Database
for
Domain Name Registration System
(DNRS)

Call for Tender
(Tender Ref.: CFT-DNRS-DB-01)

Version 1.0
Date: 18 July 2025

Hong Kong Internet Registration Corporation Limited

Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Tel.: +852 2319 1313 Fax: +852 2319 2626
Email: enquiry@hkirc.hk Website: www.hkirc.hk

IMPORTANT NOTICE

This communication contains information which is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any distribution, copying or use of this communication or the information in it is strictly prohibited. If you have received this communication in error, please notify the sender immediately and then destroy any copies of it.

Table of Contents

Summary 1
1. Definitions 2
2. About HKIRC 3
3. Background of the Project 4
4. The Required Services and System Functionalities 5
4.1. Part A – Provision of database licenses 5
4.2. Part B - Installation of database and implementation of database infrastructure 7
4.3. Part C – Data migration from current database to new database and system deployment 9
4.4. Part D – Database implementation, project management and documentation 10
4.5. Part E – Information security and data privacy protection 11
4.6. Part F – System maintenance and support 15
4.7. Part G – Training and skill transfer 17
5. Limitation of Liability and Indemnity 18
5.1. Service Level Agreement (SLA), Service Credits and Contract Termination 18
5.2. Project Management Methodology and Review Meeting 19
5.3. Intellectual Property Rights 19
5.4. Software Source Code Escrow 19
6. Information Security 19
7. Project Acceptance 20
8. Anti-collusion 20
9. Offering Advantages 21
10. Ethical Commitment 21
10.1. Prevention of bribery 21
10.2. Declaration of Interest 21
10.3. Handling of confidential information 22
10.4. Declaration of ethical commitment 23
11. Time Schedule 23
12. Payment Schedule 24
13. Elements of a Strong Tender 24
14. Service Agreement Negotiation and Signature 25
15. HKIRC Contacts 25
Appendix A – Warranty 26
Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements 29
Appendix C – HKIRC Proposal Requirements 31
1 Proposal Content 32

2 Cover Page 33
3 Executive Summary 34
4 Conflict of Interest Declaration 34
5 Company Background 34
6 Methodology 34
7 Project Management Methodology 35
8 Understanding of our requirements 35
9 Knowledge and Advices on Projects/Services 35
10 Deliverable and Services level 35
11 Proposed Costs of Service and Payment Schedule 35
12 Implementation Time Table 43
13 Commercial and Payment Terms 43
Appendix D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing 44
7. HUMAN RESOURCES SECURITY 44

Summary

Hong Kong Internet Registration Corporation Limited (HKIRC) is going to commission a Service Provider ("the Contractor") to provide and implement a database for the use of a system namely Domain Name Registration System (DNRS).

The scope of services and database functionalities is detailed in Section 4 of this document.

Parties interested in providing this service shall submit **Expression of Interest (EOI) by 23rd July 2025**. For those who have submitted EOI, they should **sign Non-disclosure Agreement (NDA) by 28th July 2025** and **proposal** (see Appendix C) to the Group **no later than 5:30pm on 8th August 2025 (Hong Kong time)**.

The Contractor should submit Tender Proposal by email to HKIRC contacts (refer to Appendix C - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix C, 2 Cover Page).

1. Definitions

The following terms are defined as in this section unless otherwise specified.

“The Contractor” and “The Service Provider” mean the company who will provide the Services after award of contract.

“HKIRC” means Hong Kong Internet Registration Corporation Limited.

“HKDNR” means Hong Kong Domain Name Registration Company Limited, a wholly-owned subsidiary of HKIRC, the company requesting the proposal for “The Services”.

“DNRS” and “The System” mean Domain Name Registration System. It consists of 2 major sub-systems, Registry System (for HKIRC) and Registrar System (for HKDNR).

“The Services” and “The Project” mean the provision and implementation of database according to the requirements stipulated in Section 4 of this document.

“CFT” means this Call for Tender.

“Tenderer” means the company who will submit proposal to provide the Services.

2. About HKIRC

Hong Kong Internet Registration Corporation Limited (HKIRC) is a non-profit-distributing and non-statutory corporation responsible for the administration of Internet domain names under '.hk' and '.香港' country-code top level domains. HKIRC provides registration services through its registrars and its wholly-owned subsidiary, Hong Kong Domain Name Registration Company Limited (HKDNR), for domain names ending with '.com.hk', '.org.hk', '.gov.hk', '.edu.hk', '.net.hk', '.idv.hk', '.公司.香港', '.組織.香港', '.政府.香港', '.教育.香港', '.網絡.香港', '.個人.香港'. '.hk' and '.香港'.

HKIRC endeavors to be:

- Cost-conscious but not profit-orientated
- Customer-orientated
- Non-discriminatory
- Efficient and effective
- Proactive and forward-looking

More information about HKIRC can be found at http://www.hkirc.hk .

HKIRC and HKDNR are listed as public bodies under the Prevention of Bribery Ordinance (Cap 201).

3. Background of the Project

The Domain Name Registration System (DNRS) was developed for the operations of HKIRC and HKDNR and is currently hosted in our on-premises data centres. In this Project, a database will be implemented for the System.

The DNRS is currently under system revamp, and the Service Provider has to work with the Application Developer of the system revamp to ensure the revamped DNRS working properly in the database and also complete and smooth data migration from the current database to the one proposed by the Service Provider.

We anticipate that the database solution will encompass, but not be limited to, the following functions and features to integrate with our revamped DNRS. These functions and features include multiple site Active-Active Cluster, Active-Standby Cluster, Distribution Database structure, Relational Database structure, Disaster Recovery Solution, ETL service for Report Servers, and data migration services, among others.
The proposed solution should not be restricted to a single brand of database. Instead, it should consider multiple database brands to ensure it can address various scenarios, particularly in handling critical infrastructure purchase constraints.

4. The Required Services and System Functionalities

The following defines the scope of service to be provided by the Contractor. The scope of service consists of the following parts, and the high-level requirements are stated below:-

- **Part A** – provision of database licenses
- **Part B** – installation of database and implementation of database
- **Part C** – data migration from current database to new database and system deployment
- **Part D** – database implementation services, project management and documentation
- **Part E** – information security and data privacy protection
- **Part F** – system maintenance and support
- **Part G** – training and skill transfer

Tenderers must provide quotation breakdown for each item in their proposals for our consideration. Please refer to **Section 11 Proposed Costs of Service and Payment Schedule** of **Appendix C – HKIRC Proposal Requirements** for the items and breakdown required. Tenderers' offers have to remain valid for at least 24 months from the tender closing date. HKIRC reserves the right to award the tender for any or none of the items; and accept partial, the whole proposal(s) or none submitted by Tenderer(s).

