Hong Kong Internet Registration Corporation Limited
香港互聯網註冊管理有限公司

Request for Proposals For Secondary Domain Name Service Provider

Version 1.1
Date: 08 July 2016

Hong Kong Internet Registration Corporation Limited

Unit 2002-2005, 20/F FWD Financial Centre,
308 Des Voeux Road Central,
Sheung Wan, Hong Kong.
Tel.: +852 2319 1313 Fax: +852 2319 2626
Email: enquiry@hkirc.hk Website: www.hkirc.hk

IMPORTANT NOTICE

Table of Contents

1. Summary

HKIRC is looking for a vendor or professional(s) system integrator ("the Contractor") to provide and setup for the subjected services.

The scope of service is detailed in section 5 of this document.

The Contractor should demonstrate a history of similar project successes and able to provide the resources for the full project life cycle, from architecture design, project management, requirements gathering and analysis, configuration, testing and handover through to nursing period.

Parties interested in providing this service shall submit **Expression of Interest (EOI) by 15 July 2016**. For those who have submitted EOI, they should **submit proposal** (see Appendix D) to the Group **no later than 5:30pm on 26 Aug 2016**.

The selection criteria when reviewing the RFP's will be as follows.

- The service provider has demonstrated through references that they have successfully delivered similar service in the past.
- The service provider has shown they have access to a pool of resources with the appropriate skill sets to deliver the service.
- Technical support arrangement / workflow / service-level agreement (SLA)

2. Definitions

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

“The Contractor” means 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”

“ISMS” means Information Security Management System. It consists of an information security organization and a set of policies, guidelines and procedures concerned with information security management.

“The Services” means the Secondary Domain Name Service Provider services with requirements stipulated in Section 5 of this document.

“RFP” means this Request for Proposal

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

3. 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 endeavours 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.

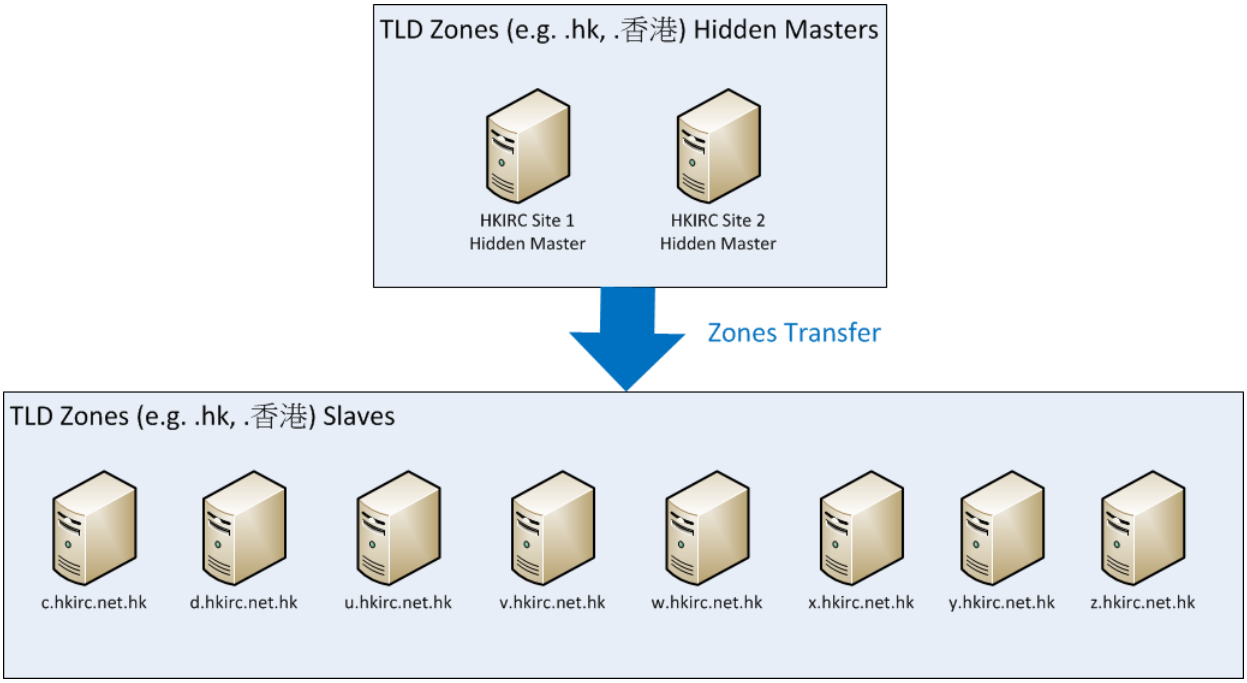
HKIRC and HKDNR are listed as public bodies under the Prevention of Bribery Ordinance (Cap 201).

