simple UI interface.

4.2.7.3. Allow portal administrators to create custom interactive dashboards to keep track of portal KPIs.

4.2.7.4. Allow portal administrators or the portal administration dashboard to access other dashboards or reports to automatically provide real-time analysis of data to identify hidden underlying patterns and drivers.

4.2.7.5. Allow portal administrators or the portal administration dashboard to access other dashboards or reports to automatically provide real-time analysis of data to identify hidden underlying patterns and drivers.

4.2.8. System administration dashboard or capabilities

4.2.8.1. System administrators shall have access privileges of all previous user groups.

4.2.8.2. Allow system administrators to configure the security policy (e.g. passwords, MFA mechanism, hash sizes, etc) and session management settings (length and entropy of session ID or token, session timeout, etc).

4.2.8.3. Allow system administrators to generate or view web analytics for the portal and service instances.

4.2.8.4. Allow system administrators to monitor overall system or instance health and performance.

4.2.8.5. Allow system administrators to configure acceptable email domains for users.

4.2.8.6. Allow system administrators to access other dashboards or reports to automatically provide real-time analysis of data to identify hidden underlying patterns and drivers.

4.2.8.7. Allow system administrators to set archiving rules and policies.

4.2.8.8. Allow system administrators to easily configure a pure cloud remote isolation environment to accommodate flexible deployment scenarios.

4.2.8.9. Allow system administrators to integrate the remote isolation environment with a variety of cybersecurity solutions (IPS/IDS, firewalls, etc) to facilitate phasing in with the existing cybersecurity framework of the Procuring Entity.

4.2.8.10. Allow system administrators to configure the remote isolation environment to allow select users to access original uploaded documents.

4.2.9. Audit dashboard

4.2.9.1. Capability to generate reports or analytics on actions taken by portal users.

4.2.9.2. Allow portal auditors to view actions taken by portal users (read privilege only).

4.2.10. General administration and configuration capabilities

4.2.10.1. Allow administration users the capability to create dynamic lists on a set of criteria or categories over a set of metrics. For example, allow the RP accounts administrator to generate the list of active RPs with a subscription type (set of criteria and categories) within the month (the metric).

4.2.10.2. Allow administration users to drill down lists.

4.2.10.3. Allow administration users to generate standard statistical measures (average, mode, mean, std devs, etc).

4.2.10.4. Allow administration users to calculate new field values using formulas based on existing data elements.

4.2.10.5. Allow administration users to print or export lists, on their dashboard, to CSV or PDF files.

4.2.10.6. Allow administration users to easily create or generate reports through self-service features.

4.2.10.7. Allow administration users to create stories and visual presentations for effective data storytelling.

4.2.10.8. Allow administration users to set threshold alerts and to receive alerts - in app, via email or SMS.

4.2.10.9. Allow administration dashboards to monitor data automatically and execute data analysis and discovery.

4.2.10.10. Allow administration dashboards to conduct AI-driven data analysis to automatically identify significant changes or important and relevant correlations.

4.2.10.11. Allow administration users to import predictive data models using PMML.

4.3. Generic Functions

4.3.1. Document Uploading

4.3.1.1. Capability of the system to limit document types for uploading.

4.3.1.2. Uploaded files will be stored in quarantine file storage.

4.3.1.3. Only files deemed clean or file copies rendered in a remote isolation platform will be viewed or downloaded by administration users with document viewing access privileges.

4.3.2. Log Management

4.3.2.1. All services, modules or microservices shall log transactions. *Log detail for each module or service to be agreed with the Procuring Entity.*

4.3.2.2. Access to the portal by site visitors, authenticated or not, must be logged.

4.3.2.3. System errors must be logged in the service logs and, separately, in an error log file.

4.3.2.4. Log transactions should be uploaded to a central log service based on a schedule configurable from the system administration dashboard.

4.3.2.5. Capability to regularly check and verify the integrity of log files easily.

4.3.2.6. Capability to access logs (per service or the central log service) shall be limited by an administration user's user group privileges.

4.3.2.7. Capability to provide interactive updates or near real-time reports of web traffic and threats identified by the remote isolation platform. Logs must contain detailed information.