Due to the complexity of the Project and considerations in different aspects, HKIRC would purchase the necessary item(s), partially or wholly, at different stages of the Project; or not make any purchase eventually, at our sole and absolute discretion within the validity period of offer. If we accept your proposed solution, your offer of license maintenance and support/ professional services also need to remain valid for at least 5 years.

Bidders are advised to present various solutions with different combinations of licenses and Total Cost of Ownership (TCO). A trial or development license for DNRS revamp is essential and will be awarded additional points during the assessment.

4.1. Part A – Provision of database licenses

The DNRS consists of the following sub-systems, and each of those requires a database (or a sub-database if supporting multi-tenant feature):

1. Registry System
2. Registrar System
3. HKIRC Membership Registration System (MRS)

The sizing and future growth projection of the databases are as follows:

Item	Registry DB	Registrar DB	MRS DB	Total
Initial Estimated Size (2025)	400 GB	350 GB	140 GB	**~890 GB**
Future Growth (3–5 yrs, ~20%/year)	+300 GB	+250 GB	+100 GB	**+~650 GB**
Growth Buffer / Overhead	100 GB	80 GB	30 GB	**+210 GB**
Projected Total Storage (2028)	~800 GB	~680 GB	~270 GB	**~1.75 TB**
Recommended Storage Allocation (Raw)	1.0 TB	850 GB	400 GB	**~2.25 TB**
vCPU Allocation	4 Cores	4 Cores	2 Cores	**10 Cores**
RAM Allocation	64 GB	48 GB	32 GB	**144 GB**
DB Deployment Option	Physical or VM	Physical or VM	Physical or VM	
Storage Type	SSD	SSD	SSD	

There are multiple environments for the system development cycles, illustrated below. Service Providers have to propose sufficient licenses for all of those environments. Lower resilience can be tolerated for Non-Production environments.

Environment	Registry	Registrar	MRS
Development (DEV)	Applicable	Applicable	Applicable
User Acceptance Test (UAT)	Applicable	Applicable	Applicable
Operational Test and Evaluation (OTE)	Applicable	Applicable	
Production (PRD)	Applicable	Applicable	Applicable

Service Providers have to propose sufficient licenses for ALL the environments listed above and the features including but not limited to:

1. Resilience and load balancing:
    a. Local: Active-Active for Primary Site; For Secondary Site, both Active-Active and Single-Node would be considered
    b. Cross-site:
        i. Alternative 1: Active-Active
        ii. Alternative 2: Active-Standby

2. Data backup – hot backup
3. Data migration from current database to new database
4. Data synchronization between current database and new database
5. Database administration and client tools
6. Database encryption

Please observe the tentative time schedule stated in Section 11 Time Schedule, and the Service Provider would need to prepare for trial licenses and temporary licenses to meet the time schedule if necessary.

4.2. Part B - Installation of database and implementation of database infrastructure

The Service Provider has to provide the following services for this Project:

1. Installation of database
    a. Service Provider has to install the database instances for all the environments specified above, with the required sizing. The required hardware will be provided by HKIRC, but the Service Provider has to provide technical advice and support for the establishment of hardware infrastructure in order to support the operation of databases.
2. Implementation of database infrastructure
    a. Establishment of database infrastructure with resilience, load balancing, data synchronization (cross-site and/or with the current database), data backup.
    b. Technical support to Application Developer – Service Provider has to work closely with the Application Developer, HKIRC and our technical/ security consultant(s) for the implementation of database infrastructure to ensure the revamped DNRS working properly with the new database; smooth data migration from the current database; and complying with the security/ data privacy standards.
    c. Application Developer is responsible for the software development of the DNRS System Revamp, however, the Service Provider has to provide technical advice and support to the Application Developer and also HKIRC's Database Administrator (DBA) for making the revamped DNRS running properly with the new database.
    d. Disaster recovery (DR) drill(s) has/ have to be conducted to ensure the built database infrastructure can support load balancing, resilience, failover, data restore, etc. as per the design of database architecture.

e. Service Provider has to propose the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the 2 alternatives:
    i. Cross-site Active-Active, with local Active-Active
    ii. Cross-site Active-Standby, with local Active-Active

f. Installation of operating system (OS) – Service Provider has to install the operating system, with hardening and database-relevant setup, for supporting the running of database. Red Hat Enterprise Linux (8 or above) is recommended to apply. If Service Provider count-propose an operating system other than Red Hat Linux, the proposed OS must be comparable to Red Hat Linux Enterprise (8 or above) and comply with Center for Internet Security (CIS) Red Hat Enterprise Linux 8 Benchmark v3.0.0. Besides Service Provider has to include the support licenses of the proposed OS in their tender proposal.

4.3. Part C – Data migration from current database to new database and system deployment

The Service Provider has to provide the following services for this Project:

1. Data migration from the current database to new database
    a. The new database must support seamless data migration from the current database, up to the latest version released, currently using Pluggable Databases, to new database, including all the schemas, users, roles, privileges, etc.
    b. During the data migration, the operation of the current database cannot be interrupted or significantly degraded, i.e. no downtime incurred.
    c. Proven tool or mechanism must be provided to ensure the data integrity and completion of data migration.
    d. Proven tool or mechanism must be provided for converting the SQL statements, PL/SQL programs, data types, etc. from the current database's syntax to new database's syntax. Technical support and advice have also been provided to the Application Developer and HKIRC's DBA for converting program codes/ SQL scripts.
2. Data synchronization/ delta load from the current database to new database
    a. Other than initial load, the tool must support delta load, i.e. the data will be continuously synchronized from the current database to new database.
    b. Besides, a proposed solution has also be provided for backward data synchronization, i.e. after migration to the new database, the data has to be synchronized backward to the current database for fallback plan.
    c. Proven tool or mechanism must be provided to ensure the data integrity and completion of data synchronization.
    d. The new database might be used for data analytics and reporting, thus, it must support Online Analytical Processing (OLAP) and ready for data analytics and reporting.