4. Requirement Background & Current Situation

HKIRC is currently providing country level Doman Name Resolution service for the .hk and .香港 domains. HKIRC is also providing whois service as well as online Domain Name Registration service as well.

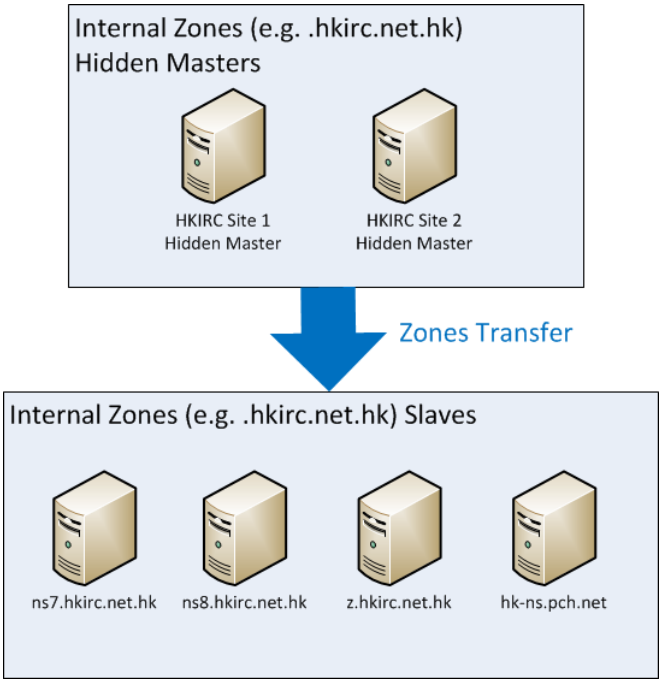
Additional Information for DNS service:

Currently 29 ccTLD zones are served by 8 slave nameservers (some of them are anycast) which zones are continuously transferred from 2 HKIRC managed hidden masters.



As of 24 June, 2016, there are 439355 delgated under 29 ccTLD zones. For detailed figure, refer to our "Statistics of Active '.hk' Domain Names" page at https://www.hkirc.hk/content.jsp?id=77#!/77&in=/aboutHK/registration_statistics_hkirc.jsp

Besdies ccTLD, HKIRC also own few internal domains, most zones are served by two HKIRC managed name servers (ns7.hkirc.net.hk, ns8.hkirc.net.hk) however there are 4 key zones (hkirc.net.hk, hkirc.hk, hkdnr.net.hk, hkdnr.hk) are also served by anycast backed slaves.


Internal Zones (e.g. .hkirc.net.hk)
Hidden Masters
HKIRC Site 1
Hidden Master
HKIRC Site 2
Hidden Master
Zones Transfer
Internal Zones (e.g. .hkirc.net.hk) Slaves
ns7.hkirc.net.hk
ns8.hkirc.net.hk
z.hkirc.net.hk
hk-ns.pch.net

5. High Level Requirements

The following defines the high level requirements to be provided by the Service Provider:-

- **DNS Protocol:** Service compliance to latest specified RFCs.
- **Zone Provisioning:** Provide functionality for frequent provisioning of new zones to respondents' name servers.
- **DNS Update:** Respondent accept timely zone update from HKIRC operated Master Servers, with proper signaling and key signing. Also for Incremental transfer as well.
- **Architecture**: Respondent to provide a DNS Service with architecture able to support and sustain the require services during the contract period.
- **Operations**: Confirm that the respondent has the operational infrastructure in order to deliver the proposed service.
- **Capacity Planning:** Respondent to provide information on current and any future planned network, server and other infrastructure capacity. Also current service performance benchmark figures will also be needed.
- **Monitoring and Measurement:** Respondent to provide monthly reports of total number of queries per zone. Near real-time performance and service status report would also be desirable. Also provide any monitoring and/or usages reports through different methods of access and distribution.
- **DNS Security:** Respondent to provide information on DNS Security support as specified in RFC 4033-4035.
- **User Interfaces and Reporting:** Provide customer interface that HKIRC can access account information, examine the contents of zones, receive reports and graphs of DNS Usage Statistics, or other relevant information.
- **Disaster Recovery:** Confirm that all data supplied by HKIRC will not be sent to any other third parties, such as escrow organizations or other DNS providers. Also any Disaster Recovery plan in place and drill plan/log.
- **Service Level Agreements (SLAs):** Provide service agreement for, unplanned, planned and other uptime/downtime events.
- **Experience and Implementation:** Provide customer's reference or case to show experience on implementation such services.
- The total length of the contract will be 36 month.