4.3.3. Integration endpoints

4.3.3.1. The portal must have the capability to provide REST API endpoints for integration with other PSA systems. *Full list of API endpoints will be disclosed to the winning contractor.* It may include:

4.3.3.1.1. the list of RPs, by status, by subscription tier, etc;

4.3.3.1.2. subscription tier and status of an RP;

4.3.3.1.3. onboarding status of an RP;

4.3.4. Authentication and Authorization

4.3.4.1. Must have an authentication and authorization service using OpenID Connect, OAuth 2.0 or SAML. Authentication and validation will be sent via JWTs along with authorization or access privileges.

4.3.4.2. The portal shall provide PSA/UCDMS the option to integrate with an external single sign-on, federated identity management or identity access management system using OpenID Connect, OAuth 2.0 or SAML.

4.3.4.3. Capability to retrieve access rules from cloud-based or on-premise LDAP or Active Directory servers.

4.3.4.4. User authentication and authorization

4.3.4.4.1. There must be two separate login pages for RP account users and administration users. *Required login fields for RP users and administration users to be disclosed to the winning contractor.*

4.3.4.4.2. Allow users to recover an account if the password has been forgotten. Must trigger a multifactor authentication.

4.3.4.4.3. If a user is added by a registered user, the portal must generate a temporary randomly generated password. The portal must send an automated email to the added user informing them of the account generation with a link to a page to update the generated password. Updating the password serves as the email verification process. Only then will the added user be able to login. For added administration users, the email shall contain the user group assignment.

5. Non-functional Requirements

5.1. Usability

5.1.1. The portal must be designed with usability in mind particularly ease-of-use across a variety of device viewport sizes, memory, and computing power.

5.1.2. The most important elements must be prominent and highlighted on the page. All important features for a user group must be accessible within two clicks on average.

5.1.3. The design must be intuitive by incorporating established or standard design elements, usability patterns and must take advantage of standard gestures in mobile devices.

5.1.4. Administration users must be able to view dashboards, tables, lists, and reports elegantly on mobile devices.

5.1.5. Accessible help or guides, clear instructions and task progress must be provided to facilitate task completion.

5.1.6. Users must be able to reverse or undo actions. Actions which could not be undone must have a confirmation prompt.

5.1.7. Must incorporate principles outlined in ISO 9241-171.

5.1.8. Rendered pages, assets or files must not adversely impact user experience and functionality (e.g. rendering delays, print capability, pixelation issues, etc).

5.2. Accessibility

5.2.1. The portal must comply with web content accessibility guidelines (WCAG) 2.1 or ISO/IEC Guide 71:2014 and follow the technical specifications defined in WAI-ARIA.

5.3. Scalability and Performance

5.3.1. Interservice communication shall, on average, not exceed 500ms for services located in the same availability zone or data center cluster.

5.3.2. Uploading or downloading of data or graphical user interface web pages containing less than 1MB of data shall load within three (3) seconds.

5.3.3. Micro- and web services must be open to connections, accept requests and issue responses 99.99% of the time for 24x7 / 365.

5.3.4. Must incorporate lightweight client-side caching to satisfy performance requirements across a variety of end-point devices and internet connection speeds.

5.3.5. Must provide an in-memory database to store denormalized view data to speed up rendering of interactive reports and analytics.

5.3.6. The portal must be able to support 6,000 concurrent sessions (authenticated or not) without significant impact on the portal’s response times.

5.3.7. The portal must support a minimum of 5,000 registered users to scale up to 15,000 in the next few years.

5.3.8. Portal pages, including dashboards, reports and analytics, must be mobile responsive.

5.3.9. The remote isolation environment must minimize rendering delays by allowing granular-level remoting strategy of DOM elements to offer options for selective rendering only or dropping of active elements while leaving safe elements as is.

5.4. Availability

5.4.1. The portal must be able to run in various deployment scenarios including running instances simultaneously in different locations to ensure high availability: various on-prem locations, multiple zones in the cloud or hybrid. *The deployment scenario will be disclosed to the winning contractor.*

5.5. Application Failure Recovery

5.5.1. The portal must be resilient to server or database failures and must have the failover capability to recover within a reasonable time to be agreed upon with the Procuring Entity.

