



ASEAN SECRETARIAT

Request for Proposal

**Provision of Hosting Service for ASEAN
Customs Transit System Central Service
(ACTS CS) Live.**

Contract Period: 12 months from 12 March 2023 - 11 March 2024,
With the possibility to extend for another period of 12 months.

PROPOSAL MUST BE RECEIVED BY
27 January 2023

DELIVER/MAIL PROPOSAL TO:
ASEAN Secretariat
Jl. Sisingamangaraja 70A
Jakarta 12110
Indonesia

Prepared by: Trade Facilitation Division – Market Integration Directorate
Date: 17 January 2023



TERMS OF REFERENCE (TOR)
HOSTING SERVICE OF THE ACTS CENTRAL SERVICE (CS)

Prepared by
Central Management Team (CMT) of the ASEAN Customs Transit System
The ASEAN Secretariat

Table of Contents

1. INTRODUCTION 1

2. HOSTING SERVICE REQUIREMENTS..... 1

 2.1 TECHNICAL EXPERIENCE AND QUALIFICATIONS REQUIREMENTS 1

 2.2 TECHNICAL SCOPE OF WORK..... 3

 2.3 SERVICE ARCHITECTURE AND QUANTITY 7

 2.4 SERVICE LEVEL AGREEMENT (SLA)..... 9

3. SCHEDULE 11

ANNEX I DATA CENTER SPECIFICATION 12

ANNEX 2 ISO/IEC 27002 (Information Security)..... 15

1. INTRODUCTION

The ASEAN Customs Transit System (ACTS) is a computerised Customs transit management system available to operators who move goods across borders without paying the required duties and taxes otherwise due when the goods enter (or leave) the country thus requiring only one (final) Customs formality. It offers an administratively simple and cost advantageous procedure to carry goods across Customs territories outside the normal import and export Customs regimes. The ACTS consists of two main components: National ACTS Applications and ACTS Central Services (CS). National ACTS Applications are installed on the ASEAN Member States and ACTS Central Services (CS) installed in a central location. Communication between National ACTS Applications and ACTS CS through ASEAN Closed Secure Network (ACSN).

The ACTS CS hosts a set of services, Reference Data System (RDS) and Management Information System (MIS) are setup as distributed database in CS and National ACTS ICT Environments in the ASEAN Member States (AMS). The following are the CS applications modules:

- Central Reference Data System (RDS) – distributed database
- User Management System
- Information Portal
- Management Information System (MIS) – distributed database
- ACSN Gateway

This TOR will specify the requirements for hosting service of the ACTS CS.

2. HOSTING SERVICE REQUIREMENTS

The following section will explain the requirements of the hosting service that must be fulfilled by service provider.

2.1 TECHNICAL EXPERIENCE AND QUALIFICATIONS REQUIREMENTS

Technical experience and qualifications requirements explain about the requirements regarding technical experience of the service provider including their engineer capability to deliver the ACTS CS Hosting service. Some documents must be provided by service provider as stated in the following table.

Table 1. Technical Experience and Qualifications Requirements

No.	Requirement details	Status	Notes
Technical Experience			
1	Service provider must have at least 3 years' experience for hosting the virtual servers in the private cloud or in the cloud for	Mandatory	List of projects experience with the brief description must be provided (at least 3 projects)

No.	Requirement details	Status	Notes
	the following activities: • Provisioning and installing the virtual servers • Configuration of the virtual servers • Data backup for the virtual servers		
2	Service provider must have at least 3 years' experience for installing, configuring and maintaining of the Linux and Windows Operating System (OS). Experience must related with the following scope of work: • Cron-tab scripting • Task scheduler configuration • Linux OS modules installation and configuration • Windows OS tuning and configuration • OS patch installation and configuration • OS modules patch installation and configuration OS modules include the following packages: • Nginx • OpenJDK • JBoss Wildfly • JBoss Keycloak • Apache Cassandra • OpenDJ • ArtemisMQ • PostgreSQL	Mandatory	List of projects experience with the brief description must be provided (at least 3 projects)

No.	Requirement details	Status	Notes
Qualifications			
3	Service provider must have qualified engineers to deliver the service. Engineers must be certified for the following systems: • Linux OS • Windows OS • Networking e.g. CCNA	Mandatory	List of certified engineers must be provided.

