Annex A

Terms of Reference

for

IMPLEMENTATION AND MANAGEMENT OF GOVERNMENT INFORMATION AND PROCESS EXCHANGE (GIPX) - ICTA/GOSL/CON/QBS/2017/05

1. Introduction;

Single Window

ICTA intends to establish single window portals for identified domains, in order to improve connected governmental services offered by respective organizations having associated functions. In this regard ICTA intends to prioritize trade and social welfare single window portals.

In order to establish the infrastructure for "Single window" concept, it is required to implement several new components as well as to improve existing infrastructure. In view of the above, it is proposed to improve the Lanka Gate middleware infrastructure, in particular, the Lanka Interoperability Exchange (LIX) component of Lanka Gate.

The proposed infrastructure shall be improved to function as an information and process exchange (GIPx) facilitating data communication among government organizations. At the same time the above improvement shall facilitate the data communication and process mapping required to implement "Single Window" for multiple domains.

2. Background;

Lanka Gate

'Lanka Gate' is a Service Oriented Architecture (SOA) based messaging infrastructure, which is the gateway for electronic information and electronic delivery in Sri Lanka. It is envisioned by the e-Sri Lanka initiative, and also stated in the e-Government Policy Document approved by the Cabinet of Ministers, that practically all the electronic services (eServices) and electronic information in Sri Lanka will be delivered via Lanka Gate.

Lanka Gate was launched in 30th December 2009, along with the first e-Government transactional eService i.e. online issuance of Revenue License (e-RL). Since then ICTA has been working in collaboration with key government organizations and has launched nearly 50 eServices by now.

Please Refer *Annex A.1* of the TOR for a high level view of Lanka Gate and core components.

3. Concise statement of the objectives;

ICTA intends to procure and obtain the services of a consultant firm to implement and manage the proposed government information and process exchange (GIPx) middleware infrastructure.

4. Scope of Work;

Implementation of GIPx

4.1. Review and understand the overall architecture & design of the Lanka Gate initiative as described by *Annexure.A.1.*

4.2. Conduct a requirement study and get a clear understanding about the project requirement.

4.3. Carryout detailed discussions with the internal stakeholders in order for outlining the concept of the proposed GIPx middleware platform which facilitate the single window concept.

4.4. Review and understand the proposed high-level architecture of GIPx.
Refer *Annexure A.2*.

4.5. Develop the proposed architecture and the detailed design of GIPx, vendor should seek the approval from ICTA .

4.6. Conduct independent reviews of core applications and other related components, which are required to implement the proposed GIPx design, and provide reports in order for ICTA to procure the production support.

4.7. Document and obtain approval for the concept and its key functionalities.

4.8. ICTA prefers to have the solution with JavaScript, if there is a greater benefits vendor can propose a different language or technology.

4.9. Consultant can propose open source solution or licensing model where applicable.

4.10. The proposed design should adhere to the non-functional requirements specified in *Annex A.3*.

4.11. Ensure following among others are facilitated by the proposed design;

a. Facilitate single window concept.
b. Ensure the proposed design complies with open standards, SOA concepts and other enterprise level design principles.
c. Facilitate all the requirements related configurations associated with a national level middleware infrastructure.
d. Ensure Interoperability standards are adhered to.
e. Ensure integration with existing middleware such as Lanka Gate, and proposed new middleware components are duly considered.
f. The proposed GIPx design should facilitate among others, high –available and high performance.

4.12. Implement the approved technical designs of GIPx.

4.13. The proposed infrastructure needs to be established either at Lanka Government Cloud (LGC) or alternative cloud environment – IaaS.

4.14. Carryout any data migration where applicable.

4.15. Conduct comprehensive quality assurance tests.
4.16. Work in collaboration with internal and external technical teams and stakeholders to ensure the proposed GIPx deployment is successful.
4.17. Provide fullest support during the IS Audit of the infrastructure, and ensure the proposed GIPx is compliant.
4.18. Adhere to project management and reporting requirements of ICTA.
4.19. If required ICTA may choose to engage third-party SQA audit teams. In which case the consultant should provide the necessary artifacts and support, in consistent with the deliverables specified.
4.20. Should participate for weekly progress meetings, design meetings and related discussions.
4.21. Should provide the required deliverables in a timely manner.
4.22. Obtain user acceptance (UAT) prior to moving into production.
4.23. Maintain project source code in the ICTA Source Code Management system (SCM).
4.24. The consultant team members are required to sign an NDA.