5.1. DNS Protocol

i. Indicate the level of compliance with the following RFCs. Where your systems are not compliant, specify how your systems differ, and why. You do not need to include discrepancies in an RFC in which you conform to a later RFC that updates the original): RFC 1034 RFC 1035 RFC 1101 RFC 1982 RFC 1995 RFC 1996 RFC 2181 RFC 2535 RFC 2845 RFC 2870 RFC 3833 RFC 4033 RFC 4034 RFC 4035 RFC 4470 RFC 4509 RFC 4592 RFC 5155 RFC 6781

ii. Confirm that all of your name servers answer well-formed queries over both TCP and UDP.

iii. Confirm that all of your name servers answer well-formed queries sent over UDP using EDNS0.

iv. Confirm that all of your name servers answer well-formed DNSSEC queries.

v. Confirm that all name servers support all resource record types defined at the time of responding, and are also capable of supporting any other resource record type without modification as an opaque type.

vi. State what portion of your name server constellation answers well-formed queries on a native IPv6 network, what portion answers queries on a IPv6 network that is tunneled through an IPv4 network, and what portion uses only IPv4.

vii. State your plan to have all name servers answering queries on IPv6 networks, if not already is.

viii. Describe plans for the evaluation and implementation of new protocols and extensions to existing protocols that might emerge in the future.

ix. Describe any participation in standards development related to the DNS or other aspects of the DNS service in which the respondent. Enumerate the personnel involved, and describe their level of involvement.

x. For respondents whose DNS responses are not generated by either BIND 9.9 (or later) or NSD 4 (or later), describe how answers to DNS queries are constructed, with particular attention to the use of the TC bit and the ADDITIONAL section. It is acceptable to describe precisely how the implementation of the protocol differs from either BIND 9.9 or NSD 4.

xi. Indicate the behavior of the DNS service when a client sends a query for a name that is external to an HKIRC's zone, but internal to other zones hosted by the respondent, to a name server provided by the respondent for inclusion in the NS set of HKIRC zones.

xii. Indicate the behavior of the DNS service with IDNs, ie. domain names contain

letters or characters from non-Latin scripts.

5.2. Zone Provisioning

i. The respondent will provide functionality for frequent provisioning of new zones to respondents' name servers.
ii. Describe the tools and/or procedures available to accommodate provisioning of new zones on your name servers. Provide diagrams in-line if possible.
iii. How does your system handle failed zone provisioning requests?
iv. On average, how long in seconds does it take for a newly-provisioned zone to be available on all name servers in your infrastructure?

5.3. DNS Updates

i. The respondent will accept TSIG-signed NOTIFY messages from one or more HKIRC operated master servers, and will respond by carrying out zone transfers in cases where NOTIFY messages indicate that new zone data is available for transfer. Incremental (IXFR) transfers will be used wherever possible.
ii. Describe the architecture used to update your name servers. Provide diagrams in-line if possible.
iii. Describe the methodology to rotate the shared TSIG (Transaction SIGnature).
iv. How does your system handle a failed update?
v. On average, how long in seconds does it take a change to propagate from the system HKIRC sends it's update to, until the last name server is updated?
vi. Describe the behavior of a name server within your system that is unable to receive updates for a prolonged period of time (e.g. due to a substantial network failure or other catastrophic event).

