Terms of Reference
for
Obtain services of a consultancy firm to revamp e-BMD system.

ICTA-SG2-GOSL-CON-QBS-2017-001

1. Introduction

The Register General's Department (RGD) which is operated under the Ministry of Home Affairs was initially established in 1864 with the purpose of registering lands and legal documents pertaining to properties. From 1867 onwards up to date this department is supposed to register Births, Marriages and Deaths of the Sri Lankan populace and thus operating with a view of safeguarding their fundamental rights.

While land registration processes are being carried out in 45 Land Registries that has been established on district level, the civil registration activities has been decentralized to all Divisional Secretariats (DSs) island wide.

The Government of Sri Lanka (GoSL) has recognized ICT as a tool, which the social integration, peace and growth can be fostered and the poverty could be reduced by the means of improving the reach and responsiveness of public services, to reduce transaction costs of businesses, making government more transparent, accountable and addressing the urgent needs of poverty - stricken communities and isolated regions.

2. Background

The Birth, Marriage and Death Certificates (BMD) are critical and essential for all important aspects in life such as education and employment. Specially, when a relief effort is required to be carried out after a disaster, the need to have a robust, secured and centralized consolidated citizen information system is essential. Therefore, Registrar General's Department with the technical assistance of ICT Agency of Sri Lanka (ICTA) developed eBMD system.

eBMD desktop application deployed at RGD head office and at DSs across the country is one of the core systems deployed in the department which enables servicing daily requests for BMD certificates from the general public.

3. Objective of the assignment

In order to overcome issues of the existing eBMD application in terms of its functionality, operability, performance, security, maintainability and various other factors, RGD has identified that a new web based solution is required. Thus, a system which would enable the smooth functioning of services offered through the existing features of the application as well as enable the department's vision of providing a superior service through new features identified is desired.

The project intends to study the requirement, design and develop the system, deploy and maintain the system. The consultant firm (Software development firm) is required to elicit or gather requirements from various sources, design, develop and implement the software, which will be delivered to RGD. The total duration of the assignment must comprise of time for requirements elicitation, design, development and final deployment including periodic user training and demonstrations.

4. Scope of the service

4.1 Conduct a system requirements study of the processes. Moreover, vendor should propose a solution to save the BMD certificates confidentially with increased integrity and availability.

4.2 On completing the above, a Detailed Software Requirements Specification (DSRS) and a Detailed Software Technical Design (DSTD) document should be submitted. Vendor should obtain approval from RGD for the DSRS and approval from ICTA for the DSTD respectively.

4.3 Test plan, test cases and UAT criteria should be submitted by vendor and approval should be obtained from ICTA.

4.4 Upon obtaining ICTA's & RGD's approval for the above, vendor should design and develop the system.

4.5 Obtain User Acceptance Test (UAT) for the implemented processes collaboratively with ICTA and RGD against the approved UAT criteria.

4.6 Maintain project source code in the ICTA Source Code Management (SCM) system and upload documents to the ICTA Document Management System (DMS).

4.7 Maintain all issues in the Issue tracking system maintained by ICTA.

4.8 Adopt a proper application release procedure to release the BMD system to ICTA during the deployment in the staging/ production environments at the could and server (configure and replicate the eBMD app to the server provided by RGD) environments provided by ICTA.

4.9 Participate for Project Review Committee meetings and Project Implementation Committee (PIC) Meetings as a member.

4.10 Provide support and maintenance services, from the date of launch to an agreed time period.

4.11 Adhere to the Service Level Agreement (SLA), during the support and maintenance phase indicated.

4.12 Adherence to Web 2.0 concepts, open standards and Service Oriented Architecture (SOA) principles.

4.13 Need to coordinate with a relevant service provider to conduct system vulnerability assessment and etc. (Relevant service provider should share the test script with ICTA).