Management of GIPx - Support and Maintenance:

4.25. Manage the GIPx middleware infrastructure in compliance with the Service Levels indicated in *Annex A.4.*
4.26. Collaboratively work with infrastructure and other vendors to resolve infrastructure related application issues.
4.27. Where applicable, assist troubleshooting of issues associated with applications, which may leverage GIPx. This may include Single window applications / components.
4.28. Regularly maintain project source code in the ICTA SCM.
4.29. Maintain all issues in the Issue tracking system maintained by ICTA.
4.30. Participate for Project Review Committee meetings.
4.31. Work collaboratively with ICTA stakeholders throughout the tenure of the project.
4.32. GIPx middleware software Support and Maintenance
    a. Apply critical patches and security updates
    b. Monitoring and reporting on software performance
4.33. GIPx Core Applications Software Support and Maintenance
    a. Core applications integration exercise
    b. Apply fixes for critical issues and security issues
    c. Monitoring and reporting on software performance
4.34. GIPx Operation Support and Maintenance
    a. Integrate eServices
    b. Enhance performance (if any) and /or load balancing
    c. Fix identified general issues and changes.

5. Deliverables and time line and payment schedule;

The Consultancy firm will be engaged for a period of 17 months.

The GIPx needs to be established within 5-month time period, and upon obtaining UAT acceptance and launched in to production, should manage the infrastructure for a period of 12 months.

a) Implementation of GIPx

No	**Deliverables**	**Duration**	**Deliverables Submission**
5.1	Successful acceptance of the following; 5.1.1 Proposed detailed work plan including the work schedule.	2 weeks	Effective date + 2 weeks
5.2	Successful acceptance of the following; 5.2.1 System Requirement Specification (SRS) 5.2.2 Implementing schedule 5.2.3 Quality Assurance Plan 5.2.4 QA Test cases 5.2.5 Acceptance criteria for Deliverables, UAT	4 week	Effective date + 6 weeks
5.3	Successful acceptance of the following; 5.3.1 Detailed System Technical Design (DSTD) including related integrations.	2 weeks	Effective date + 8 weeks
5.4	Successful acceptance of the following; 5.4.1 Proper maintenance of Source codes and related artifacts in the SVN and CMS.	12 weeks	Effective date + 20 weeks
5.5	Successful acceptance of the following; 5.5.1 Solutions installation guide 5.5.2 User manual 5.5.3 QA Status Report 5.5.4 UAT acceptance certificate.	4 weeks	Effective date + 24 weeks

b) Management of GIPx

No	Deliverables	Duration	Deliverables Submission
5.6	Successful acceptance of the following; 5.6.1 Monthly monitoring and performance report for the middleware and core applications. 5.6.2 Monthly critical patches and security updates where applicable 5.6.3 SCM Report	1 month	Monthly, during the 12-month Support and Maintenance period

- Payments will be released quarterly upon successfully competition of section no 5.6

6. Services and Facilities Provided by ICTA

6.1 Documents relevant to the Lanka Gate Components;
6.2 Web-based access to the ICTA SCM (Software Configuration Management) system
6.3 Access to staging/ production servers
6.4 Issue Tracking System
6.5 Project Technical Audit dashboard