5.4. Architecture

i. Describe the overall architecture of the DNS service that will be used for the HKIRC's zones. Include diagrams where appropriate. Indicate any sections of this architecture that are not currently in place, and list the projected deployment date.
ii. State the name and version of the software application running on your name servers that will resolve the zones to the end user community. If this is not your own application, state any warranty / service level agreement you have with

vendors for this software. If this is your own application, describe your software development life cycle.

iii. Specify the number of authoritative-only name servers which can be made available to serve HKIRC zones.

iv. Indicate the IPv4 and Ipv6 addresses that would be used for each name server, or, where exact addresses cannot be specified at the time of response, how such addresses would be acquired. Describe the routing advertisements which correspond to each address. Indicate whether any of the routing advertisements would cover addresses used for any other service as well as the services provided to HKIRC.

v. Describe any use of anycast to provide the DNS service. Specify whether the service is to be provided (entirely or in part) without the use of anycast.

vi. Where service is constructed by the use of multiple installations (e.g. separate anycast nodes) please identify the location of each installation, and summarize differences between installations in terms of co-location facilities, network services, hardware, software, bandwidth, and capacity if possible.

vii. If service is constructed by the use of multiple installations (e.g. separate anycast nodes) please describe capabilities for selection of nodes in service

viii. Identify any single points of failure in the system. Describe any diversity in hardware and software that has been implemented.

ix. Please state your point of present in the mainland China (excluding Hong Kong) and any special operational consideration instated in your mainland China operation.

5.5. Operations

i. Confirm that no name server used as an authority server for HKIRC zones will provide recursive DNS service to any client.

ii. Confirm that public zone transfers will not be permitted from any name server used to serve HKIRC zones.

iii. Confirm that HKIRC may, from time to time, have an independent third party conduct tests to assess readiness of your infrastructure for attacks.

iv. State the number of network providers at each installation, along with the amount of bandwidth (both sustained and peak) provisioned.

v. State any peering arrangements you have.

vi. Describe the procedures by which operating systems and other software used to provide the DNS service are administered, including procedures for upgrades and

configuration changes.

vii. Describe the procedures by which system and software logs are stored, retained and analyzed.

viii. Describe the mechanism by which problems identified with the DNS service can be reported to the respondent by HKIRC. Include details of contact methods, the time following a report within which the respondent undertakes to provide responses, escalation procedures, and coverage at different times of day and on holidays.

ix. Describe the respondent's involvement in operator forums, conferences, and other organizations relevant to the operation of networks and services on the Internet.

x. Describe the respondent's policies for interconnection with external networks, e.g. at exchange points. Summarize all external network interconnections.

xi. Describe your methodology for deploying new components to the service. Will you provide a platform for HKIRC to perform regression tests against before deploying changes into production?

xii. Describe how many other customers exist on the platform you plan to deploy for HKIRC. Will HKIRC be segmented away from these other customers? If so, how?

xiii. Specify your minimum requirements for selecting a production co-location or data center facility

xiv. Specify your systems, procedures, and processes for mitigating Distributed Denial of Service (DDoS) attacks. Please also give account (if any) on any DNS attacks handled eg. size, type of attack, mitigation method etc.

xv. Do you deploy/applies any filtering to DNS traffic?

5.6. Capacity Planning

Note:

Where service is being provided by multiple installations (e.g. different anycast nodes), please provide answers to the following questions for the service as a whole, and for each individual installation.

i. State the bandwidth available for use in performing zone transfers. Indicate the maximum frequency of zone transfers which can be supported, assuming minimal-sized updates. Indicate the maximum volume of zone transfers which

can be supported, measured in number of resource records per minute.

ii. Indicate whether the network resources used to carry zone transfer and other control traffic are the same as (or overlap with) the resources used to answer queries from clients.

iii. Indicate the maximum query loads that the DNS service is able to handle. If based on estimates, please list all assumptions on which the estimate is based. If based on empirical testing, describe the test methodology in as much detail as possible.

iv. Indicate the maximum size of a zone which can be served by the DNS service, measured in "number of resource records". Indicate the maximum number of zones which can be served by the DNS service. Indicate the maximum combined size of all zones which can be served by the DNS service, measured in "number of resource records".

v. Describe procedures within which capacity of various components of the system is monitored, and indicate the policies within which capacity will be augmented in response to observed need.

vi. Identify all practical limits to the scaling of the system to handle increased query loads.