5.5.2. The portal must, at all times, be at a known state. The portal should provide default response behavior for unplanned events (e.g. broken connection or session, corrupted or irreparable messages, etc.).

5.5.3. The portal must have an automatic recovery mechanism after system failure.

5.5.4. The portal must be able to alert system administrators of the inaccessibility of a resource, a component or service.

6. Technical Requirements

6.1. General Design Principles

6.1.1. The portal must be designed using a domain-driven service-based type of architecture consisting of decoupled and autonomous services.

6.1.2. Must be guided by security-by-design principles (e.g. ISO 27001, OWASP, NCSC, AWS SbD, etc) during the design and development stages.

6.1.3. Must adopt edge computing principles into consideration where possible.

6.1.4. Must be ready to employ either asynchronous (preferred) or synchronous interservice communication depending on the specific requirements of the producer-consumer service pair. *Specific requirements to be disclosed to the winning contractor*.

6.1.5. Must provide configurable capability over the remote isolation key perenvironment to prevent infected assets or active content from reaching the endpoint device of administration users.

6.1.6. The remote isolation environment must quickly discard used containers to reduce risk of persisting malware or infections in the isolation environment.

6.1.7. Nearly static content should be cached in the frontend service instances.
6.1.8. Must provide asset versioning and cache busting capabilities.
6.1.9. Must provide load balancing and web server capabilities.
6.1.10. Must provide a near plug-and-play capability for third-party tools in services that make use of them.
6.1.11. Must support OpenAPI.
6.1.12. Interservice communication must be secure and encrypted at all times by using HTTPS/TLS protocols.
6.1.13. Interservice communication must include access and identity tokens to allow a service to verify privileges with the authentication and authorization service.
6.1.14. Must persist all transactions and data to allow compliance with data retention rules of the government or of the Procuring Entity for audit purposes.
6.1.15. Must provide administration users secure access to the portal regardless of their location (office, business trip or at home) while using their device's native browser by providing a remote isolation environment without requiring a disconnected network or physical reconfiguration of the network.
6.1.16. Must provide administration users a way to safely view portal pages and assets or download files from a remote isolation platform that renders clean and malware-free assets and files.

6.2. Technology Specifications
6.2.1. Must utilize the latest stable open-source operating systems, databases, development frameworks and languages, caching, and interservice frameworks.
6.2.2. Must be under the latest versions of the MIT, BSD, GPL, MPL or Apache License.

6.3. Development, Testing and Deployment Pipeline
6.3.1. Must adhere to secure software development standards such as those specified in OWASP Secure Coding Practices, NIST Special Publication 800-218 or equivalent standards from BSA or SAFECode. This includes taking measures to mitigate security risks outlined in the latest OWASP Top 10.
6.3.2. Encryption must use the latest KDF-type of standards or protocols. For hashing secrets, the algorithm must be resistant to GPU-based and side channel attacks.
6.3.3. Error stacks will only be displayed in the development and testing environments. For staging and production, only general error messages will be displayed.
6.3.4. Must utilize open source containerization and orchestration tools.
6.3.5. Integration and deployment pipeline should incorporate security, unit and integration testing for each scrum cycle.

6.3.6. Must implement comprehensive unit tests, functional tests, security or application vulnerability tests, regression tests and load tests as part of user acceptance testing.
6.3.7. Security testing must adhere to the general principles and standards set in OWASP Web Security Testing Guide and OWASP Web Application Penetration Checklist.
6.3.8. The system must be deployable in various deployment scenarios: cloud, on-premise or hybrid environments. *Production environments will be disclosed to the winning contractor.*

7. Collaborative Tool Requirements
   7.1. Project Management Tool
      7.1.1. Allow the creation of Kanban or Scrum boards.
      7.1.2. Provide a to-do list for planned tasks.
      7.1.3. Allow some workflow customization and automation.
      7.1.4. Provide encryption in transit and at rest.
      7.1.5. Accessible 24/7 throughout the project duration.
      7.1.6. Provide PSA/UCDMS five (5) seats for the tool.