7. Review Committees and Review Procedures

Deliverables shall be reviewed by the team appointed by ICTA

Annex A.1

THE LANKA GATE INITIATIVE
OVERALL ARCHITECTURE & DESIGN

1. Introduction to Lanka Gate

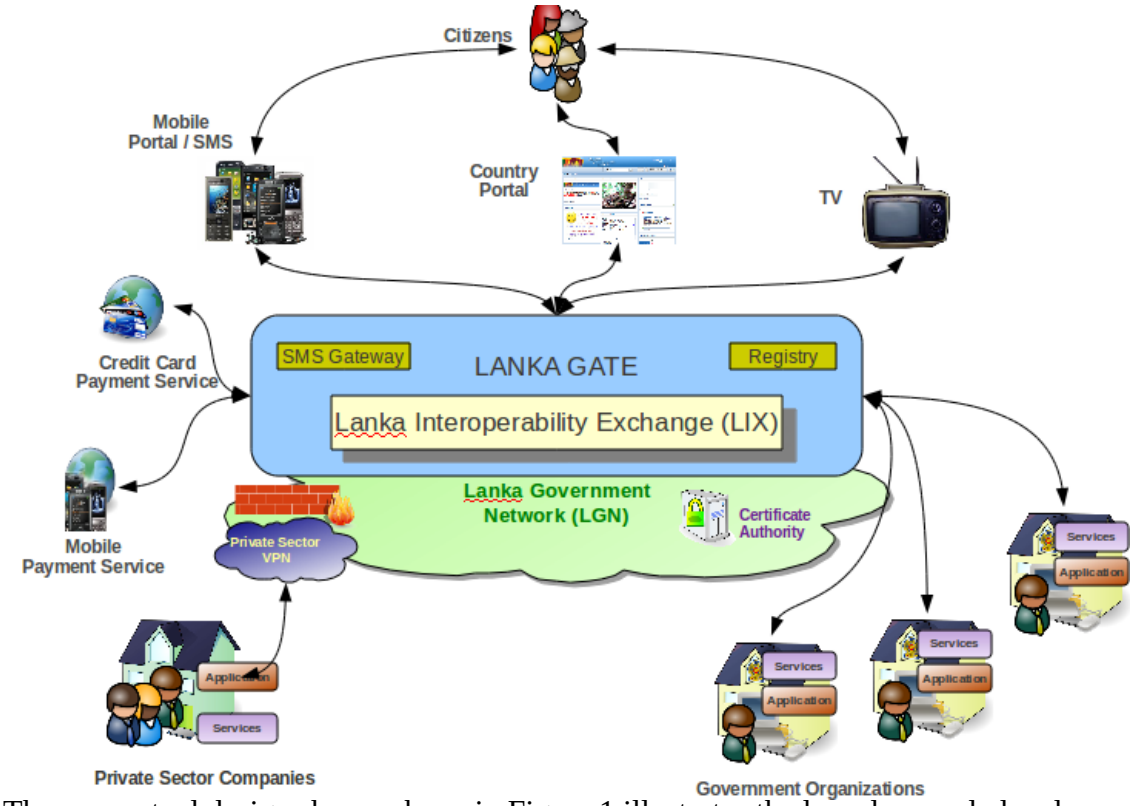
As an important component of the e-Sri Lanka initiative, it is envisioned that practically all the eServices and electronic information in Sri Lanka will be delivered via a comprehensive integration platform. This wide collection software infrastructure and systems which is envisioned to be the gateway for electronic information and electronic interactions in Sri Lanka, is generally referred to as the 'Lanka Gate' initiative.

Many eServices will be generated as a result of various projects done at the ICT Agency, such as the Population Registry project, the ePensions project and the Samurdhi Services project. In addition, many other eServices could be generated by government, public and private sector organizations as well as by community groups. Lanka Gate would include a comprehensive collection of infrastructural mechanisms to easily 'plug-in' an eService or to 'compose' a set of eServices in order to generate an composite eService, such that these eServices would be readily and easily available to other applications and portals that comprise Lanka Gate. For this purpose, it is envisioned that the projects within Lanka Gate would be designed to leverage Web 2.0 concepts, open standards and a Service Oriented Architecture (SOA), enabling dynamic, customizable, collaborative and compose-able services via multiple delivery channels.

Thus the collection of software systems that comprise Lanka Gate would collectively provide an *enabling infrastructure for rapid integration and delivery of eServices*, leveraging loosely-coupled architectural principles to encourage the creation of innovative applications, solutions, and business models, communication models, pricing models and service mash-ups by various stakeholders across the country.