5.7. Monitoring and Measurement

i. HKIRC will require at least monthly reports of total number of queries per zone/sub-zone in day resolution.

ii. Describe capabilities for query traffic capture and analysis, including routine measurement (that which is always performed) and tactical measurement (that which can be performed in response to an operational situation). Indicate how data is stored and summarized.

iii. Describe how individual components in the system are monitored for problems. Describe the internal escalations which would normally follow the identification of such a failure.

iv. Describe the group within your organization that is responsible for monitoring the production systems. Is it available 24x7? Does this include shift overlap?

v. In the traffic captured in i., do you make this data available to other parties for analysis? If so, to whom, and how often? Will this data be made available to HKIRC?

vi. Will HKIRC have access to any real-time monitoring tools provided by your organization?

vii. Describe DNS usage statistics your organization can provide to HKIRC which exceed those described in i.?

5.8. Security

i. Confirm that queries which request signed responses will be answered as specified in RFC 4033-4035, in the case where the zones concerned are signed.
ii. Describe the operational security practices employed to safeguard the infrastructure used to provide the DNS service.
iii. Describe procedures and policies in place to identify, characterize and mitigate denial-of-service (including distributed denial-of-service) traffic.
iv. Describe the procedures used to exchange secret keys (e.g. for TSIG) with customers. Are secret keys shared across multiple customers? Are secret keys shared across multiple zones for the same customer?
v. Describe the prerequisites and requirements for the proposed architecture to support the use of NSEC3 records in zones signed by HKIRC, consistent with RFC 5155. Include estimates of when such a capability might be available, noting all external dependencies on which the estimate depends. Include details of specific interoperability testing that is expected to take place.
vi. Are you currently responsible for signing any zones? If so, describe your key management policy and security measures.
vii. Describe the security practices and procedures on patching security vulnerabilities on your systems.
viii. Indicate which functional groups within the respondent's organization will have administrator-level access to individual components used to provide the DNS service.
ix. Describe your hiring and firing procedures for personnel with the access described in vii.
x. Describe the respondent's involvement with security forums, conferences and other organizations relevant to network, system and service security.
xi. Describe, in as much detail as possible, the operational response and impact to service of the most serious security incident experienced by the infrastructure to date.
xii. Specify the last date in which an independent audit of your security practices and procedures was conducted. Who performed this audit?
xiii. Provide evidence of periodic reviews of perimeter security devices (firewall logs, IDS alerts, router configurations etc.) and their procedures, if available.

5.9. User Interfaces and Reporting

i. Describe any customer interface that HKIRC would use to access account information, examine the contents of zones, receive reports and graphs of DNS Usage Statistics, or other relevant information.
ii. Describe any monitoring or usages reports that would be made available to HKIRC, including description, frequency, and method of access or distribution (API, email, web interface, RSS, etc.). At a minimum, HKIRC will require a monthly report of number of queries per zone.
iii. Do you have any type of mechanism to allow HKRIC to generate it's own reports?
iv. Describe your retention schedule for all data and reports. How are older reports accessed by HKIRC?

5.10. Disaster Recovery

i. Confirm that all data supplied by HKIRC will not be sent to any other third parties, such as escrow organizations or other DNS providers.
ii. Do you have a disaster recovery plan in place? If so, provide that plan here.
iii. If you have multiple locations, describe which are mission critical to your operation. How many locations can fail before service is impacted? Include this for the DNS service itself, the update mechanisms, and the user interface and/or reporting systems.
iv. Do you escrow data to a third party? If so, how often is the data sent? If the data is encrypted, describe the methodology for retrieving the secret keys to decrypt the data.
v. Have you tested your disaster recovery plan? If so, can you share the results with us?

5.11. Service Level Agreements (SLAs)

Note: for the next section, assume the following definitions:

Unplanned Outage: an interruption of service in which HKIRC has not received at

least seven (7) days notice prior to the incident.

Planned Outage: an interruption of service in which HKIRC has received at least seven (7) days notice prior to the incident.

Downtime: if, after three consecutive attempts to reach a service within a 5 minute period, from multiple network providers, a service is not reachable, that service is said to be down starting at the time stamp of the first attempt.