4.4. Part D – Database implementation, project management and documentation

The Contractor shall carry out database implementation works, with proper documentation, and perform project management to ensure the Project is delivered within the planned project schedule and with acceptable quality and information security level:

#	Project Activities/ Deliverables	Documentation (by the Contractor)
1.	Project management • Project review meetings (at least once per month) • Ad-hoc project review meetings	• Project Implementation Plan (by phases, by timeline) • Data Migration Plan • Cut-Over and Go-Live Plan • Change Management Plan • Post-Go-Live Support Plan • All Meeting Agendas • Meeting Minutes • Weekly and/or Monthly project progress reports
2.	Project Initiation	• Project initiation document (PID) • Project Chapters
3.	System Architecture Design	• System Architecture Design
4.	Testing	• Test Plan, Test Scenarios
4.1.	Quality assurance (by the Contractor)	• Quality Assurance Report
4.2.	System integration testing	• Test cases, Test Scenarios
5.	Training	
5.1.	Database administration training	• Database administration manual
6.	Disaster recovery drill	• Disaster recovery plan and procedures
7.	Security Risk Assessment and Audit • The exercise will be conducted by a third-party service provider; and the vulnerabilities will be fixed by the Contractor	• SRAA report(s)
8.	Privacy Impact Assessment (PIA) • The exercise will be conducted by a third-party service provider; and the remedial actions will be implemented by the Contractor	• PIA report(s)

9.	System nursing	After new system goes on Production (go live) or ready to go live, system nursing period must be provided at least 6 months to support the entire system functions.

4.5. Part E – Information security and data privacy protection

Information security and data privacy are crucial to safeguard the digital assets of/ derived from the System. Security risk assessment and audit (SRAA), Red Team's penetration testing and Privacy impact assessment (PIA) will be conducted by a third-party service provider at different stages of the Project. The Contractor must collaborate with the security service provider for carrying out those exercises, and fix the identified vulnerabilities/ issues accordingly.

#	Requirements
1.	Security by design
1.1.	The approach of "security by design" has to be adopted throughout the entire system development life cycle. SRAA and PIA professionals would be involved in the system implementation works, i.e. starting from system analysis and design. The personal data protection must be compliant with the following prevailing regulatory requirements and/or ordinance including HK Cap. 486 Personal Data (Privacy) Ordinance, China's Personal Information Protection Law (PIPL), and EU General Data Protection Regulation (GDPR).
2.	Security risk assessment and audit (SRAA) (by a third-party service provider)
2.1.	A third-party security service provider will be recruited by HKIRC for the project. There will be at least 3 times of SRAA conducted for each sub-system (i.e. Register / Registrar System): • During system analysis and design • After user acceptance testing (i.e. pre-production) • After system live run (i.e. post-production) Additional SRAA exercise(s) might be required if there are significant concerns or findings raised in the previous exercise(s).
2.2.	Code scanning shall be conducted and the Contractor has to provide source code for this exercise.
3.	Red Team's penetration testing (by a third-party service provider)

#	Requirements
3.1.	A third-party security service provider will be recruited by HKIRC for the project. There will be at least 2 times of penetration testing (in either grey or white box approach) conducted for each sub-system (i.e. Register / Registrar System): • After user acceptance testing (i.e. pre-production) • After system live run (i.e. post-production)
4.	Privacy impact assessment (PIA) (by a third-party service provider)
4.1.	A third-party security service provider will be recruited by HKIRC for the project. There will be at least 3 times of PIA conducted for each sub-system (i.e. Register / Registrar System): • During system analysis and design • After user acceptance testing (i.e. pre-production) • After system live run (i.e. post-production) Additional PIA exercise(s) might be required if there are significant concerns or findings raised in the previous exercise(s).
5.	Vulnerability fixing and system enhancement for data privacy
5.1.	The Contractor must fix the vulnerabilities and data privacy issues identified/ raised in the SRAA, penetration testing and PIA according to the testing results and reports.

As the proposed database might have web-based tool and platform; and the database will be used at application-level (i.e. for DNRS), the Contractor also needs to observe and comply with the following security guidelines, if and when applicable, when designing its solution; and during the system implementation and on-going system maintenance:

1. Website and Web Application Security
   1.1. Common Threats for Websites and Web Applications
      1.1.1. Ensure no components with known vulnerability.
      1.1.2. Ensure System/security with proper configuration.
      1.1.3. Ensure defence in depth concept in design.
      1.1.4. Ensure enough control to prevent from Distributed Denial of Service (DDoS) attack.
      1.1.5. Ensure enough control to defense Altering website code and/or web defacement.
      1.1.6. Ensure enough control to prevent from Web forgery.
   1.2. Additional Threats for Web Applications
      1.2.1. Ensure enough control to minimize the web application security risks mentioned in OWASP Top 10 and other good practices.
2. Website and Web Application Life Cycle
   2.1. Project Initiation

2.1.1. Ensure project requirements such as functions and features of new website/web application, which are operation or business focused.

2.1.2. Ensure proper data classification involved to the website and web application.

2.1.3. Ensure enough security requirements for the new project such as encryption requirements, data storage protection and physical protection requirement are mentioned in the project documentation.

2.2. Feasibility Study

2.2.1. Ensure security requirement analysis and security planning if the project is technically feasible.

2.3. Systems Analysis & Design

2.3.1. Ensure security requirements based on the business needs, including the legal and regulatory requirements (e.g. the Personal Data (Privacy) Ordinance) and the best practice security requirements.

2.3.2. Ensure corresponding security controls should be incorporated to the design such that secure architecture, design and structure can be achieved.

2.3.3. Ensure appropriate technical and organisational security measures should be adopted to protect personal data from unauthorised or accidental access, processing, erasure or other use, including but not limited to ensuring the compliance with all applicable laws and regulations, conducting privacy impact assessment to identify and manage data protection risks, ensuring the processes and systems are designed such that the collection and processing of personal data are limited to what is necessary for the identified purpose, and improving staff awareness of the possible consequences (such as violation of security policies, damage of government image, disciplinary actions) when personal data is breached.

2.3.4. Ensure adequate security review conducted in the design stage in the SDLC, which serves as a checkpoint to ensure necessary security requirements are identified and incorporated in the system design.

2.4. Implementation

2.4.1. Ensure the requirements defined and the suggested counter measures from risk for the assessment result should be followed for system/application development.

2.4.2. Ensure that the website or web application is ready for production with acceptable risks for security assurance.

2.4.3. Ensure inspection and acceptance of developed components for website and web application and integration of security controls should be performed to current environment, or new production environment, if any.

2.4.4. Ensure the web application secure coding practices in developing web applications should be observed so as to withstand some common web application security vulnerabilities.