The intention is that this architectural blueprint will guide the various software engineering projects that would eventually be integrated into Lanka Gate. Since Lanka Gate will always be in a state of flux with the continuous addition of eServices from new projects, removal of old eServices as well as the generation of new applications, portals or composite eServices via services mash-ups or services composition, it is hoped that this overall architectural blueprint would continue to 'live' as a vision of what the end result should embody. Furthermore, it is expected that the launch of the Lanka Gate initiative will be coupled with the roll-out of a strong SOA Governance Model.

2. Lanka Gate: The Core Components



The conceptual design shown above in Figure 1 illustrates the loosely-coupled and flexibility of the Lanka Gate infrastructure. It is composed of following core components.

2.1 Lanka Interoperability Exchange Project (LIX)

The Lanka Interoperability Exchange (LIX) delivers all the interconnectivity and discovery capabilities that services implemented by the various projects need, by facilitating message routing, transport management, transaction management, mediation, transformation, policy enforcement and service discovery. As an example, considering the eGovernment domain, the LIX would provide the fundamental capabilities necessary for government-wide services to efficiently achieve the vision of re-engineering government in Sri Lanka. Likewise, considering the eCommerce domain, the LIX would enable businesses to create revenue-generating models that would be able to innovatively utilize the infrastructural interconnection capabilities of the LIX to consume the eServices.

LIX is built on top of an Enterprise Service Bus (ESB). It therefore harnesses ESB capabilities such as routing, mediation, messaging, service orchestration and management of eServices and allows the use of a wide range of open protocols and open standards such as JMS, SMTP, XMPP, CORBA, REST and SOAP to connect existing and new systems/services.

In addition to providing message transport related services, the LIX also provides service discovery capabilities and features a collection of important authentication and authorization related eServices that would facilitate business & e-government transactions which require higher levels of security.

Thus the LIX and its associated protocols create an enabling framework that provides a secure, trusted channel through which government, public and private sector organizations may communicate and transfer information amongst each other. The LIX enables organizations to offload common functions such as authentication, authorization and payment, thereby allowing them to focus on business or domain specific functions. By providing such a shared infrastructure reduces the cost of implementation, enabling organizations to rapidly innovate and implement eServices that they otherwise may not even have considered. End users benefit from this shared infrastructure as it drives consistency in the way services are delivered compressing the user adoption and learning curves.

Conceptually, the capabilities offered by LIX are aligned with the enterprise computing notion of integration-as-a-service (IAAS) where businesses access a single hub that interconnects all trading partners, facilitated by SOA.

2.2 Country Portal (CP)

The Country Portal (srilanka.lk) serves as a primary web interface that connects users to the eServices provided within the Lanka Gate concept. Thus the Country Portal is a fundamental access point for citizens, non-citizens, businesses, agents and government employees to various government organizations and businesses in Sri Lanka. The Country Portal features multiple service delivery channels to accommodate various end user realities.

The Country Portal project basically contains a set of portlets which are self-contained front-end interfaces to either a single eService, several eServices from a specific project, or a transactional/mashup combination of eServices across several projects.
All the portlets should comply with JSR-168 portlet specification and it can host the portlets and provide necessary services as defined in JSR-168 specification including a unified user friendly interface and searching capability.

The web browser based delivery channel of the Country Portal features a highly user-friendly, dynamic interface, providing the end-user with the capability to design their own interactive user experience based on their particular needs and preferences. Most of the Web 2.0 capabilities available in Lanka Gate will be delivered through the web browser based delivery channel.

2.3 Mobile Portal (MP)

The Mobile Portal (mobile.icta.lk) the repository of mobile applications delivering useful government services utilizing the Lanka Gate infrastructure.

2.4 Credit Card On-line payment Services

A system to enable credit card payments for government enabled eServices, thereby facilitating electronic commerce for credit card holders.

2.5 Mobile Payment Services

A system to enable payment via a mobile phone for government enabled eServices, thereby facilitating electronic commerce for mobile phone users (This is yet to be integrated).

2.6 SMS Gateway (GovSMS)

A common interface open for mobile service providers to establish in-bound and out-bound Short Messaging Services (SMS) with Lanka Gate architecture. The mobile information and service gateway built as a part of Lanka Gate by ICTA to use the common, short telephone code "1919" should be used by all government organizations for delivery of such information and services.