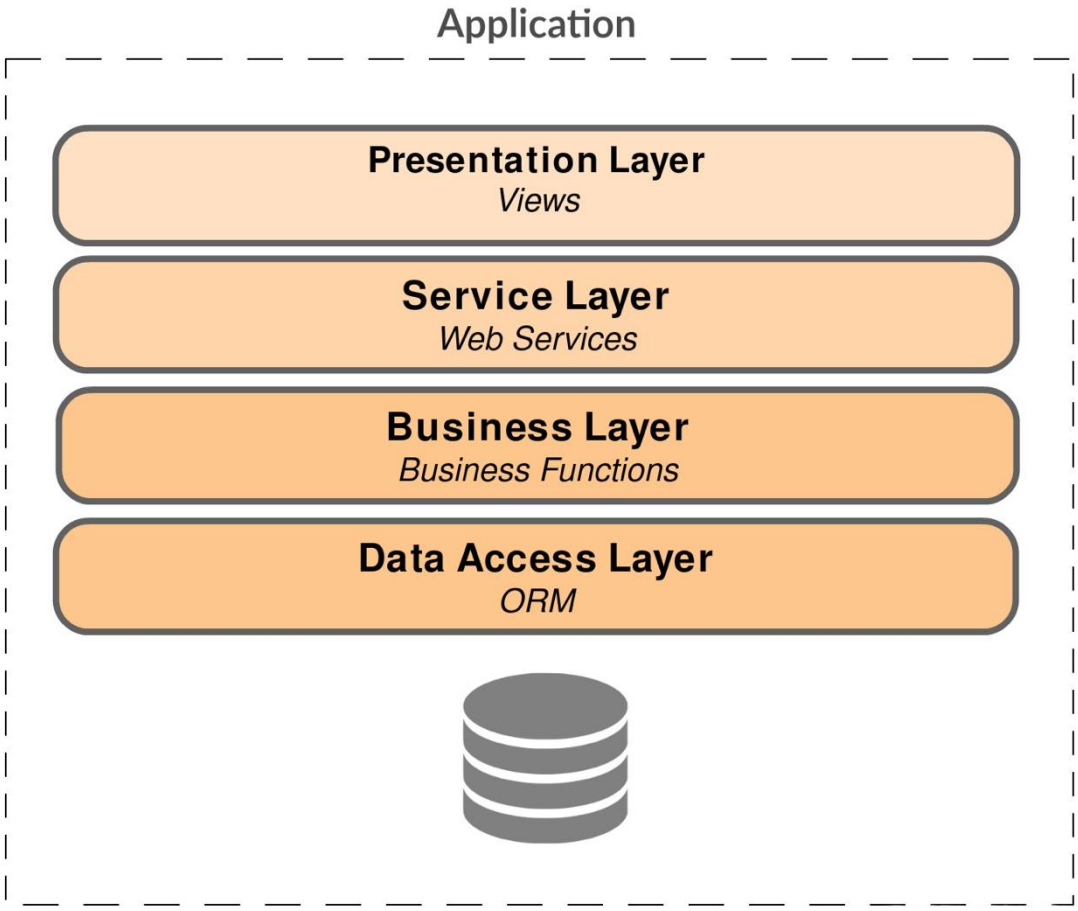

Figure 1: eBMD Layered Architecture Diagram.

4.14 Refer following Annexes which form a part and parcel of the Terms of References.

Annex 1 - Functional Requirements
Annex 2 - Non-Functional Requirements
Annex 3 - Transition Requirements
Annex 4 - Service Level Agreement for Support and Maintenance Services

5. Deliverables and timeline.

Consultancy firm is required to submit the following list of deliverables for the eBMD solution.

No	Deliverables	Phase	Duration
1	Successfully acceptance of following; Implementation Proposal 1.1 Implementation schedule / Project plan 1.2 Detailed Software Requirements Specification (DSRS) 1.3 Acceptance criteria for the UAT	Inception	Commencement + 3 Weeks

2	Successfully acceptance of following: 2.1 Design System Technical Documentation (DSTD) 2.2 Data migration and integration plan (if applicable) 2.3 Release Management plan (including staging, production and support and maintenance) 2.4 Proper maintenance of issues in the Issue tracking System 2.5 API documentation	Elaboration	Commencement + 3 Weeks
3	Successfully acceptance of following; 3.1 Proper maintenance of source code in SCM report 3.2 Proper maintenance of issues in the Issue tracking System	Construction	Commencement + 3 Weeks
4	Successfully acceptance of following; 4.1 Solutions deployment and installation guide 4.2 User Manual / Administrator Manual 4.3 Successful UAT acceptance of the system	Transition	Commencement + 3 Weeks
5	Successfully acceptance of following; 5.1 Monthly support and maintenance Report 5.2 Final S&M report should consist with comprehensive knowledge transfer documentation.	Transition	Date of launch +6 Months

Table 1: Deliverables and timeline.

6. Services and facilities provided by ICTA and RGD

6.1. Access to staging/ production environment.
6.2. Web-based access to the ICTA Source Code Management (SCM) system and Document Management System (DMS).
6.3. Access to Issue Tracking System.
6.4. Arranging meetings with stakeholders.

7. Review Committees and Review Procedures

All deliverables will be reviewed by the team appointed by ICTA.