2.2 TECHNICAL SCOPE OF WORK

Technical scope of work explains about the scope of work for ACTS CS hosting service. Service provider must provide all items stated in the scope of works.

Table 2. Technical Scope of Work

No.	Requirement details	Status	Notes
	General		
1.	Provide IT infrastructure components with guaranteed computing power and capacity in virtual environments OR cloud. The following infrastructure components must be provided: • computing/virtual server components • network and connection components • security components • storage components • backup components	Mandatory	Detail requirements appear in Chapter 2.3
2.	In case of virtual server setup hosted in a private data center, IT infrastructure components must hosted in the TIA 942 certified data center at least Tier III specification. Service provider must also inform the compliance of the data center	Mandatory	Certificate of Standard Conformity must be provided (Specification appears in ANNEX 1)

No.	Requirement details	Status	Notes
	international certification standard if the virtual server hosted in the public data center (cloud).		
3.	Dedicated internet international connection with minimum bandwidth 1 Mbps Downstream and 1 Mbps Upstream.	Mandatory	Service provider must provide the burst bandwidth policy
4.	IT governance and security compliance (e.g.: ISO 27000 series)	Mandatory	Certificate of Standard Conformity must be provided (Specification appears in ANNEX 2)
Operating System Managed Service			
5.	Provide Operating System (OS) as required by software platforms and ACTS applications	Mandatory	Detail requirements appear in Chapter 2.3
6.	OS (Operating system) managed service: • Versioning control as required by software platforms and ACTS applications. Upgrading or changing of operating system must be accommodated based on application requirements, end-of-support condition, or security issues. • OS modules and dependencies installation and configuration as required by application, end-of-support condition, or security issues. • Patch management based on compatibility, severity and security consideration, or end-of support condition. • Incident and problem management related with OS • Operate and manage the OS of the server OS modules include the following packages:	Mandatory	

No.	Requirement details	Status	Notes
	• Nginx • OpenJDK • JBoss Wildfly • JBoss Keycloak • Apache Cassandra • OpenDJ • ArtemisMQ • PostgreSQL		
7.	Provide Migration Service to migrate the existing web-based applications from the current hosting provider by ensuring minimal downtime during the migration through proper planning and execution.	Mandatory	Service Provider to provide the migration plan
Network and Security Managed Service			
8.	Provide network and security as required by systems. The following network and security components must be provided: • Network zoning • VLAN creation and management • Firewall connection management • Pfsense installation, configuration and management • VPN site-to-site creation and management	Mandatory	Detail requirements appear in Chapter 2.3
9.	Perimeter security protection: • Firewall • Anti DOS-attack (Distributed Denial of Service) • IPS (Intrusion Prevention System)	Mandatory	Service provider could inform their additional perimeter protection e.g.: web application firewall
10.	Network and security managed service: • Patch management based on compatibility, severity and security consideration • Incident and problem management related with network and security • Operate and manage the network and security • Security incident management	Mandatory	
Data and Backup Managed Service			
11.	Capacity management of data and storage	Mandatory	Detail requirements appear in Chapter 2.3

No.	Requirement details	Status	Notes
12.	Daily regular backup of the ACTS virtual machines to ensure the availability of recovery when needed. Virtual machine backup retention for 6 months is required.	Mandatory	
13.	At the end of the contract, must provide the most updated virtual machine image in the Open Virtualization Format (OVF) or other formats that could be imported to the other virtualization platform.	Mandatory	
Monitoring and Administration			
14.	Service monitoring: - IT Infrastructure components - System processes of the ACTS	Mandatory	
15.	Monthly reporting: - Uptime/Availability - Response time - CPU Utilization - RAM Utilization - Storage Utilization - Backup Status - Link Utilization	Mandatory	
16.	Accessibility of the IT infrastructure components through internet connection.		
Service Level Agreement (SLA)			
17.	Provide the service based on the required SLA for availability, incident and problem resolution		Detail requirements appear in Chapter 2.4