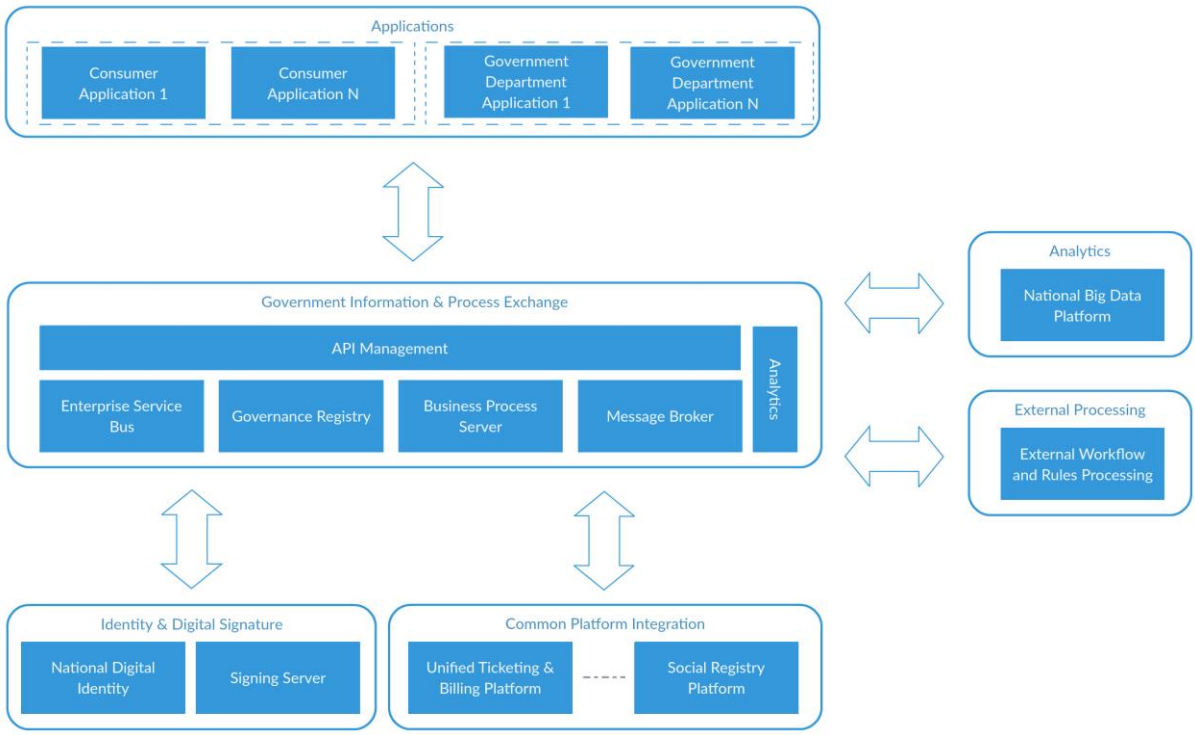
2.7 Service Registry

The service registry provides the infrastructure to define and manage meta data of the SOA in a well structured manner. Features such as, access control, version management, tagging, linking, searching, and notification, can be utilized in order to implement the "design-time SOA governance".

LIX uses this service registry as the configuration store as well as the policy store to read policy information associated to each of the service. This is in combination with the monitoring capability of the LIX to formulate the "runtime SOA governance".

Annex A.2

PROPOSED HIGH-LEVEL ARCHITECTURE
for
THE GOVERNMENT INFORMATION AND PROCESS EXCHANGE (GIPX)



1. Introduction

Government Information and Process Exchange (GIPx) is based on Service Oriented Architecture (SOA) to provide seamless integration with multiple parties to act as the common middleware platform for the whole of government. Above pictures depicts the core components and integrations of the GIPx which are described below.

2. Core Components

1. Government Information and Process Exchange (GIPx)
   - API Management – should facilitate managed API access, API lifecycle management, API governance and analysis with visualization for the ease of API management.
   - Enterprise Service Bus – should act as the common integration platform enabling interoperability among various heterogeneous systems to be integrated into GIPx.