2.4.5. Ensure source Code Review and Protection.

2.4.6. Ensure security risk assessment should be performed before the production launch of the website or web application.

2.4.7. Ensure privacy impact assessment should be conducted to examine the adequacy, effectiveness and practicability of the planned protection measures for the protection of personal data.

2.5. Post-Implementation

2.5.1. Ensure a post-implementation review should be performed such that there is no unexpected problem during the system installation and deployment task.

2.5.2. Ensure all proposed changes or patches should be verified in testing environment and they do not incur security issue to the production environment.

2.5.3. Ensure backup task should be performed to prevent from unexpected loss of information and to ensure that fallback is available when the change is failed.

2.5.4. Ensure security monitoring should be adopted to detect malicious activities targeted to website and web application.

2.5.5. Ensure an incident response and handling procedure should be defined for website and web application.

2.5.6. Security risk assessments for websites and web applications should be performed at least once every two years or after major changes.

2.6. Decommission

2.6.1. Ensure that the replacement is run properly and necessary migration has been performed such as data and user migration in case there is a replacement of website or web application for the original system.

3. Additional Security Consideration for Web Content Management System and Web 2.0

3.1. Web Content Management System (WCMS)

3.1.1. Ensure WCMS is subject to the same security threats and operation process vulnerabilities as other web applications.

3.2. Web 2.0

3.2.1. Ensure Security Concerns and Precautionary Measures should be adopted in the use of Web 2.0 technologies.

4.6. Part F – System maintenance and support

#	Requirements
1.	Unlimited e-mail and telephone/ virtual conference support
1.1.	Support operating hours: • 7 days x 24 hours
2.	Database issue fixing
2.1.	The Contractor has to conduct an assessment and effort estimation for every reported issue and perform bug fixing according to the plan.
3.	Database patching and vulnerability fixing
3.1.	Database patching and vulnerability fixing have to conducted by the Contractor, including but not limited to regular System hotfix, Operating System (OS) patching, database patching, critical vulnerability fixing, according to the importance of the identified vulnerabilities and business impact incurred by the patch(s).
4.	Disaster recovery (DR) drill
4.1.	DR drill will be run once per year, and the Contractor has to provide support in this exercise at the database level.
5.	Incident response, system recovery and critical issue fixing
5.1.	For any critical issue (top severity), system down and security breach, 24x7 support has to be provided for resuming the System into the normal state as soonest as possible.
6.	Supporting regular security scanning and audit
7.	HKIRC reserves the rights to do ad-hoc system enhancement or develop add-on components based on the Contractors' solution without voiding the warranty.

1. Problem classification

Severity	Definition
Critical (Severity 1)	Production server or other mission critical system(s) are down and no workaround is immediately available. • All or a substantial portion of our mission critical data is at a significant risk of loss or corruption. • Have had a substantial loss of service. • Business operations have been completely halted. • Payment gateways have been completely not functioning
Major (Severity 2)	Major functionality is severely impaired. • Operations can continue in a restricted fashion, although long-term productivity might be adversely affected. • A major milestone is at risk. Ongoing and incremental installations are affected. • A temporary workaround is available.
Minor (Severity 3)	Partial, non-critical loss of functionality of the software. • Impaired operations of some components, but allows the user to continue using the software. • Initial installation milestones are at minimal risk.
Cosmetic (Severity 4)	General usage questions. • Cosmetic issues, including errors in the documentation

2. Security classification

Severity	Definition
Critical (Severity 1)	Intruders can easily gain control of the host, which can lead to the compromise of the entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.
Major (Severity 2)	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, and unauthorized use of application and unauthorized use of data.

Severity	Definition
Medium (Severity 3)	Intruders may be able to determine the operating system running on the host and view banner version.
Minor (Severity 4)	Intruders can collect information about the host (open ports, services, etc.)

3. <u>Problem resolution/ vulnerability fixing time</u>

Severity	Response time	Resolution/ fixing time
1	30 minutes	4 hours
2	2 hours	12 hours
3	4 hours	60 hours
4	8 hours	120 hours

Service Provider has to provide local support and onsite support, especially for high-severity issues. Service Provider has to provide the detailed qualifications and team's composition/ competence of System Support Team, including but not limited to:

1. Number of certified professionals of proposed database stationed locally
2. Average years of experience in proposed database of the team members
3. Qualifications/ certifications attained in the team.
4. The local technical support is provided by Service Partner (i.e. System Integrator) or the proposed database manufacturer.

4.7. Part G – Training and skill transfer

Service Provider has to offer technical training to the Database Administrator of HKIRC. Service Provider has to propose a series of technical training for HKIRC's DBA to master the technical skills and knowledge required for daily database administration and audit.

5. Limitation of Liability and Indemnity

The company submitting the tender agrees that if the company becomes the Contractor of the Project, it shall indemnify HKIRC / HKDNR and HKIRC / HKDNR against any claim, demand, loss, damage, cost, expense or liability which the company may suffer from.

5.1. Service Level Agreement (SLA), Service Credits and Contract Termination

All services provided by the Service Provider shall be sized and scaled to meet the agreed SLA, including but not limited to implementing the Project according to the agreed project schedule without significant deviation; delivering project deliverables up to industrial standards and quality levels; protecting data integrity and confidentially; and maintaining system availability at the agreed level. All planned activities which would affect the Production environment and daily operations shall be notified to and agreed with HKIRC four weeks in advance.

In case of the Service Provider's service level does not meet with the proposed SLA, the Service Provider shall, as part of the SLA, include a Service Credit scheme or any applicable remedial actions (at the Service Provider's own cost) for compensation for the service which did not meet the SLA. Service Provider may propose detail scheme during the contractual negotiation stage, but will need to outline the proposed scheme within the tender for HKIRC to evaluate.

In the event of any project delay with respect to a Project Milestone, HKIRC shall be entitled to service credits (in terms of man-days) equivalent to (a) the percentage of Project delay (i.e. number of months of delay divided by overall Project duration) times (b) the Project Sum divided by (c) the higher of (i) the Service Provider's man-day rate to HKIRC at the time of the delay or (ii) a man-day rate mutually agreed (the "Service Credits").

HKIRC also reserves the right to terminate the contract based on a "3-strike" principle; the Service Provider shall not break the SLA for more than three times during the project period. HKIRC also reserves the right to terminate the service if the service provided:

- Causes disruption and/or losses to HKIRC business and operation.
- Causes service downtime without notices.