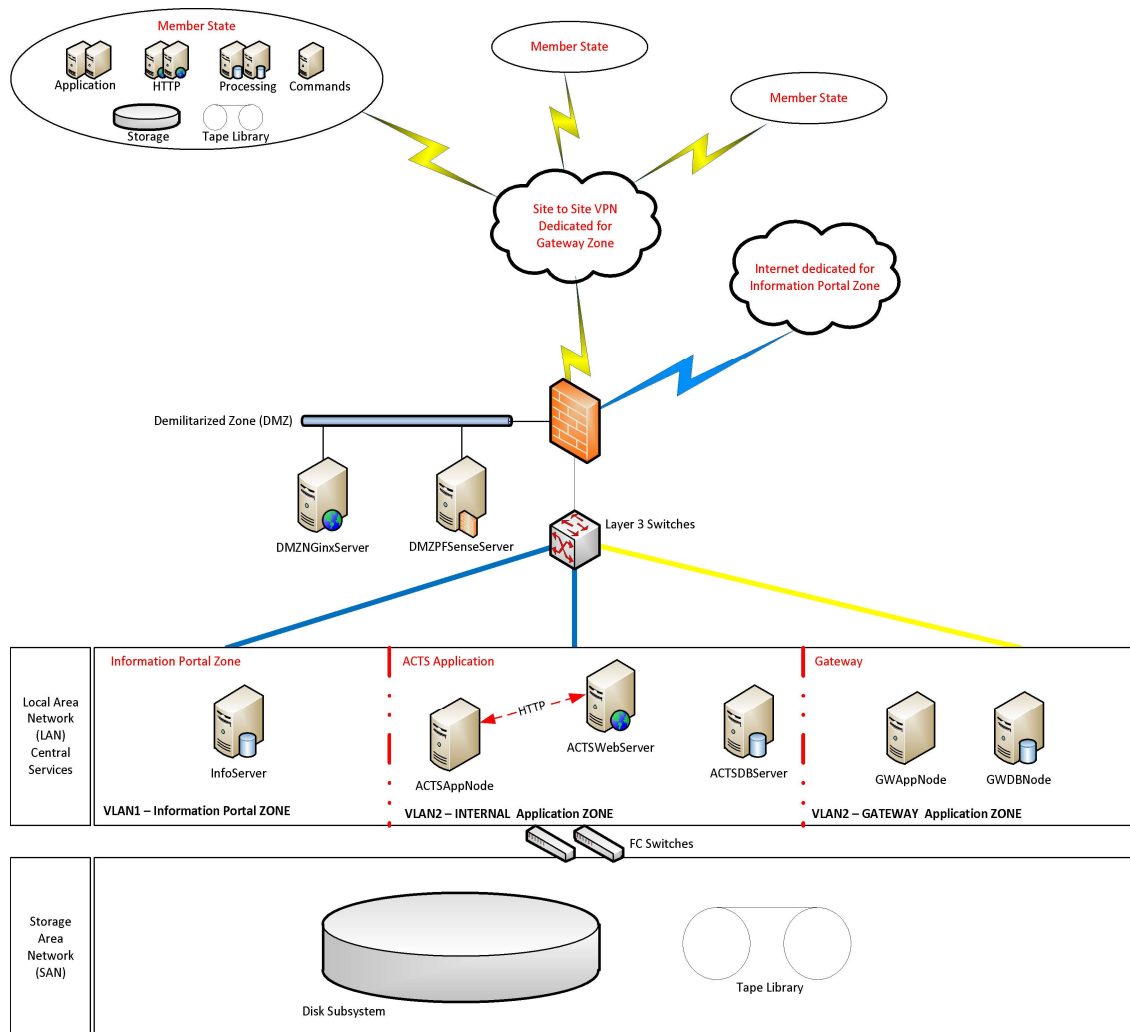
ACTS system could need relocation and reconfiguration from existing server to the new hosting service. The activity will be done by the application developer. All access related to the virtual server should be shared at least 20 days before the Live date.

2.3 SERVICE ARCHITECTURE AND QUANTITY

The Central Services (CS) environment implemented in 4-zones architecture which consists of the following zones:

- Information Portal (Proxy);
- ACTS Applications Zone;
- Application DB Zone;
- Demilitarized Zone (DMZ).