- Governance Registry – should support metadata management with SOA governance.
- Business Process Server – should act as the business process manager which allows to define and manage business processes using BPMN, BPEL etc.
- Message Broker – should provide reliable messaging across the GIPx. It should support Publish/Subscribe model.
- Analytics – Should provide analytical information across the GIPx platform to get more insights and make decisions based on the provided information.

2. External Processing – For memory and process intensive workflow and rules will be executed in External Workflow and Rules Processing environment and the result will be taken back to GIPx. Based on the result rest of the operations can be carried out. In this manner smooth operation of GIPx can be ensured.
3. Analytics – The National Big Data Platform will provide computation and storage using a cloud-sourced, Hardtop solution where data can be analyzed and visualized effectively in a meaningful manner.
4. Identity and Digital Signature
    - National Digital Identity – The platform will provide biometrics based authentication and authorization for GIPx. It will also be used to provide Single-Sign-On (SSO). These functionalities will be provided as Representational state transfer (REST) APIs in order to be integrated.
    - Signing Server – This will allow to implement non-repudiation using digital signature.
5. Common Platform Integration – Any given platform should be integrated into GIPx using Representational state transfer (REST) API to communicate and exchange data which are required to execute to task at GIPx.
6. Applications - There can be two types of the applications which are consumer applications and government department applications where those will be communicating with GIPx using REST APIs provided.

Annex A.3

NON-FUNCTIONAL REQUIREMENTS

1. Security

1.1. User authentication and authorization

All eService web applications should be able to access via Lanka Gate and independently via respective department's web site. Any authorization requirement should be implemented within the specific eServices web application.

However the solution should have the provision to integrate with the Lanka Gate Identity Management solution in future.

An administrative application need to be developed wherever applicable.

Wherever applicable internal small applications need to be developed to capture and store relevant data.

1.2. Confidentiality and Integrity

All developed eServices Web applications/ back end e-services should ensure "confidentiality" and "integrity" whenever required by adhering to transport and message level security standards. (i.e. HTTPS, WS-Security)

1.3. Availability

All eServices Web applications / back end e-services should be developed to ensure "High Availability" to remain the system available all the time. (e.g. eServices Web applications clustering capability should be taken into consideration in the development)

1.4. Non-repudiation

All eServices Web applications / back end e-services should ensure non-repudiation by having standard audit-trails and provisions to have WS-Security using digital signatures.

2. Audit Facilities

Wherever applicable, an audit trail of all activities must be maintained. On a service or operation being initiated, the system should log the event, creating a basic 'audit log entry'. It should not be possible for the operation to be executed without the log entry being made.

The information recorded in the audit trail depends on the type of activity which takes place. Each service would be responsible for logging detailed information. The different types of operations are -

- Data Capture & Maintenance
- Creation of an entry / item
- Modification an item
- Deletion
- Control (or status change)
- Process execution
- Data synchronization
- Print (only selected item)
- Retrieval
- Monitor

Detail logging may be enabled or disabled for each type of operation, and/or for each business object. It should be possible to configure which attributes of a data item should be traced at the detail level. Tracing of some attributes may be considered mandatory, and they should not be turned off.

3. Backup and Contingency Planning

The main contingencies that should be considered and the training with regards to these shall be given to the relevant staff -

- Equipment failure
- Physical / natural Disaster
- Messaging or communication facilities.
- Changes in operations and policy
- Sudden absence of key personnel
- Breach in Security

Automatic Backups daily, weekly and monthly should be taken. All the backup procedures and backups needs to be tested regularly for restoration.

4. Performance

Following performance criteria is provided as a guideline only. If the actual performance is falling below the stipulated figures, the consultant is to justify the reasons. However, the performance level must be accepted by the technical evaluation committee appointed by the client.

The bandwidth is assumed at 512kbps (shared) (point to point between LIX and the Department web service) with 1,000 concurrent users (50% load factor) in total.