5.2. Project Management Methodology and Review Meeting

Please propose the project management methodology the Service Provider would adopt for governing the implementation of the Project. Review meetings, on monthly basis, should be arranged for the purposes including but not limited to:

- Monitor and review the overall project progress, quality of project deliverables.
- Discuss and propose action plans for any project-level issues.
- Manage any project-related risks and incidents.

5.3. Intellectual Property Rights

The Service Provider's proposed solution, and its components, shall not infringe the intellectual property rights of any third party. The Service Provider shall bear the liability or consequence for any intellectual property rights infringement made by the Service Provider and/or in its solution for the Project.

5.4. Software Source Code Escrow

It is required to use open source frameworks for the development of the System and release the source code to HKIRC/ HKDNR without additional cost incurred. If this arrangement cannot be made, the Service Provider is required to make software source code escrow arrangement to allow HKIRC/ HKDNR to retrieve and use the software source code of the System for any circumstances in which the Service Provider no longer supports and maintains its solution.

6. Information Security

The company submitting the proposal ("the company") shall acknowledge and agree that, if the company is selected as the Contractor, it shall be bounded by our Non-Disclosure Agreement (NDA) and Information Security Policy (highlights of the policies are illustrated in Appendix D). The company shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

The company shall be provided with a set of NDA after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA shall be signed and returned to HKIRC before the scheduled deadline. HKIRC will only consider proposals from companies which have signed the NDA.

The proposal should be marked "RESTRICTED" at the centre-top of each page in black color. It must be encrypted if transmitted electronically.

Each proposal will be reviewed under the terms of non-disclosure by the HKIRC's staff and Board of Directors of HKIRC.

7. Project Acceptance

The overall project acceptance can be broken down into acceptances at various levels:-

1. System architecture design
2. Installation of databases and establishment of database infrastructure
3. User acceptance testing / security assessment and audit (SRAA) / privacy impact assessment
4. Data migration, system integration (internal and external) and system live run
5. System nursing

8. Anti-collusion

(1) The Tenderer shall not communicate to any person other than HKIRC the amount of any tender, adjust the amount of any tender by arrangement with any other person, make any arrangement with any other person about whether or not he or that other person should or should not tender or otherwise collude with any other person in any manner whatsoever in the tendering process. Any breach of or non-compliance with this sub-clause by the Tenderer shall, without affecting the Tenderer's liability for such breach rules and laws or non-compliance, invalidate his tender.

(2) Sub-clause (1) of this Clause shall have no application to the Tenderer's communications in strict confidence with his own insurers or brokers to obtain an insurance quotation for computation of tender price and communications in strict confidence with his consultants/sub-contractors to solicit their assistance in preparation of tender submission.

(3) The Tenderer shall submit to the HKIRC a duly signed warranty in the form set out in Appendix A to the effect that he understands and will abide by these clauses. The warranty shall be signed by a person authorized to sign the contract on the Tenderer's behalf.

(4) Any breach of any of the representations and/or warranties by the Tenderer may prejudice the Tenderer's future standing as a HKIRC's contractor.

9. Offering Advantages

(1) The Tenderer shall not, and shall procure that his employees, agents and sub-contractors shall not, offer an advantage as defined in the Prevention of Bribery Ordinance, (Cap 201) in connection with the tendering and execution of this contract.

(2) Failure to so procure or any act of offering advantage referred to in (1) above committed by the Tenderer or by an employee, agent or sub-contractor of the Tenderer shall, without affecting the Tenderer's liability for such failure and act, result in his tender being invalidated.

10. Ethical Commitment

10.1. Prevention of bribery

(A) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, except with permission of Hong Kong Internet Registration Corporation Limited (hereafter referred to as the Organisation) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organisation. The Contractor shall also caution his directors, employees, agents and sub-contractors against soliciting or accepting any excessive hospitality, entertainment or inducements which would impair their impartiality in relation to the business of the Organisation. The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors are aware of the aforesaid prohibition and will not, except with permission of the Organisation, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organisation.

(B) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, offer any advantage to any Board member or staff in relation to the business of the Organisation.

10.2. Declaration of Interest

(C) The Contractor shall require his directors and employees to declare in writing to the Organisation any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract. In the event that such conflict or potential conflict is disclosed in a declaration, the Contractor shall forthwith take such reasonable

measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(D) The Contractor shall prohibit his directors and employees who are involved in this Contract from engaging in any work or employment other than in the performance of this Contract, with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(E) The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors who are involved in this Contract are aware of the provisions under the aforesaid sub-clauses (C) and (D).

10.3. Handling of confidential information

(F) The Contractor shall not use or divulge, except for the purpose of this Contract, any information provided by the Organisation in the Contract or in any subsequent correspondence or documentation, or any information obtained when conducting business under this Contract. Any disclosure to any person or agent or sub-contractor for the purpose of the Contract shall be in strict confidence and shall be on a "need to know" basis and extend only so far as may be necessary for the purpose of this Contract. The Contractor shall take all necessary measures (by way of internal guidelines or contractual provisions where appropriate) to ensure that information is not divulged for purposes other than that of this Contract by such person, agent or sub-contractor. The Contractor shall indemnify and keep indemnified the Organisation against all loss, liabilities, damages, costs, legal costs, professional and other expenses of any nature whatsoever the Organisation may suffer, sustain or incur, whether direct or consequential, arising out of or in connection with any breach of the aforesaid non-disclosure provision by the Contractor or his directors, employees, agents or sub-contractors.

10.4. Declaration of ethical commitment

(G) The Contractor shall submit a signed declaration in a form (see Appendix B) prescribed or approved by the Organisation to confirm compliance with the provisions in aforesaid sub-clauses (A) (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and confidentiality. If the Contractor fails to submit the declaration as required, the Organisation shall be entitled to withhold payment until such declaration is submitted and the Contractor shall not be entitled to interest in that period. To demonstrate compliance with the aforesaid sub-clauses (A), (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and handling of confidential information, the Contractor and the sub-contractors employed for the performance of duties under this Contract are required to deposit with the Organisation a copy of the internal guidelines issued to their staff.