All the applications and subsystems will operate on CentOS 7 64-bit operating system except for PfSense server. The following diagram illustrates the system physical architecture:



Computing/server requirements on the following zones:

- Information Portal (Proxy);

Server Name	ACTS-Proxy_WebServer
Operating System	CentOS 7 64bit
CPU	4 cores
RAM	16 GB
Hard disk	300 GB
Ethernet ports	1 x 1 Gbps

- ACTS Applications Zone

Server Name	ACTS-MGR
Operating System	CentOS 7 64bit
CPU	4 cores
RAM	8 GB
Hard disk	300 GB
Ethernet ports	1 x 1 Gbps

Server Name	ACTS-Portal
Operating System	CentOS 7 64bit
CPU	8 cores
RAM	32 GB
Hard disk	300 GB
Ethernet ports	1 x 1 Gbps

Server Name	ACTS-App
Operating System	CentOS 7 64bit
CPU	8 cores
RAM	16 GB
Hard disk	300 GB
Ethernet ports	1 x 1 Gbps

- Application DB Zone

Server Name	ACTS-DB1
Operating System	CentOS 7 64bit
CPU	4 cores
RAM	16 GB
Hard disk	300 GB
Ethernet port	1 x 1 Gbps

Server Name	ACTS-DB2
Operating System	CentOS 7 64bit
CPU	4 cores
RAM	24 GB
Hard disk	300 GB
Ethernet port	1 x 1 Gbps

Server Name	ACTS-DB3
Operating System	CentOS 7 64bit
CPU	8 cores
RAM	32 GB
Hard disk	300 GB
Ethernet port	1 x 1 Gbps

- Demilitarized Zone (DMZ)

Server Name	ACTS-Pfsense_DMZPfsenseServer
Operating System	PfSense OS
CPU	2 cores
RAM	2 GB
Hard disk	300 GB
Ethernet port	2 x 1 Gbps

PfSense is a free open source firewall/router computer software distribution. It is installed on a computer to make a dedicated firewall/router for a network and is noted for its reliability and offering features often only found in expensive commercial firewalls. It can be configured and upgraded through a web-based interface. PfSense is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNS server, and as a VPN endpoint.

Specifically, for the Central Services Environment the following hardware performance requirements have to be met:

- CPU/Cores mentioned above are physical cores. When using virtualization technology, the same performance can be achieved either by setting configuration parameters for control core sharing to None on the virtual platform or alternatively by allocating 2x the Cores mentioned, i.e. 2 physical cores equal 4 virtual cores.
- MINIMUM recommended IOPS for the server's storage should be, on local disks ~800 IOPS, on SAN/NAS disks ~1800 IOPS.
- MAXIMUM recommended Latency for the server's storage should be, on local disks ~3 ms, and on SAN/NAS disks ~2 ms.
- MAXIMUM recommended Seek Time for the server's storage should be, on local disks ~0.2 ms, on SAN/NAS disks ~0.1 ms.

2.4 SERVICE LEVEL AGREEMENT (SLA)

The ACTS CS hosting service must deliver under following Service Level Agreement:

SLA Criteria	Description	SLA Target
Service availability	Availability of the CS hosting service	Minimum 99.5%
Operational	Operational time of the helpdesk	ASEAN normal working time operations, with 24/7 critical issues hotline

SLA Criteria	Description	SLA Target
Call response time	Time to acknowledge a Call	Maximum 2 working hours (1 hour critical call)
"Critical" problem resolution time	Time to resolve (repair) the problem and continue operation	Maximum 8 hours
"Critical" problem resolution update time	Time to give regular update on the "critical" problem	Every 1 hour until resolve
"Normal" problem resolution time	Time to resolve (repair) the problem	Maximum 4 working days
"Normal" problem resolution update time	Time to give regular update on the "normal" problem	Every 1 working day until resolve
"Low" problem resolution time	Time to resolve (repair) the problem	Maximum 14 working days
"Low" problem resolution update time	Time to give regular update on the "low" problem	Every 4 working days until resolve

Definition:

- Critical problem, faults that seriously impair or halt performance of the system, with concerns on the following conditions:
 - System, server or critical application down
 - The system is running, but with repeated interruptions
 - The user cannot make use of a 'must-have' business-essential function in the production system
 - The problem cannot be solved by a restart or a bypass or a workaround
- Normal problem, faults that affect productivity or development of the system, with concerns on the following conditions:
 - Problems which do not have a significant impact on current productivity
 - The production system is running, but with limitations
 - A function in the production system is failing, but there is a bypass available
- Low problem, minor faults which do not affect the use of the system and issues with low priority.