Item	Performance
Screen Navigation: field-to-field	< 10 milliseconds
Screen Navigation: screen-to-screen	< 5 seconds
Screen Refresh	< 3 seconds
Screen list box, combo box	< 3 seconds
Screen grid – 25 rows, 10 columns	< 5 seconds
Report preview – (all reports) – initial page view (if asynchronous)	< 60 seconds in most instances. It is understood that complicated / large volume reports may require a longer period
Simple enquiry – single table, 5 fields, 3 conditions – without screen rendering	< 5 seconds for 100,000 rows
Complex enquiry – multiple joined table (5), 10 fields, 3 conditions – without screen rendering	< 8 seconds for 100,000 rows
Server side validations / computations	< 10 milliseconds
Client side validations / computations	< 1 millisecond
Batch processing (if any) per 100 records	< 120 seconds
Login, authentication, and verification	< 3 seconds
Daily backups (@ Dept.) – max duration	1 hour (on-line preferred)
Total Restore (@Dept) – max duration	4 hours

Annex A.4

SERVICE LEVEL AGREEMENT

for

SUPPORT AND MAINTENANCE SERVICES

THE MANAGEMENT OF GOVERNMENT INFORMATION

AND PROCESS EXCHANGE (GIPX)

BETWEEN

INFORMATION AND COMMUNICATION TECHNOLOGY AGENCY OF SRI LANKA

AND

<Vendor>

Table of Contents

1. Introduction

The aim of this agreement is to provide a basis for close co-operation between the Consultant (name) and the Client (ICTA) for support and maintenance services to be provided by the Consultant, thereby ensuring a timely and efficient support service is available. The objectives of this agreement are detailed in section below.

This agreement is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

1.1. Objectives of Service Level Agreements

1. To create an environment conducive to a co-operative relationship between Client, Consultant and Client's representatives (government organizations) to ensure the effective support of all end users.
2. To document the responsibilities of all parties taking part in the Agreement.
3. To define the commencement of the agreement, its initial term and the provision for reviews.
4. To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
5. To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
6. To provide a common understanding of service requirements/capabilities and of the principles involved in the measurement of service levels.
7. To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

2. Definitions

PPS – Principle Period of Support

3. Service Level Monitoring

The success of Service Level Agreements (SLA) depends fundamentally on the ability to measure performance comprehensively and accurately so that credible and reliable information can be provided to customers and support areas on the service provided.

Service factors must be meaningful, measurable and monitored constantly. Consultant is supposed to provide relevant MIS reports to Client, on an agreed upon frequency. Actual levels of service are to be compared with agreed target levels on a regular basis by client.

Such MIS reports may include (but not limited to) the following:

- Uptime and availability of the systems with mentioned maintenance downtime (if any);
- SLA compliance reports;
- Consultant's Helpdesk report including details of each call, time of call, defects reported, time of call resolution, action taken, risk mitigation steps and lesson learnt;
- Helpdesk report of repetitive incidents;
- Incident reports leading to security violations or possible security threats;
- Contract compliance report indicates that the Consultant is not violating the terms of contract, statutory/ regulatory requirements to ensure & commit continued services as applicable

Additionally if Client requests any other relevant MIS reports Consultant should provide additional reports in a pre-specified format.

In the event of a discrepancy between actual and targeted service levels both Client and Consultant are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.

4. Agreed Level of Service

4.1 PPS Requirements

The Principal Period of Support (PPS) is considered in 2 categories as follows;

PPS category	Duration	Applicability
PPS1	From 08:00 AM to 09:00 PM, all days in the week (including public and mercantile holidays)	GIPx middleware infrastructure
PPS2	From 08:00 AM to 05:00 PM Monday to Friday (excluding public and mercantile holidays)	GIPx middleware infrastructure

Consultant MUST provide System Support and Maintenance Services during the above stipulated times.

The Consultant shall be liable to comply the SLA, to adhere to PPS1 during the first 6-months of the 1-year support and maintenance period.

The Consultant shall be liable to comply the SLA, to adhere to PPS2 during the second 6-months (7^{th} month to 12^{th} month) of the 1-year support and maintenance period.

Support and maintenance is effective from the date of successful launch and the duration is 12 months.