11. Time Schedule

	Tasks	To be Completed by	Remark
1	Publish CFT	18-Jul-2025	
2	Expression of Interest	23-Jul-2025	
3	Sign Non-disclosure Agreement (NDA)	28-Jul-2025	
4	Deadline for vendors to submit proposal	8-Aug-2025, 5:30pm	
5	Sign service agreement contract with the appointed vendor	October - November 2025 (for first procurement)	
6	Kick-start of the project	November 2025 (for first procurement)	
7	Database installed and ready for application development	December 2025	
8	Project completion	November 2026	

Service Provider please do fair assessment on the implementation work of database and propose a practical and feasible project schedule, with detailed work plan and justification, for our consideration. Such project schedule, according to your own assessment, is for our reference only, and will not affect your scoring in the tender evaluation process.

12. Payment Schedule

The following payment schedule is recommended but interested vendors may propose their own in their tenders.

Milestone	Items	Payment
1.	System architecture design	5%
2.	Installation of databases and establishment of database infrastructure	10%
2.	User acceptance testing / security assessment and audit / privacy impact assessment	10%
3.	Data migration, system integration, and system live run or ready to go live	45%
4	System nursing (6-month)	30%

13. Elements of a Strong Tender

All submitted tender must follow the format as stated in Appendix C - HKIRC Proposal Requirements

Successful vendor is the one who submitted a clearly worded proposal that demonstrates the following attributes:

- A persuasive section on the company background.
- Internationally recognized certification(s) for quality assurance and information security.
- Strong and flexible service and tools meeting HKIRC requirements with minimum customization.
- High level of interaction between HKIRC and the vendor.
- Excellent fit with the capabilities and facilities of HKIRC.
- Strong company and project management team.

The vendor selection criteria consist of 2 parts: Technical (accounting for 70% of the total score), based on submitted proposal and technical evaluation, and Price (accounting for 30% of the total score).

The Price score is calculated based on the following formula:

Lowest price among qualified tenders / Offered price of the tenderer x 30%

14. Service Agreement Negotiation and Signature

The service agreement will be drawn up between the selected vendor and HKIRC. HKIRC welcomes the vendor's proposal on a suitable service agreement for the project/service.

The service agreement must be signed by both parties within one week from the project/service award date. If the agreement is not signed within the said period, HKIRC will start the negotiation with the next qualified vendor on the selection list.

15. HKIRC Contacts

HKIRC Contacts information

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong +852 2319 2303 – telephone +852 2319 2626 – fax http://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**IT Project Manager** Ricky Fung +852 2319 3822 ricky.fung@hkirc.hk **Manager, IT Infrastructure** Keith Chan +852 2319 3845 keith.chan@hkirc.hk

Appendix A – Warranty

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

Dear Sir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the Call for Tender of Database for Domain Name Registration System (DNRS) (Ref.: CFT-DNRS-DB-01):

(i) it has not communicated and will not communicate to any person other than the HKIRC the amount of any tender price;
(ii) it has not fixed and will not fix the amount of any tender price by arrangement with any person;
(iii) it has not made and will not make any arrangement with any person as to whether it or that other person will or will not submit a tender; and
(iv) it has not otherwise colluded and will not otherwise collude with any person in any manner whatsoever in the tendering process.

(2) In the event that the Tenderer is in breach of any of the representations and/or warranties in Clause (1) above, the HKIRC shall be entitled to, without compensation to any person or liability on the part of the HKIRC :

(i) reject the tender;
(ii) if the HKIRC has accepted the tender, withdraw its acceptance of the tender; and
(iii) if the HKIRC has entered into the contract with the Tenderer,
terminate the contract.

(3) The Tenderer shall indemnify and keep indemnified the HKIRC against all losses, damages, costs or expenses arising out of or in relation to any breach of any of the representations and/or warranties in Clause (1) above.

(4) Clause (1) shall have no application to the Tenderer's communications in strict confidence with its own insurers or brokers to obtain an insurance quotation for computation of the tender price, or with its professional advisers, and consultants or sub-contractors to solicit their assistance in preparation of tender submission. For the avoidance of doubt, the making of a bid by a bidder to the HKIRC in public during an auction will not by itself be regarded as a breach of the representation and warranty in Clause (1)(i) above.

(5) The rights of HKIRC under Clauses (2) to (4) above are in addition to and without prejudice to any other rights or remedies available to it against the Tenderer.

Authorized Signature & Company Chop :

Name of Person Authorized to Sign (in Block Letters) :

Name of Tenderer in English (in Block Letters) :

Date :

Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)
Contract No.: CFT-DNRS-DB-01
Title: Database for Domain Name Registration System (DNRS)

In accordance with the Ethical Commitment clauses in the Contract:

1) We confirm that we have complied with the following provisions and have ensured that our directors, employees, agents and sub-contractors are aware of the following provisions:

   a) prohibiting our directors, employees, agents and sub-contractors who are involved in this Contract from offering, soliciting or accepting any advantage as defined in section 2 of the Prevention of Bribery Ordinance (Cap 201) in relation to the business of HKIRC except with the permission of HKIRC;

   b) requiring our directors, employees, agents and sub-contractors who are involved in this Contract to declare in writing to their respective company management any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract, and in the event that a conflict or potential conflict is disclosed, take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed;

   c) prohibiting our directors and employees who are involved in this Contract from engaging in any work or employment (other than in the performance of this Contract), with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract and requiring our agents and sub-contractors to do the same; and

   d) taking all measures as necessary to protect any confidential/privileged information or data entrusted to us by or on behalf of HKIRC from being divulged to a third party other than those allowed in this Contract.

Signature
(Name of the Contractor)
(Name of the Signatory)
(Position of the Signatory)
(Date)

Appendix C – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 11 – Time Schedule, item no. 4 for the proposal submission deadline.
Hard copies	No Hard Copy is required
Electronic copy	Electronic copy is mandatory. It shall be sent by email to **ricky.fung@hkirc.hk** and **keith.chan@hkirc.hk**; also cc **john.lam@hkirc.hk**.
Proposal format	Specified in this document
Page count	40 pages or fewer
Font	Electronically published or typed. Times New Roman 12-point font.

1 Proposal Content

The proposal should contain the following:

- Cover Page
- Executive Summary
- Conflict of Interest Declaration
- Company Background
    - Financial Situation
    - Track Records
    - Organization and management team
    - Project team with credentials
    - Company credentials
    - Staff credentials
- Methodology
- Project management methodology
- Understanding of our requirements
- Knowledge and Advice on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Timetable
- Commercial and Payment Terms. e.g. Compensation for delay

2 Cover Page

Prepare a non-confidential cover page with the following information in the order given.