   7.2. Code versioning and repository
      7.2.1. Must be a secured and private code repository.
      7.2.2. Must use git for versioning.
      7.2.3. Provide PSA/UCDMS three (3) seats with full repository access.

   7.3. Document Sharing
      7.3.1. Must provide collaborative document storage for all documents, files, assets, etc that will be part of this contract.
      7.3.2. Procuring entity must have full editing access to these files.

8. Training
   8.1. The following trainings will be conducted:
      8.1.1. system functionality for twenty (20) business users
      8.1.2. technical components (IT, system administration, deployment configuration, etc) for ten (10) technical users
      8.1.3. project management for five (5) personnel.
   8.2. The contractor shall provide all training manuals and meals/snacks.
   8.3. The contractor shall include hands-on lab modules in the conduct of the training.

9. BIdder Requirements
   9.1. Prospective bidders must
      9.1.1. have a proven track record in Information Technology, Software Development and Systems Integration.
      9.1.2. have completed at least three (3) software development projects with the Philippine government.
      9.1.3. be duly registered with the National Privacy Commission under RA 10173 of 2012. The certificate must be attached to and submitted with the bidding documents.
      9.1.4. have the personnel or key experts described under the Personnel Requirements section of this document. Prospective bidders must submit all the CVs and certifications along with the bidding documents.
      9.1.5. shall assign key personnel exclusively for the project.

10. Personnel Requirements
   10.1. One (1) Project Manager
      10.1.1. Must have at least five (5) years of solid experience in managing software development projects. Must present certification as proof of this experience.
      10.1.2. Must have the following certifications issued by the recognized certifying organizations:
         10.1.2.1. Project Management Professional
         10.1.2.2. PRINCE2 Foundations
         10.1.2.3. Agile Project Management
         10.1.2.4. Professional Scrum Master
      10.1.3. Must be an authorized training instructor of the Project Management Institute of the Philippines.
      10.1.4. Must have managed at least one (1) distributed web-based system or document management system.
      10.1.5. Proficiency in distributed systems and service-based architectures
      10.1.6. Demonstrable experience using online project management tools including designing project workflows.
      10.1.7. Proficiency in software quality assurance and audit checks.
      10.1.8. Experience in managing software quality assurance.

   10.2. One (1) Business Analyst
      10.2.1. Must have at least five (5) years of experience in aligning business and technical requirements to meet client needs.
      10.2.2. Must have attended at least one (1) Project Management Training.
      10.2.3. Strong background in digital transformation and organizational change management.
      10.2.4. Demonstrable experience in UML 2.0 in at least two (2) projects.
      10.2.5. Proficiency in SQL, data management and data analytics.
      10.2.6. Excellent use case documentation and technical writing capabilities.

10.3. One (1) UI/UX Designer

10.3.1. Must have at least five (5) years of experience in adaptive or responsive web design.
10.3.2. Demonstrable experience in Adobe Photoshop or other equivalent online collaborative design tools such as InVisio, Bootstrap Studio, LucidChart or Canva.
10.3.3. High proficiency in HTML5 and CSS3.
10.3.4. Proficiency in template engines and at creating page and email templates.
10.3.5. Demonstrable experience in usability analysis in one (1) project..

10.4. Two (2) Senior Developers

10.4.1. Must have at least five (5) years of experience in developing distributed systems, service-based web applications or document management systems.
10.4.2. Must have experience developing systems for at least three (3) national-level government agencies.
10.4.3. Demonstrable experience in MySQL, Java, C++ , PHP, React or Vue, HTML5, CSS3, BootStrap to be demonstrated by certifications provided by internationally-regarded organizations or by three (3) projects completed within the last two (2) years.
10.4.4. High proficiency in service-oriented architectures, especially using asynchronous messaging.
10.4.5. High proficiency in OAuth2.0 and OpenID Connect.
10.4.6. Must have either an AWS developer certification or proven experience in at least two (2) AWS software development with at least one (1) in a hybrid set-up.
10.4.7. High proficiency in UML2.0.
10.4.8. Experience in containerization and process orchestration.
10.4.9. Demonstrable experience in secure coding practices.