Uptime: Any time period that is not considered Downtime.

i. Does the respondent agree to 100% Uptime for your DNS resolution infrastructure as a whole (meaning that at all times, at least one server defined in each zone's apex will respond to queries)?
ii. Notwithstanding Planned Outages, does the respondent agree to 99.9% Uptime for your DNS zone update mechanism per month (this corresponds to 43 minutes of Unplanned Outages per month)?
iii. Does the respondent agree to a maximum of 4 hours per month of Planned Outages for the DNS zone update mechanism?
iv. Does the respondent agree to a maximum of 4 hours per month of Planned Outages for any User Interface used by HKIRC?
v. State your SLA resolution policy with HKIRC in the event that you do not meet a Service Level Agreement for a given month, including any remuneration.
vi. Does the respondent provide any SOC (Security Operation Centre)/NOC (Network Operation Centre) support (hotline/IM/email).Any emergency technical support?

5.12. Experience and Implementation

i. Does the respondent have provided service for TLD before? Please give example on size and extend of the service provided.
ii. What is the typical setup/lead time for service provision?

5.13. 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 A). 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 and Information Security Compliance Statement after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA and the Information Security Compliance Statement shall be signed and returned to HKIRC attached with documents required by the Compliance Statement before the scheduled deadline. **HKIRC will only consider proposals from companies which have signed both the NDA and the Information Security Compliance Statement.**

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.

6. 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 B 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.

7. 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.

8. Ethical Commitment

8.1. 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.

8.2. 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).

8.3. 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.

8.4. Declaration of ethical commitment

(G) The Contractor shall submit a signed declaration in a form (see Appendix C) 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.

9. Project Schedule

	Project schedule Tasks	*To be Completed by*	*Remark*
1	Publish of RFP	8-Jul-2016	
2	Expression of interest	15-Jul-2016	
3	Sign NDA and InfoSec Compliance Statement with all interested vendors	22-Jul-2016	
4	Deadline for vendors to submit proposal and quotation with Warranty Letter	26-Aug-2016, 05:30PM	
5	Selection of vendor by panel	12-Sep-2016	
6	Conclude final decision and appoint the vendor	23-Sep-2016	
7	Prepare service agreement	13-Oct-2016	
8	Sign service agreement with the appointed vendor	20-Oct-2016	
9	Technical Proficiency Tests	27-Oct-2016	
10	Nursing Period complete	11-Nov-2016	
11	Project complete with deliverables	2-Dec-2016	

10. Payment Schedule

Interested vendors shall provide the breakdown of the cost, in Hong Kong Dollars, of the whole service specified in the proposal.

The Respondent should make certain that prices quote are accurate before submitting their proposal. Under no circumstances will the HKIRC accept any request for adjustment on the grounds that a mistake has been made in the proposed prices.

Payment for service could be monthly or annually. Please state billing is prepay or in arrear of service.

11. Elements of a Strong Proposal

All submitted proposal must following the format as stated in Appendix D - HKIRC Proposal Requirements

12. Service Agreement Negotiation and Signature

The service agreement will be drawn up between the selected vendor and HKDNR, the wholly-owned subsidiary of 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.

13. HKIRC Contacts

HKIRC Contacts information

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central, Sheung Wan, Hong Kong +852 23192303 – telephone +852 23192626 – fax http://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**IT Project Manager (System & Network)** Ben Choy +852 23193819 ben.choy@hkirc.hk **Head of IT** Ben Lee +852 23193811 ben.lee@hkirc.hk **Head of Operations and Business Development** Bonnie Chun +852 23193808 bonnie.chun@hkirc.hk

Appendix A – HKDNR Information Security Policy and Guidelines: An Extract Relevant to Outsourcing

This document provides an extract of the HKDNR Information Security Policy and Guidelines with the purposes of (a) introducing various measures and controls to be executed by HKDNR 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 and Guidelines applies to HKDNR'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 members of the contractor and those of any other subcontractors under the contractor's purview.

Herein, HKDNR would also set the expectation of any potential contractors that upon their expression-of-interest to the project/service, they shall be required in the subsequent stages (a) to sign off a non-disclosure agreement (NDA) on all information to be provided and (b) to sign off a Compliance Statement where compliance requirements are specified in more details.

(A) Extract from the HKDNR Information Security Policy

In the following, "the organization" means Hong Kong Domain Name Registration Company Limited, the company requesting the proposal for "the Project."

8. Human resources security

8.1 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.

8.1.1 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.

8.1.2 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.

8.1.3 As part of their contractual obligations, 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.

8.2 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.