-END-

[ANNEX 1]

FUNCTIONAL REQUIREMENTS

Module	Feature	Description
Admin Functionalities through a CMS	Manage new user profiles in the system	The admin user must be able to define the different user roles along with the login credentials to log in to the system. The admin user must be able to add, update, remove and view user roles defined in the system.
	Manage user privileges	The admin user must be able to add, update, remove and view the privileges assigned to each user role in terms of permissible functionalities (role based access control). User roles and privileges displayed should be specific to different departments (Eg: Police, Department of Immigration and etc).
	Manage master data in the system	The admin user must be able to add, update, remove and view the following key information in the system. • List of DS offices. • List of divisions within the DS. • List of certificate types. • Applicable rates for certificate copies. • Applicable rates for certificate search. • List of Additional District Registrars and their service duration respectively. • List of registrars.
	Certificate and data entry upload capability	The admin user must be able to scan and upload physical certificates in to the system as well as insert relevant certificate data. The uploading of image/images must be associated with capturing of certificate related information through manual data entry or uploading in bulk as an excel/ csv file.
	Reporting the issues	The Admin user must be able to report the issues identified in the certificates and the issues related to data entry (Eg: No image, image not clear and issues with data entry etc). Moreover, Admin user must be able to tag the relevant certificates (e.g.: Name changes and etc.). Super admin must be able to define and amend error types via CMS.
	Data classification	Elements of BMD certificates should be able to be customized when displaying (via UI) and exposing (via API) to stakeholders.
User Login		Birth, Death and Marriage certificates issued from any DS office across the 25 districts of Sri Lanka must be accessible through one single application. Thus the officer from RGD must be able to login to the web application by

		providing the username and password provided. The application must capture the RGD office (DS, district or head office) from which the user is logging in.
Request Management	Certificate request	The officer from RGD must be able to create a new request in the system with the details provided by the applicant in the application for certificate or search or registers. The application must contain key information as listed below. • Name of Applicant (mandatory) • NIC Number/ Passport Number/ Driving license • Applicant's postal address • Mobile number • Email address • District • Divisional Secretariat • Type of certificate requested (mandatory) → Birth, Death or Marriage • Date of registration • Number of certificates • Total amount payable Key information unique to Birth certificate • Fathers name • Mothers name Key information unique to Marriage certificate • Place where solemnized Key information unique to Death certificate • Fathers name • Mothers name A unique request number must be auto-generated from the system enabling tracking of the request. The requested date and time, along with the logged in user profile, logged in RGD office must be automatically captured and tagged to the request.
	Translation of Certificate request	The officer from RGD must be able to create a new request in the system to provide translation of BMD certificate with the details provided by the applicant and data within the system database.

		The application must contain key information as listed below. • Name of Applicant (mandatory) and postal address • NIC Number/ Passport Number/ Driving license • Applicant's postal address • Mobile number • Email address • District • Divisional Secretariat • Type of certificate requested (mandatory) → Birth, Death or Marriage • Number of certificates • Date of registration • Total amount payable A unique request number must be auto-generated from the system enabling tracking of the request. The requested date and time, along with the logged in user profile, logged in RGD office must be automatically captured and tagged to the request. (key information fields can be varied)
	Search certificate	The officer from RGD must be able to search for a certificate by providing the relevant search criteria. The applicable search criterion to search for birth, death and marriage certificates respectively is as listed below. <u>Birth Certificates</u> The RGD officer must be able to search for the certificate by the Name, Date of Birth / Date range, Certificate Number, Date of Registration, Mother's Name, Gender, Division or DS division or using any combination of the above criteria. <u>Death Certificates</u> The RGD officer must be able to search for the certificate by the Certificate Number, Date of Registration, Date of Death / Date range, Name, Division or DS division or using any combination of above criteria. <u>Marriage Certificates</u> The RGD officer must be able to search for the certificate by the Certificate Number, Type of Marriage, Name of male party, Name of female party, Name of marriage