10.5. One (1) UI or Frontend Developer

10.5.1. Must have at least three (3) years of experience in developing web or mobile frontends.
10.5.2. High proficiency in a JavaScript or TypeScript framework demonstrated by either a certification by an internationally-recognized organization or two (2) demonstrable projects within the last year.
10.5.3. High proficiency in HTML5, CSS3, pre-CSS compilers, and Webpack.
10.5.4. High proficiency at creating custom Gutenberg-compatible WordPress themes or plugins.
10.5.5. Demonstrable experience in creating and using web page and email templates.
10.5.6. Proficient in UML2.0.
10.5.7. Proficient at creating and accessing RESTful services.
10.5.8. Experience in micro-frontends and established open-source content management systems.

10.5.9. Proficient in secure coding practices.

10.6. Three (3) Developers

10.6.1. Must have at least two (2) years of experience in developing service-based web or mobile application;
10.6.2. Must have development experience with at least one (1) government agency.
10.6.3. High proficiency in the language or framework chosen for developing the service.
10.6.4. Experience in at least one (1) AWS-based software development project. An AWS developer certification is a plus.
10.6.5. Experience in containerization and process orchestration.
10.6.6. Experience in OAuth2.0 and OpenID Connect.
10.6.7. Experience accessing LDAP and Active Directory servers.
10.6.8. Experience in RESTful API and OpenAPI.
10.6.9. Proficiency in UML2.0..
10.6.10. Proficiency in secure coding practices.

10.7. One (1) Database Engineer

10.7.1. Must have five (5) years experience in SQL databases and at least one (1) year in a NoSQL database.
10.7.2. At least two (2) year experience with AWS and hybrid storage deployments. AWS certification is highly preferred.
10.7.3. Solid background in distributed database set-up, security and optimization.
10.7.4. High proficiency in UML 2.0.
10.7.5. Experience in writing scripts for automated deployments, monitoring or running backups.

10.8. One (1) Test Analyst

10.8.1. Must have at least three (3) years of experience in creating test plans, conducting testing on software, websites, and other similar systems.
10.8.2. Experience in creating test plans and conducting tests for a web-based distributed system.
10.8.3. Proficiency at running regression, integration and load testing.
10.8.4. Demonstrable experience using testing tools like Katalon, Selenium, Apache JMeter or other similar tools.
10.8.5. Demonstrable experience with testing in automated agile-based development and test cycles.
10.8.6. Proficiency at using bug tracking tools.

10.9. One (1) Data Management Analyst

10.9.1. Must have at least three (3) years experience as a data management specialist with one (1) completed project with a government agency.
10.9.2. Must have at least one (1) year experience in data analytics.

10.9.3. High proficiency in analyzing data requirements and creating data flow diagrams.
10.9.4. Experience in designing data pipelines.
10.9.5. High proficiency in data privacy and data security.
10.9.6. Must be certified or have at least one (1) year demonstrable experience using the analytics tool to be used in this portal.
10.9.7. High proficiency in understanding data and reporting requirements, data flows and converting these into report templates and analytics dashboards.

10.10. One (1) Technical Writer
10.10.1. Must have at least two (2) years of experience in documenting technical specifications and creating user guides or manuals for both technical and non-technical business users with at least one (1) completed project with a government agency.
10.10.2. Experience writing documentation using ReST is preferred.
10.10.3. Must have experience using online documentation tools like Sphinx.

10.11. Two (2) Training Specialists
10.11.1. Must have two (2) years experience creating training modules and conducting training in physical, virtual or blended modes.
10.11.2. Must have conducted training in at least two (2) government projects.
10.11.3. Must be part of the project team and involved during development.
10.11.4. Experience in creating hands-on lab modules for both technical and non-technical users.

11. COVID Precautions
11.1. All personnel by the winning contractor that shall be required for a physical meeting or visit to PSA premises must be vaccinated and boosted for at least two (2) weeks beforehand.

12. Service Level Agreement

12.1. The winning contractor and the Procuring Entity shall agree on an SLA and escalation protocols to be implemented during the warranty period. The SLA should reflect the general severity levels described below.