8.2.1 Management shall require employees, contractors and third party users to apply security measures in accordance with established policies and procedures of the organization.

8.2.2 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates on organizational policies and procedures, as relevant to their job functions.

8.3 Termination or change of employment
Security objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

8.3.2 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.

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

12. Information systems acquisition, development and maintenance
12.5.5 Outsourced software development shall be supervised and monitored by the organization

13. Information security incident management

13.1 Reporting information security events and weaknesses

Security objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action.

13.1.2 All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

(B) Extract from the HKDNR Information Security Guidelines

6. ORGANIZING INFORMATION SECURITY

6.2 EXTERNAL PARTIES

6.2.1 Identification of Risks Related to External Parties

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting the access.

6.2.3 Addressing Security in Third Party Agreements

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

7. ASSET MANAGMENT

7.1.3 Acceptable Use of Assets

Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

8. HUMAN RESOURCE SECURITY

8.1.1 Roles and Responsibilities

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.

8.1.2 Screening

Background verification checks on all candidates for employment, contractors, and third party users shall be conducted 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.

8.1.3 Terms and Conditions of Employment

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.

8.2.1 Management Responsibilities

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

12. Information systems acquisition, development and maintenance

12.5.5 Outsourced Software Development

Outsourced software development shall be supervised and monitored by the organization.

Appendix B – Warranty

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 tender of Secondary Domain Name Service Provider:

(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 C – Declaration Form by Contractor on their compliance with the ethical commitment requirements

To: Hong Kong Internet Registration Corporation Limited (HKIRC)
Contract No.:
Title:

In accordance with the Ethical Commitment clauses in the Contract:
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 D – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 10 - Schedule, item no. 4 for the proposal submission deadline. If tropical cyclone warning signal No.8 or above or the black rainstorm warning is hoisted on the deadline date, the deadline will be postponed to the next working day without advance notice.
Delivery address	Hong Kong Internet Registration Corporation Limited Unit 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central, Sheung Wan, Hong Kong
Hard copies	2 copies of the full proposal are required. The proposal shall be to the attention of Elisa Chung (Finance Officer) or Bonnie Chun (Acting CEO)
Electronic copy	Electronic copy is required, on disk or by email to elisa.chung@hkirc.hk and bonnie.chun@hkirc.hk; also cc ben.lee@hkirc.hk and ben.choy@hkirc.hk. This is not a substitute for the physical copies mentioned above.
Proposal format	Specified in this document
Page count	30 pages or fewer. Stapled. Do not bind.
Font	Electronically published or typed. Times New Roman 12 point font.

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

- a persuasive section on the company background
- international recognize certification for quality assurance
- a 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

1.1 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
- Knowledge and Advices on Projects/Services
    - Understanding of our requirements
    - Advice on implementation of service

- Deliverable and Services Level
- Proposed Cost of Services and Payment Schedule
- Implementation Time Table
- Commercial and Payment Terms. e.g. Monthly or annual. Pre or post pay.

1.2 Cover Page

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

Cover Page		
Project Title		
Secondary Domain Name Service Provider		
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

1.3 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

1.4 Conflict of Interest Declaration

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

1.5 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.

1.6 Knowledge and Advices on Projects/Services

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

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

1.7 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.

1.8 Proposed Costs of Service and Payment Schedule

The vendor should provide the breakdown of the cost of the whole project/service. 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 hour, non-working hour 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.
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

1.9 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.

1.10 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 E –Technical Proficiency Tests

Once a winning bid has been selected, HKIRC may conduct a series of tests to verify the bidder's ability to handle the loads generated by our zones. The respondent should be ready to have HKIRC conduct these tests at the end of the proposal evaluation period. The following list of tests will be conducted:

1. Query Load Test This test will be used to determine the ability of the respondent to answer an appropriate amount of queries per second.

2. Update Load Test This test will be used to determine the ability of the respondent to handle high frequency, large updates, and have these propagate out to production on a timely basis.

3. IPv4/6 Query Test This test will be conducted to verify that the respondent can receive and answer queries for both A and AAAA records received using IPv4/6 transport.

4. DNSSEC Query Test This test will be conducted to verify that the respondent can serve a signed zone and respond to queries which request signed answers consistent with RFC 4033-4035 and 5155.