		registrar, Date of marriage / Date range, Division or DS division or using any combination of the above criteria. • The user must be able to do a wild card search where the application must show suggestive search results when the user types in the search criteria. • The date search must facilitate exact search or search for records within a date range. • Combination of search criterion must further filter the search results allowing the user to narrow down to the required record quickly.
	View search results	The user must be able to view search results as a grid. The information to be displayed in the results list for each type of certificate search must be as follows. <u>Birth Certificates</u> Certificate Number, Date of Registration, Name, Date of Birth, Gender, Mother's Name, DS division, Division <u>Marriage Certificates</u> Certificate Number, Date of Registration, Type of Marriage, Name of male party, Name of female party, Name of marriage registrar, Date of Marriage, DS division, Division <u>Death Certificates</u> Certificate Number, Date of Registration, Name of person, Date of death, DS office, Division Note: When search does not return any results the user must be provided with a message indicating that the searched artefact is not available in the system advising the user to search for records where the event was recorded.
	Export search results	The RGD officer must be able to export the search results in to an MS Excel, PDF or MS Word format.
	Save, replicate and edit search	The RGD officer must be able to save a search for a certificate with a name where the search criteria must be saved (not the search result). The user must be able to easily select saved searches, modify the search criteria as required and execute as a fresh search which must display the appropriate search results as per the selected certificate category as described above.

	View certificate	The RGD officer must be able to select a certificate from the list and preview the certificate on screen. The user must be able to crop, zoom in, zoom out, rotate and navigate to the next pages of the certificate. The user should be able to print the certificates in A4 paper size (paper size can be varied).
	View applicable charges and update receipt of payment	The RGD officer must be able to enter the number of copies of the certificate required and view a breakdown of the applicable charges. The breakdown must include, • Charges for certificates • Charges for search • Total charges The RGD officer must be able to accept the payment from the applicant and update the receipt of the amount on the system. The capability to print the certificate must get enabled once the due amount has been paid.
	Print certificate	The RGD officer must be able to print the certificate and hand over the certificate to the applicant. The status must be updated as 'Issued'.
	Print receipt	Upon collection of charges and printing of the certificate, the RGD officer must also be able to print a receipt indicating the receipt of money. The information to be available in the receipt must be as per the receipt which is being used by the department.
System Logging		An audit trail of all the user actions performed on the application must be maintained. The information to be maintained includes, • User / user role • Date and Time • Module / Feature Accessed • Action Performed
Reports		1. Admin user must be able to generate a report on user activity on the system. The user must be able to filter the information by date / date range, DS office, user role etc. and the report must contain, a. Date and time b. DS office c. User Role d. Action Performed 2. The user must be able to generate a daily transactions report with details of certificates issued. The user must be able to filter information about the certificates

		issued by date / date range, DS office, Division, certificate type, etc. and the report must contain, a. Date and time b. DS office c. Division d. User e. Certificate Type 3. The user must be able to generate a summary report indicating the number of certificates issued of each type. The user must be able to filter the information by date or date range, DS office, Division and be able to see, a. Number of Birth certificates issued b. Number of Death certificates issued c. Number of Marriage certificates issued d. Total Number of certificates issued 4. The user must be able to view a summary of the charges obtained and the revenue generated by issuing certificates. Information to be displayed on the report includes, a. Date and time b. DS office c. Division d. Type of Certificate e. Charges for line item f. Sum total of all charges 5. The user must be able to generate a report on the issues reported. Information to be displayed on the report includes, a. Date b. DS office c. Division d. Type of Certificate e. Certificate no f. Reported Issue g. Incorporated Tags Up to 5 ad-hoc reports should be generated which will be decided on the requirement gathering. Viewing the reports should be role based.

Table 2: Functional Requirements.

[ANNEX 2]

NON - FUNCTIONAL REQUIREMENTS

1. Security

1.1. User Authentication and Authorization

All 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 web application.

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

An administrative application needs 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 Web applications 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 Web applications should be developed to ensure "High Availability" to make sure that the system remains available all the time (Eg: Web applications clustering capability should be taken into consideration in the development).

1.4. Non-repudiation

All Web applications should ensure non-repudiation by having standard audit-trails and provisions to have WS-Security using digital signatures.

1.5. OWASP Guidelines

All web applications should ensure that the OWASP guidelines for security are followed when designing, developing and deploying the web application.

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 detailed 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 must 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

5. Usability

The web application should be extremely usable, even a greenhorn user should be able to handle the system and incorporate all the functionality of the system in a simple and user friendly interface. The web application should be internationalized and localized if needed. The web application should be responsive where it should be viewable on any computing device.

6. Web Interoperability

The web application should be able to view in standard compatible web browsers.

7. Availability

The web application should be performed as follows,

- 99.99% available unless the web application is designed with expected downtime for activities such as database upgrades and backups.
- Hence to have high availability, the web application must have low downtime and low recovery time.

8. Robustness

The web application should be able to handle error conditions gracefully, without failure. This includes a tolerance of invalid data, software defects, and unexpected operating conditions.