Severity level	Maximum Resolution Time (from the time problem is determined to the time of resolution)	Support Channel
High/Critical/Down	Four (4) hours	Dedicated phone (24x7) Chat or Online Customer Portal Email
Medium/Normal	Next business day	Phone Chat or Online Customer Portal Email
Low/General Question	Two (2) business days	Chat or Online Customer Portal Email

13. Activities and Delivery Roadmap

	Activities	Deliverables	Schedule
13.1.	**Project Kickoff and Planning**	● Project Inception Report and Planning Documents ● Approved Team Composition ● Non-Disclosure Agreements with Contractor and Personnel ● Signed Personnel Code of Conduct when assigned to PSA facilities ● Provision of full access (for this project) to a project management collaboration tool and document sharing	Within fourteen (14) calendar days from issuance of Notice to Proceed.
13.2.	**Business Requirements Analysis**	● Business Requirements Document ● Data Management Plan ● System Requirements Specifications	Within fourteen (14) calendar days from delivery of Project Kickoff and Planning

13.3. System Design	• Updated System Requirements Specifications (include high-level system design)	Within seven (7) calendar days from delivery of Business Requirements Analysis
13.4. Development of Feature Set One 13.4.1. General Information 13.4.2. Authentication and Authorization ***13.4.3. Client-facing*** 13.4.3.1. Account management ***13.4.4. Administration Dashboard*** 13.4.4.1. User administration 13.4.4.2. Content Management 13.4.4.3. Subscription Tier Management	The following all refer to functional and nonfunctional requirements included in Feature Set One: • Updated Business Requirements Document • Updated System Requirements Specifications (including architecture decisions, technical diagrams such as ERDs, data flows, sequence diagrams, etc) • Wireframes and Designs • Test Scenarios, Test Scripts and Test Reports • Provision of full access (for this project) to design collaboration	Within thirty (30) calendar days from delivery of System Design
13.5. Development of Feature Set Two ***13.5.1. Client-facing*** 13.5.1.1. Application Module ***13.5.2. Administration Dashboard*** 13.5.2.1. RP Accounts Administration 13.5.2.2. Catalog Administration 13.5.2.3. Application Processing 13.5.3. Document Uploading	The following all refer to functional and nonfunctional requirements included in Feature Set Two: • Updated Business Requirements Document • Updated System Requirements Specifications (including architecture decisions, technical diagrams such as ERDs, data flows, sequence diagrams, etc) • Wireframes and Designs • Test Scenarios, Test Scripts and Test Reports (inc Regression Tests) • Quality Assurance Audit report	Within fifty (50) calendar days from delivery of Development of Feature Set One

13.6. Development of Feature Set Three ***13.6.1. Client-facing*** 13.6.1.1. Subscription Management ***13.6.2. Administration Dashboard*** 13.6.2.1. Log Management	The following all refer to functional and nonfunctional requirements included in Feature Set Three: ● Updated Business Requirements Document ● Updated System Requirements Specifications (including architecture decisions, technical diagrams such as ERDs, data flows, sequence diagrams, etc) ● Wireframes and Designs ● Test Scenarios, Test Scripts and Test Reports (inc Regression Tests) ● Quality Assurance Audit report	Within thirty-five (35) calendar days from delivery of Development of Feature Set Two
13.7. Development of Feature Set Four ***13.7.1. Administration Dashboard*** 13.7.1.1. System Administration 13.7.2. Integration Endpoints	The following all refer to functional and nonfunctional requirements included in Feature Set Four: ● Updated Business Requirements Document ● Updated System Requirements Specifications (including architecture decisions, technical diagrams such as ERDs, data flows, sequence diagrams, etc) ● Wireframes and Designs ● Test Scenarios, Test Scripts and Test Reports (inc Regression Tests) ● Quality Assurance Audit report	Within fifteen (15) calendar days from delivery of Development of Feature Set Three
13.8. Load, Security and User Acceptance Testing	● Delivery of source and production code and/or subscription contracts to third-party tool providers ● Deployment Script and Guide/Documentation ● Installation in Staging Environment ● Load Scenarios, Scripts and Reports ● User Test Scenarios, Test Scripts and Test Reports ● Cybersecurity Testing	Within fourteen (14) calendar days from delivery of Development of Feature Set Four