Cover Page		
Project Title		
		Database for Domain Name Registration System (DNRS) (Tender Ref.: CFT-DNRS-DB-01)
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

3 Executive Summary

The executive summary provides a brief synopsis of the commercial and technical solution the vendor proposed for the project/service. This summary must be non-confidential. It should fit on a single page.

The executive summary should be constructed to reflect the merits of the proposal and its feasibility. It should also clearly specify the project/service's goals and resource requirements. It should include:

- Rationale for pursuing the project or service, the methodology/technology needed and the present state of the relevant methodology/technology.
- Brief description of the vendor's financial situation.
- Brief description of the vendor's facilities and experience on similar projects or services

4 Conflict of Interest Declaration

Declare any conflict of interest in relation to the project and the '.hk' ccTLD registry HKIRC.

5 Company Background

The vendor must describe its company background. Major activities, financial situation, organizational structure, management team and achievements in similar projects/services or service outsourcing of the company should be elaborated. Track records are preferred.

List the key technical and management personnel in the proposal. Provide a summary of the qualifications and role of each key member. Please indicate where the key members station, i.e. local or non-local.

Please specify the following details:

a. Whether the implementation/ support services carried out by the Database manufacturer or its Service partner(s).
b. Database manufacturer – whether the implementation/ support services are conducted locally or offshore.
c. Service partner – whether the implementation/ support services are conducted locally or offshore.
d. Number of certified professionals of the proposed Database possessed by the Database manufacturer and its Service partner(s).

6 Methodology

The vendor must describe the methods to be used, and briefly explain its advantage and disadvantage. Track records are preferred.

Please specify the methodologies for:

a. Local/ cross-site resilience, failover, load balancing
b. Data migration/ synchronization between the current database and new database
c. Hot backup
d. Database encryption
e. Any other technical requirements specified in this CFT

7 Project Management Methodology

The vendor must describe the methods to be used, and briefly explain its advantage and disadvantage. Track records are preferred.

8 Understanding of our requirements

The vendor shall describe their understanding of our requirements. With the use of a table, the vendor should clearly state their compliance with the requirements listed in the scope of service section; and briefly explain how they are achieved.

9 Knowledge and Advices on Projects/Services

The vendor should describe their knowledge and advice to ensure the success of this project/service or projects/services with similar nature.

10 Deliverable and Services level

The vendor should detail the project/service deliverables, and the services level of the proposed services. Tables of content of all reports included in the deliverables should be provided in the proposal.

11 Proposed Costs of Service and Payment Schedule

The vendor should provide the breakdown of the cost of the whole project/service, including "Core" and "Quotation for Reference". The cost shall be broken down by milestone/phases. The payment shall be scheduled based on the milestones and/or deliverables.

Such costs should include, if applicable:

- Fixed setup cost
- Labour unit costs for additional services or requirements. They are typically quoted in unit man day. Quoted in normal working hours, non-working hours and in emergency.
- Equipment that is permanently placed or purchased for HKIRC to complete the project or service, if any.
- Subsequent support, maintenance or consultation service. (for at least the subsequent 3 years)
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

Service Provider please provide separate cost items, with at least 2-year validity period for perpetual licenses/ one-off implementation; and at least 5-year validity period for license maintenance and support/ professional services, with the breakdown as follows:

Cost Item 1	Database licenses (Production): • For Registry System, Registrar System and Membership Registration System • Production environment • Perpetual license [Note] + 3-year warranty OR 3-year subscription *[Note] If Perpetual license has included 1-year warranty, then, only need to quote additional warranty for 2 more years, i.e. total 3 years.*	• Cost Item 1a: Perpetual license • Cost Item 1b: 3-year license maintenance • Cost Item 1c: 3-year license subscription Assuming same for cross-site Active-Active and cross-site Active-Standby Please also quote the cost reduction if local resilience of Secondary Site is trimmed down from Active-Active to Single-Node.

Cost Item 2	Database licenses (Non-Production):
	• For Registry System, Registrar System and Membership Registration System
	• Non-Production environment
	  o Development (DEV)
	  o User Acceptance Test (UAT)
	  o Operational Test and Evaluation (OTE) (Not applicable to MRS)
	• Perpetual license [Note] + 3-year warranty OR 3-year subscription
	[Note] If Perpetual license has included 1-year warranty, then, only need to quote additional warranty for 2 more years, i.e. total 3 years.
		• Cost Item 2a: Perpetual license
		• Cost Item 2b: 3-year license maintenance
		• Cost Item 2c: 3-year license subscription
		Assuming same for cross-site Active-Active and cross-site Active-Standby
		
		Please also quote the cost reduction if local resilience of Secondary Site is trimmed down from Active-Active to Single-Node.

Cost Item 3	Database related licenses, including but not limited to:
	• Database administration tool
	• Clustering
	• Cross-site resilience
	• Data backup
	• Data synchronization (between the current database and new database)
	• Operating system (if applicable)
		• Cost Item 3a – local Active-Active; cross-site Active-Active
		  o Quotation 3a(i): Perpetual license
		  o Quotation 3a(ii): 3-year license maintenance
		  o Quotation 3a(iii): 3-year license subscription

	Perpetual license [Note] + 3-year warranty OR
	3-year subscription
	[Note] If Perpetual license has included 1-year warranty, then, only need to quote additional warranty for 2 more years, i.e. total 3 years.
		• Cost Item 3b – local Active-Active; cross-site Active-Standby
		  o Quotation 3b(i): Perpetual license
		  o Quotation 3b(ii): 3-year license maintenance
		  o Quotation 3b(iii): 3-year license subscription
		
		Please also quote the cost reduction if local resilience of Secondary Site is trimmed down from Active-Active to Single-Node.