9. Maintainability

The code of web application should be properly documented with appropriate comments and no complex codes (highly cohesive and loosely coupled) to do modifications such as corrections, improvements or adaption.

10. Reusability

The web application should be able to use of existing assets in some form with the software product development process. Assets are products and by-products of the software development life cycle and include code, software components, test suites, design and documentation.

11. Internationalization

The web application should be able to access in Sinhalese, English and Tamil. The web application should be able to view in a usable manner in all three languages.

12. API Management

12.1. API standards and best practices

API standards and best practices that should be adhered to the code.

12.2. API security

The web application should be used appropriate API security protocol mentioned below.

- Basic API authentication
    - Basic authentication should never be used without TLS (formally known as SSL) encryption as username and password combination can be easily decoded otherwise.
- OAuth1.0a
    - Uses cryptographic signature value that combines the token secret, nonce, and other request based information. Can be safely used without SSL.
    - Recommend for sensitive data applications
- OAuth2
    - No need to use cryptographic algorithms to create, generate and validate signatures as all the encryption handled by TLS.
    - Recommend for less sensitive data applications
- JWT (JSON Web Tokens)

13. Scalability

The application is expected to support storage and search of 35 million citizen certificates starting from way back as 1920. These numbers are expected to grow with the issuance of birth, death and marriage certificates on a daily basis. Thus the application must support secure storage and retrieval of the afore-mentioned magnitude of data.

14. Accessibility

The application must be accessible from the head office and from 331 DS offices across 25 districts across the country and must be accessible via the web. The application must be device independent and be accessible via any web browser.

15. Other

W3C standards should be followed where applicable.

[ANNEX 3]

TRANSITION REQUIREMENTS

The following are identified as capabilities to be in place in order to transition from the existing eBMD systems to a new web based solution.

1. Training

Necessary training on using the application must be provided through proper documentation of functionality as training manuals and through knowledge transfer sessions.

2. Data Migration

The 35 million (and growing) certificates and other relevant pieces of data are expected to be available / accessible through the new application. Thus migration from the current databases / servers may need to happen seamlessly through a phased out approach (i.e. parallel running of multiple databases). Staging and production servers should configure and manage by the the vendor.

BMD certificates which are currently encrypted needs to be decrypted by vendor when deploying and key will be provided by RGD.

[ANNEX 4]

SERVICE LEVEL AGREEMENT *for* SUPPORT AND MAINTENANCE SERVICES

(i) Introduction

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

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.

(ii) Objectives of Service Level Agreements

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

(iii) Principal Period of Support (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 07:00 PM Monday to Friday.	For the essential component applications and online payment service platform related departments.

Service Provider MUST assure System Support and Maintenance Services during the above stipulated times.

(iv) On-Call Services Requirements

Provider 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 Provider'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

Provider notification can occur outside PPS time, and thus the response may occur after the next PPS begins. Furthermore, "Time to Arrive On-Site (Table-3)" starts from PPS starting time and "Time to Resolve the Problem" is PPS time starting from the actual time of arrival on site.

(v) Problem Resolution and Penalties

If problems have not been corrected within two (2) hours of the initial contact, the Provider 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. Maximum ceiling of penalty for a given month is 10% of the invoice amount for the month.

	Business Critical	Non-Business Critical
Fatal	1 Hours LKR 12,000.00	2 Hours LKR 8,000.00
Impaired	2 Hours LKR 5,000.00	5 Hours LKR 3,000.00

Table-2: Resolution Time and Penalties

The time to arrive on-site is specified in the Table-3.

	Business Critical	Non-Business Critical
Fatal	2 Hours	3 Hours
Impaired	3 Hours	5 Hours

Table-3: Time to arrive on-site

(vi) Service Level Monitoring

The success of Service Level Agreements depends fundamentally on the ability to meet agreed service levels and effective measuring of performance, comprehensively and accurately so that reliable information is available for both parties in agreement. Thereby a clear understanding and effective communication can be maintained between the provider and customer.

Service factors must be meaningful, measurable and monitored constantly. Actual levels of service are to be compared with agreed target levels on a regular basis by both Client and Provider. In the event of a discrepancy between actual and targeted service levels both Client and Provider are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.

Compliance to SLA will be monitored via:

a. Completion of deliverables as per agreed time lines;
b. Accuracy, completeness and quality of the deliverable;
c. Issues resolution within the agreed upon time;
d. On call support within agreed upon time;

Service level monitoring will be mainly performed by Client. Provider may also monitor the level of compliance, for possible improvements. Reports will be produced as and when required and forwarded to the necessary parties.