13.9. Training	● Training Modules ● System Administration Documentation ● End-User Documentation ● Conduct of Training	Within ten (10) calendar days from delivery Load, Security and User Acceptance Testing
13.10. Deployment	● Deployment in production environment without high/critical/downtime cases for at least one (1) calendar week	Within three (3) calendar days from delivery of Training
13.11. Project sign-off	● Service Level Agreement ● Project Sign-off Document	Within three (3) calendar days from delivery of Deployment

14. Payment Terms

Activity / Milestone	% Progress
Project Kickoff and Planning	10% of contract price net of 10% retention, upon submission of Acceptance (Verification) Report
Business Requirements Analysis	
System Design	
Development of Feature Set One	40% of contract price net of 10% retention, upon approval of PSA on the Partial Acceptance (Validation) Report
Development of Feature Set Two	
Development of Feature Set Three	30% of contract price net of 10% retention, upon approval of PSA on the Partial Acceptance (Validation) Report
Development of Feature Set Four	
Load, Security and User Acceptance Testing	20% of contract price net of 10% retention, upon approval of PSA on the User Acceptance Report and its issuance of a Certificate of Completion.
Training	
Deployment	
Project Sign-off	
TOTAL	**100%**

15. Warranty, Maintenance and Support
    15.1. The warranty period shall commence after consummation of the contract (after Project Sign-off).
    15.2. The winning contractor must provide one (1) year of maintenance and support services during the warranty period.
    15.3. The winning contractor must ensure a timely response to provide updates (e.g. security patches, OS and third-party tool updates) on components, design features, libraries or tools.
    15.4. There must be an adequate and timely response to address bugs and system errors.

16. Responsibilities of the Contractor
    16.1. The Contractor shall be expected to provide all services and goods specified in its Scope of Work outlined in this document.
    16.2. The Contractor shall ensure the confidentiality of all communications with the Procuring Entity.
    16.3. The Contractor shall recognize that the Procuring Entity exercises all intellectual property rights over all documents, diagrams, designs, wireframes, graphic assets, code, scripts, etc that have been developed or written for this project engagement.
    16.4. The Contractor shall endeavor to satisfy the deadlines set in this terms of reference. However, parameters for flexibility in delivery deadlines may be outlined in the Project Planning Report especially where approvals or actions by the Procuring Entity are necessary.
    16.5. The Contractor shall ensure that all contractor employees that may be assigned to the premises of the Procuring Entity are expected to obey the code of conduct, and other rules of the Procuring Entity.
    16.6. Employees of the contractor assigned to the project are not considered employees of the Procuring Entity. The Contractor must ensure provision of allowances, insurance, and other incentives to their employees as required by law.
    16.7. The Contractor shall host the environments for development, testing, and staging.
    16.8. The Contractor shall assign key personnel exclusively for the project.

17. Responsibilities of the Procuring Entity
    17.1. The Procuring Entity shall be expected to ensure a timely response to steps or actions (reviews, approvals, permits to access to the premises for installation, etc) needed by the Contractor to satisfy the delivery of services and goods.

17.2. The Procuring Entity must supply the Contractor their Code of Conduct and other rules that prescribe employee behavior.
17.3. The Procuring Entity shall provide adequate work space and internet connectivity to employees of the Contractor that may be assigned to work on the premises of the Procuring Entity.
17.4. The Procuring Entity shall host the environments for production.
17.5. The Procuring Entity shall provide the venue, projectors or monitors, audio system and shall be in-charge of choosing and inviting participants to attend training sessions to be conducted by the Contractor.

18. Confidentiality

18.1. All project personnel of the contractor shall be required to sign a non-disclosure agreement immediately at the start of the project.

18.2. All systems to which the project personnel of the contractor shall be granted access to, its components, parts, specifications, data, ideas, technology, and technical and non-technical materials (collectively referred to here as “Proprietary Information”) are confidential and proprietary to the Procuring Entity.
18.3. The contractor agrees to hold the Proprietary Information in strict confidence and further agrees not to reproduce, transcribe, or disclose the Proprietary Information to third parties without the prior written approval of the Procuring Entity.