3. SCHEDULE

The following tentative schedule for delivery of the ACTS CS Hosting Service:

No.	Activities	Duration
1	Kick-off implementation meeting.	1 day
2	Assessment of ACTS CS System (if point 7 is required).	5 days
3	Installing and configuring the virtual servers of the ACTS CS (if point 7 is required).	10 days
4	Relocation/Migration from the existing hosting provider including testing (if required).	20 days
5	Delivery of the ACTS CS Hosting service.	Based on the contract period



ANNEX I

DATA CENTER SPECIFICATION

A data center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. It secures the installed servers and components in use, protects them from external dangers, and provides the infrastructure required for continued reliable operation. The physical structure provides protection against unauthorized access, fire and natural disasters. The necessary power supply and climate control ensure reliability.

Accurate planning as well as sustainable operation of a modern data center are steps companies need to take to meet the network security standards requirements. The enormous infrastructural requirements involved lead many companies to opt for an external supplier and outsource their data center needs.

In April 2005, the TIA responded with the TIA-942 Telecommunications Infrastructure Standards for Data Centers, the first standard to specifically address data center infrastructure. Intended for use by data center designers early in the building development process, TIA-942 encompasses site space and layout, cabling infrastructure, tiered reliability, and environmental considerations.

a. Tier-I: Basic Data Center Site Infrastructure

A Tier-I site is a basic data center, with non-redundant capacity components (e.g. generator, UPS, or chiller) and a non-redundant electrical distribution path serving the computer equipment. A Tier-I site is also required to have a minimum of twelve hours of fuel storage for onsite generation in the event of utility loss. A Tier-I data center is a significant step up from a server room or IT closet, which may not have generators, UPS, or other common data center equipment.

b. Tier-II: Redundant Data Center Site Infrastructure Capacity Components

A Tier-II site builds upon the requirements of a Tier-I site and adds redundancy to capacity components, such as adding an additional UPS (either an extra UPS in a module-redundant configuration or an extra UPS in a UPS-redundant configuration), or by including redundant CRACs beyond what is required to cool the load. These redundant capacity components will avoid some outages and speed service restoration in other outages compared to a Tier-I site.

A Tier II data center has redundant capacity components (N+1) and single non-redundant distribution path for power and cooling distribution and 30 % raised floors are required.

c. Tier-III: Concurrently Maintainable Data Center Site Infrastructure

A Tier-III site builds upon the requirements of a Tier-II site and adds multiple independent electrical and cooling distribution paths serving the computer equipment. All computer equipment must have multiple power sources, either through multiple power supplies or front-

ended by a static switch connected to different UPSs. The key requirement for a Tier-III site is that each and every capacity component and element in the distribution paths can be removed for service on a planned basis without impacting any of the computer equipment (servers housing inside the data center). This is critical because no computer equipment outage is required to perform infrastructure maintenance.

d. Tier-IV: Fault Tolerant Data Center Site Infrastructure

A Tier-IV site builds upon Tier-III and in addition requires that multiple distribution paths must be active at all times, the distribution paths must be physically isolated from one another (compartmentalization), and that cooling must always be available - even in the event of a loss of utility or other failure. The key added value from a Tier-IV site is that a single failure of any capacity system, capacity component, or distribution element will not impact the computer equipment, and that the system is automated to respond to a failure in the system.

TIA-942 is the comprehensive Data Centre standard that has been developed by the Telecom Industry Association, USA, and is the most widely recognized Data Centre standard in the world.

The American standard is currently the most comprehensive body of standards for data centers. Not only is cabling described, but also the entire data center among other things, the data center is divided up into so-called “tiers”, or different classes of availability. The data center must satisfy specific requirements for each class in order to guarantee availability.