4.2 On-Call Services Requirements

Consultant MUST make at least ONE qualified personnel available to the Client by telephone and email for the reporting and resolution of non-conformities or other issues, defects or problems. Dedicated telephone numbers and emails should be available for reporting issues. Client will nominate the personnel who are authorized to report non-conformities or other problems with the system from the departments. Reporting of non-conformities includes requests by the Client to apply critical software updates or patches.

Table-1 shows the response priority assigned to faults according to the perceived importance of the reported situation and the required initial telephone response times for the individual priority ratings. All times indicated represent telephone response time during specified PPSs. The indicated telephone response time represents the maximum delay between a fault/request being reported and a Consultant's representative contacting the Client by telephone. The purpose of this telephone contact is to notify the Client of the receipt of the fault/request and provide the Client with details of the proposed action to be taken in respect of the particular fault/request.

	Business Critical	Non-Business Critical
Fatal	30 minutes	45 minutes
Impaired	45 minutes	90 minutes

Table-1: Response Priority

Note:

Fatal - Total system inoperability

Impaired - Partial system inoperability

Business Critical - Unable to perform core business functions

Non-Business Critical - Able to perform limited core business functions

Consultant notification can occur outside PPS time, and thus the response may occur after the next PPS begins. Furthermore, “Time to Attend” starts from PPS starting time.

5. Penalties

If service issues have not been corrected within two (2) hours of the initial contact, the Consultant shall send qualified maintenance personnel to the respective Client's site to take necessary actions to correct the issue reported (defect, problem or non-conformity).

If faults are not corrected within the time limits specified in the Table-2, the Client shall be entitled to a penalty payment for each hour that the Consultant fails to resolve the fault.

The total price of penalties shall not exceed 10% of the monthly service fee.

	Business Critical	**Non-Business Critical**
Fatal	6 Hours LKR 15,000.00	10 Hours LKR 8,000.00
Impaired	10 Hours LKR 8,000.00	15 Hours LKR 5,000.00

Table-2: Resolution Time and Penalties

6. Roles and Responsibilities

6.1 Consultant's Responsibilities

The key responsibilities of the Consultant should include
(but not limited to):

- The Consultant should nominate a single point of contact for Client. At the absence of primary contact there has to be a nominated secondary contact for easy reference of Client's. Further Consultant should maintain close coordination with Client to ensure continuity of expected operational levels.
- The Consultant shall follow Policies, Procedures and guidelines as suggested by Client.
- The Consultant should also support diagnosing the problems related to their service.

- The Consultant shall ensure proper handover/ takeover of documents & other relevant materials in the event of change in personnel-in-charge.
- All the internal review documents / reports used to monitor & execute the project should be shared with Client as & when desired.
- Consultant should not share any of information, contact details, user credentials, device configuration settings or any other confidential information with any third parties without Client's prior approval.

6.2 Client's Responsibilities

The key responsibilities of the Client should include but not limited to:

- Client should nominate a single point of contact for easy reference of Consultant's. At the absence of the primary contact, there has to be a nominated secondary contact.
- Client shall provide the required information such as site details, IP addresses etc.
- Client should clearly state the regulatory requirements, expected policies, procedures and guidelines for Consultant to operate.
- Client shall provide approvals & sign-offs to the deliverables within the stipulated time period.

7. Issue Management

- When either Consultant or Client faces a problem, that need to be recorded with sufficient information. Business or the technical issue to be detailed with the identified points of disagreements with possible solutions.
- Client may determine which executive level should be involved in issue resolution.
- The Client and the Consultant shall develop an interim solution, if required, until the permanent solution is in hand, subsequently. Client will then communicate the resolution to all interested parties.

8. Acceptance of Data Service Level Agreement

IN WITNESS WHEREOF, the parties hereto have caused this Service Level Agreement to be executed by their respective authorized representatives.

For and on behalf of:	For and on behalf of:
_____Service Provider	_____ICTA
Address: _____	Address: _____
Date: _____	Date: _____
Name:_____	Name_____
Title: _____	Title: _____
Office Seal: _____	Office Seal: _____

---------- End of Document ----------