Cost Item 4	Installation of database and implementation of database infrastructure (Production): • Including database implementation services, project management and documentation • Information security and data privacy protection • For Registry System, Registrar System and Membership Registration System • Production environment	• Cost Item 4a – local Active-Active; cross-site Active-Active • Cost Item 4b – local Active-Active; cross-site Active-Standby Please also quote the cost reduction if local resilience of Secondary Site is trimmed down from Active-Active to Single-Node.
Cost Item 5	Installation of database and implementation of database infrastructure (Non-Production): • Including database implementation services, project management and documentation • Information security and data privacy protection • For Registry System, Registrar System and Membership Registration System • Non-Production environment	• Cost Item 5a – local Active-Active; cross-site Active-Active • Cost Item 5b – local Active-Active; cross-site Active-Standby Please also quote the cost reduction if local resilience of Secondary Site is trimmed down from Active-Active to Single-Node.
Cost Item 6	Data migration from current database to new database and system deployment (Production): • Including database implementation services, project management and documentation	Assuming same for cross-site Active-Active and cross-site Active-Standby

	• Information security and data privacy protection • For Registry System, Registrar System and Membership Registration System • Production environment	
Cost Item 7	Data migration from current database to new database and system deployment (Non-Production): • Including database implementation services, project management and documentation • Information security and data privacy protection • For Registry System, Registrar System and Membership Registration System • Non-Production environment	Assuming same for cross-site Active-Active and cross-site Active-Standby
Cost Item 8	7x24 System maintenance and support (Production) • 3-year service period • For Registry System, Registrar System and Membership Registration System • Production environment	• Cost Item 8a – local Active-Active; cross-site Active-Active • Cost Item 8b – local Active-Active; cross-site Active-Standby
Cost Item 9	5x8 System maintenance and support (Non-Production) • 3-year service period • For Registry System, Registrar System and Membership Registration System • Non-Production environment	• Cost Item 9a – local Active-Active; cross-site Active-Active • Cost Item 9b – local Active-Active; cross-site Active-Standby
Cost Item 10	Training and skill transfer • 1 seat if it is offered on per-seat basis • 1 session if it is tailor-made training/ skill transfer for our team • Specify the topics, languages, duration, format (hand-on or lecture), pre-requisites, etc. of your proposed training/ skill transfer	Assuming same for cross-site Active-Active and cross-site Active-Standby
Cost Item 11	7x24 On-site technical support • Man-day rate during office hours • Man-day rate during non-office hours (if different)	Assuming same for cross-site Active-Active and cross-site Active-Standby

	• For emergency support (following **4.6 Part F – System maintenance and support**) and scheduled support	
Cost Item 12	Professional services • Man-day rate during office hours • Man-day rate during non-office hours (if different)	Assuming same for cross-site Active-Active and cross-site Active-Standby

A table is prepared, as below, for your to provide the cost breakdown information:

Cost Item	**Description**	**One-off**	**Year 1**	**Year 2**	**Year 3**	**Total**
1a	Database licenses (Production) - perpetual license					
1b	Database licenses (Production) – license maintenance					
1c	Database licenses (Production) – license subscription					
2a	Database licenses (Non-Production) - perpetual license					
2b	Database licenses (Non-Production) – license maintenance					
2c	Database licenses (Non-Production) – license subscription					
3a(i)	Database related licenses (Active-Active) – perpetual license					
3a(ii)	Database related licenses (Active-Active) – license maintenance					
3a(iii)	Database related licenses (Active-Active) – license subscription					
3b(i)	Database related licenses (Active-Standby) – perpetual license					
3b(ii)	Database related licenses (Active-					

Cost Item	**Description**	**One-off**	**Year 1**	**Year 2**	**Year 3**	**Total**
	Standby) – license maintenance					
3b(iii)	Database related licenses (Active-Standby) – license subscription					
4a	Installation of database and implementation of database infrastructure (Production) – Active-Active					
4b	Installation of database and implementation of database infrastructure (Production) – Active-Standby					
5a	Installation of database and implementation of database infrastructure (Non-Production) – Active-Active					
5b	Installation of database and implementation of database infrastructure (Non-Production) – Active-Standby					
6	Data migration from current database to new database and					

Cost Item	**Description**	**One-off**	**Year 1**	**Year 2**	**Year 3**	**Total**
	system deployment (Production)					
7	Data migration from current database to new database and system deployment (Non-Production)					
8a	7x24 System maintenance and support (Production) – Active-Active					
8b	7x24 System maintenance and support (Production) – Active-Standby					
9a	5x8 System maintenance and support (Non-Production) – Active-Active					
9b	5x8 System maintenance and support (Non-Production) – Active-Standby					
10	Training and skill transfer (per seat/ session, please specify)					
11a	7x24 On-site technical support (Man-day rate during office hours)					
11b	7x24 On-site technical support (Man-day rate during non-office hours)					

Cost Item	**Description**	**One-off**	**Year 1**	**Year 2**	**Year 3**	**Total**
12a	Professional services (Man-day rate during office hours)					
12b	Professional services (Man-day rate during Non-office hours)					

12 Implementation Time Table

The vendor should present in this section the implementation schedule of the project/service. The schedule should be realistic and achievable by the vendor.

13 Commercial and Payment Terms

The vendor should describe the commercial and payment terms of the services e.g. compensation for the delay of the project/service.

Appendix D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing

This document provides an extract of the HKIRC Information Security Policy (the "Policy") with the purposes of (a) introducing various measures and controls to be executed by HKIRC regarding outsourcing, and (b) setting the expectation of any potential contractors that their participation and conformance in these measures and controls are essential contractual obligations.

The original Policy applies to HKIRC's employees, contractors, and third-party users. However, a potential contractor may interpret the clauses up to their roles and responsibilities only. Nonetheless, the keyword "Contractors" hereby refers to all relevant staff of the contractor and of any other subcontractors under the contractor's purview.

Herein, HKIRC would also set the expectation of any potential contractors that upon their indication of interest to the project, they shall be required in the subsequent stages to sign off a non-disclosure agreement ("NDA") on all information to be provided.

<->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->-><->

7. HUMAN RESOURCES SECURITY

7.1 PRIOR TO EMPLOYMENT

Security objective: To ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

7.1.1 Security roles and responsibilities of employees, contractors and third-party users shall be defined and documented in accordance with the Organization's information security policy.

7.1.2 Background verification checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

7.1.3 As part of their contractual obligation, employees, contractors and third-party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the Organization's responsibilities for information security.

7.2 DURING EMPLOYMENT

Security objective: To ensure that all employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

7.2.1 Management shall require employees, contractors and third-party users to apply security in accordance with established policies and procedures of the Organization.

7.2.2 All employees of the Organization and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

7.3 TERMINATION AND CHANGE OF EMPLOYMENT

Security objective: To ensure that employees, contractors and third-party users exit the Organization or change employment in an orderly manner.

7.3.2 All employees, contractors and third-party users shall return all of the Organization's assets in their possession upon termination of their employment, contract or agreement.

7.3.3 The access rights of all employees, contractors and third-party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

14.2.7 The organization shall supervise and monitor the activity of outsourced system development.

16. INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

Security objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.3 Employees and contractors using the Organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.