TIA-942 Requirements

Tier requirements	Tier-I	Tier-II	Tier-III	Tier-IV
Distribution paths and power and cooling	1	1	1 active / 1 alternate	2 active
Redundancy active Components	N	N+1	N+1	2N+1
Support space to raised floor ration	20 %	30%	80-90%	100%
Raised floors	12 inches	18 inches	30-36 inches	30-36 inches
Floor Loading	85	100	150	150+
Initial build out per Cabinet	<1 kW	1-2 kW	1-2 kW	1-3 kW
Ultimate kW / Cabinet (typical)	<1 kW	1-2 kW	>3 kW	>4kW
Utility Voltage	208, 480	208, 480	12-15kV	12-15kV
Annual site down time	28.8 hours	22 hours	1.6 hours	0.4 hours

Concurrently Maintainable	No	No	Yes	Yes
SPOF (Single Points Of Failures)	Many + Human errors	Many + Human errors	Some + Human errors	Fire, EPO + Human errors
Staffing shifts	None	1 shift	1+shift	24 by forever
Staff / shift	None		1-2 / shift	2+ / shift
Availability	99.671%	99.749%	99.982%	99.995%

TIA-942 Standards

In terms of space needed to meet TIA-942 standards:

- Entrance Room (ER): the location for access provider equipment and demarcation points, as well as the interface with campus cabling and carrier entrance facilities
- Main Distribution Area (MDA): the location of main cross-connect (MC)
- Horizontal Distribution Area (HDA): the location of horizontal cross-connect (HC)
- Zone Distribution Area (ZDA): the location of zone outlet (ZO) or consolidation point (CP)
- Equipment Distribution Area (EDA): the location of equipment cabinets and racks

Ideally, separate rooms for each point listed above should be available for use, but this is not realistic and is often consolidated to defined areas. Careful planning is needed to upgrade the existing ASEC server room to TIER-III. For example, since the system is already setup and running, the service cannot be interrupted and the space is limited.

TIA-942 Average Space Layout

Data center type	Server cabinet	Server room	Small data center	Mid-size data center	Large data center
# of servers	4.8	19	150	600	6000
Total power	1.9 kW	11 kW	105 kW	550 kW	5,700 kW
Floor size	5 m ²	20 m ²	150 m ²	600 m ²	6,000 m ²

ANNEX 2

ISO/IEC 27002 (Information Security)

The majority of errors are due to human error – avoiding this requires implementation of IT governance in line with international recognized operational procedures such as ISO/IEC 27002.

The ISO/IEC 27002 catalog includes:

- Framework
- Acceptable Use of Information Technology Resources
- Information Security Definition & Terms
- Risk assessment
- Security policy – management direction
- Organization of information security – governance of information security
- Asset management – inventory and classification of information assets
- Human resources security – security aspects for employees joining, moving and leaving an organization
- Physical and environmental security – protection of the computer facilities
- Communications and operations management – management of technical security controls in systems and networks
- Access control – restriction of access rights to networks, systems, applications, functions and data
- Information systems acquisition, development and maintenance – building security into applications
- Information security incident management – anticipating and responding appropriately to information security breaches
- Business continuity management – protecting, maintaining and recovering business-critical processes and systems
- Compliance – ensuring conformance with information security policies, standards, laws and regulations

The information security controls clearly defined within ISO/IEC 27002 are generally regarded as the best practice means of operational procedures. Some typical examples found in the catalog are as follows¹:

1. Physical and Environmental security

- Physical access to premises and support infrastructure (communications, power, air conditioning etc.) must be monitored and restricted to prevent, detect and minimize the effects of unauthorized and inappropriate access, tampering, vandalism, criminal damage, theft etc.
- The list of people authorized to access secure areas must be reviewed and approved periodically (at least once a year) by Administration or Physical Security Department, and crosschecked by their departmental managers.

¹ **Note:** these examples are merely an illustration.

- Photography or video recording is forbidden inside Restricted Areas without prior permission from the designated authority.
- Suitable video surveillance cameras must be located at all entrances and exits to the premises and other strategic points such as Restricted Areas, recorded and stored for at least one month, and monitored around the clock by trained personnel.
- Access cards permitting time-limited access to general and/or specific areas may be provided to trainees, vendors, consultants, third parties and other personnel who have been identified, authenticated, and authorized to access those areas.
- Other than in public areas such as the reception foyer, and private areas such as rest rooms, visitors should be escorted at all times by an employee while on the premises.
- The date and time of entry and departure of visitors along with the purpose of visits must be recorded in a register maintained and controlled by Site Security or Reception.
- Everyone on site (employees and visitors) must wear and display their valid, issued pass at all times, and must present their pass for inspection on request by a manager, security guard or concerned employee.
- Access control systems must themselves be adequately secured against unauthorized/inappropriate access and other compromises.
- Fire/evacuation drills must be conducted periodically (at least once a year).

2. Human Resource security

- All employees must be screened prior to employment, including identity verification using a passport or similar photo ID and at least two satisfactory professional references. Additional checks are required for employees taking up trusted positions.
- All employees must formally accept a binding confidentiality or non-disclosure agreement concerning personal and proprietary information provided to or generated by them in the course of employment.
- Human Resources department must inform Administration, Finance and Operations when an employee is taken on, transferred, resigns, is suspended or released on long-term leave, or their employment is terminated.
- Upon receiving notification from HR that an employee's status has changed, Administration must update their physical access rights and IT Security Administration must update their logical access rights accordingly.
- An employee's manager must ensure that all access cards, keys, IT equipment, storage media and other valuable corporate assets are returned by the employee on or before their last day of employment

3. Access control

- Users of corporate IT systems, networks, applications and information must be individually identified and authenticated.

- User access to corporate IT systems, networks, applications and information must be controlled in accordance with access requirements specified by the relevant Information Asset Owners, normally according to the user's role.
- Generic or test IDs must not be created or enabled on production systems unless specifically authorized by the relevant Information Asset Owners.
- After a predefined number of unsuccessful logon attempts, security log entries and (where appropriate) security alerts must be generated and user accounts must be locked out as required by the relevant Information Asset Owners.
- Passwords or pass phrases must be lengthy and complex, consisting of a mix of letters, numerals and special characters that would be difficult to guess.
- Passwords or pass phrases must not be written down or stored in readable format.
- Authentication information such as passwords, security logs, security configurations and so forth must be adequately secured against unauthorized or inappropriate access, modification, corruption or loss.
- Privileged access rights typically required to administer, configure, manage, secure and monitor IT systems must be reviewed periodically (at least twice a year) by Information Security and cross-checked by the appropriate departmental managers.
- Users must either log off or password-lock their sessions before leaving them unattended.
- Password-protected screensavers with an inactivity timeout of no more than 10 minutes must be enabled on all workstations/PCs.
- Write access to removable media (USB drives, CD/DVD writers etc.) must be disabled on all desktops unless specifically authorized for legitimate business reasons.

a. PROPOSAL SUBMISSION INSTRUCTION

- a. All proposals must be submitted in English.
- b. **Vendors should not include any financial/cost data in the Technical Proposal, but only in the separate envelope titled Financial Proposal. Failure to adhere to this will lead to disqualification.**
- c. The proposal should be concisely presented and structured, and should explain in detail the Vendor's availability, experience and resources to provide the requested services.
- d. Proposals must be submitted by the Closing Date and Time, as indicated in the RFP.
- e. Proposals that are incomplete or do not address the required criteria may not be considered in the review process.
- f. All communications with regard to this RFP shall be in writing and send to:

Procurement Unit
Administration and General Affairs Division
ASEAN Secretariat
Email : procurement@asean.org

4.2. CLOSING DATE AND TIME OF SUBMISSION OF PROPOSALS

All proposals must be submitted not later than **Friday, 27 January 2023** by following options:

2.2.1 HARDCOPY

The Technical and Finance Proposals must be submitted separately in two different envelopes, in two sets i.e. original and a copy, to the following address:

Chairman of Sub-Committee on Tender
Administration and General Affairs Division
The ASEAN Secretariat
JI Sisingamangaraja No.70A
Kebayoran Baru
Jakarta 12110
Indonesia

Compliance

In conformance to the ASEAN Secretariat's Financial Rules and Procedures (AFRP), the vendor shall submit Tender Bids in **two** sealed envelopes as follows:

1) **First Envelope (Technical Proposal):**

a. **Technical Proposals (original and copy)**

First Set, which shall consist, among others, of the technical specifications of the services to be procured; delivery schedule; manpower requirements; printed hardcopies of the duly filled Appendix 1 and 1a - Company General Information and Customer Reference; Appendix 2 – Technical Requirement and completed Compliance Checklist as per Appendix 4;

b. **Second Set**, which shall consist, among others, the company profile; business name registration issued by appropriate government agency; authority of signatory; valid business permit and other appropriate licenses; taxpayer identification number; latest audited financial statements;

2) **Second Envelope (Financial Proposal):**

Financial Proposal (original and copy) which shall consist of among others the bid amount; payments schedule; etc; duly filled Appendix 3 – **Price**

Any notices with respect to this RFP should also be mailed to the above contact and address.

All documents not submitted in English shall not be considered and quoted price in the hardcopy submission shall be in **IDR for local bidders and USD for international bidders**.

The ASEAN Secretariat may, after the closing date, request additional information or clarification of tenders in writing.

2.2.2 SOFTCOPY

The Technical and Financial proposals shall be sent separately to the following email address:

Chairman of Sub-Committee on Tender
Administration and General Affairs Division
Email: procurement@asean.org

Compliance

The softcopy of Technical and Financial proposals must be sent **separately** protected by a **different password** for each proposal in encrypted format of PDF/ZIP file.

1. **Technical Proposals;**

a. **First set;** which shall consist, among others, of the technical specifications of the services to be procured; delivery schedule; manpower requirements; printed hardcopies of the duly filled Appendix 1 and 1a - Company General Information and Customer Reference; Appendix 2 – Technical Requirement and completed Compliance Checklist as per Appendix 4;

b. **Second Set;** which shall consist, among others, the company profile; business name registration issued by appropriate government agency; authority of signatory; valid business permit and other appropriate licenses; taxpayer identification number; latest audited financial statements;

2. **Financial Proposal:**

Financial Proposal which shall consist of among others the bid amount; payments schedule; etc; duly filled Appendix 3 – **Price**

All documents not submitted in English shall not be considered and quoted price in the softcopy submission shall be in ***IDR for local bidders and USD for international bidders.***

3. **Do not mention the password in body email.**

4. Inform the password only when the Procurement staff contact you to request it.

4.3. ***RFP terms & conditions***

4.3.1. **Bid Expiration Date**

*Received tender proposals shall be valid until **14 March 2023***

4.3.2. **Implementation/Delivery Schedule**

As stated in the Term of Reference

4.3.3 **Pre-Bid Meeting**

No Pre-Bid Meeting is scheduled, for any inquiries related to the RFP, please write to procurement@asean.org.

The ASEAN Secretariat may, after the closing date, request additional information or clarification of tenders in writing.

Appendix 1
Company General Information
*To be submitted together in the **Technical Proposal***

Company LEGAL Name:			
Division or Subsidiary (if applicable):			
Company Address:			
City:			
Province / State:			
Country:			
Postal Code:			
Telephone:			
Business Name Registration:			
Tax Registration Number:			
Valid Business Permit:			
Company Contact:		Telephone no.:	
Title / Position:		Fax no.:	
E-Mail:			
Indicate number of years involved in similar business			
Are you a subsidiary of a financial institution? *If Yes, Please indicate your Holding Company			

Appendix 1a.
Customer Reference
*To be submitted together in the **Technical Proposal***

Customer Details	
Company name	
Company address	
Telephone number	
Fax number	
Contact name	
Email address	
Project title	

Customer Details	
Company name	
Company address	
Telephone number	
Fax number	
Contact bame	
Email address	
Project title	

Customer Details	
Company name	
Company address	
Telephone number	
Fax number	
Contact name	
Email address	
Project Title	

APPENDIX 2
Technical Requirements
To be submitted in the *Technical Proposal*

1. Referring to the table from **Chapter 2.1** “TECHNICAL EXPERIENCE AND QUALIFICATIONS REQUIREMENTS” of the ToR, please fill in your compliance status (“Comply or “Not Comply”) for each of the items mentioned.
2. Referring to the table from **Chapter 2.2** “TECHNICAL SCOPE OF WORK” of the ToR, please fill in your compliance status (“Comply or “Not Comply”) for each of the items mentioned.
3. Referring to Points 1 and 2 above, please attach all of the related documents (CVs, Experience, Certifications) to support compliance claims.
4. Provide planning for *Migration Service* to migrate the existing web-based applications from the current hosting provider by ensuring minimal downtime during the migration through proper planning and execution.

APPENDIX 3
Price
*To be submitted in the **Financial Proposal***

No.	Description	Unit	Price