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

Domain Name System Security Extensions (DNSSEC) Implementation Project

Request for Proposal

Version 1
Date: 27 February 2026

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

1. Summary 1
2. Definitions 2
3. About HKIRC 3
4. Background of the Project 4
5. The Required Services 5
5.1. System Requirement 5
5.1.1 Current Systems: 5
5.1.2 General Requirement 6
5.1.3 System Requirement 7
5.2. Professional Services 10
5.3. Information Security 11
5.4. Service Acceptance 12
5.5. Contractual Consideration 12
5.6. Cost Breakdown 12
6. Limitation of Liability and Indemnity 12
7. Information Security 12
8. Project Acceptance 13
9. Anti-collusion 14
10. Offering Advantages 14
11. Ethical Commitment 15
11.1. Prevention of bribery 15
11.2. Declaration of Interest 15
11.3. Handling of confidential information 16
11.4. Declaration of ethical commitment 16
12. Schedule 17
13. Payment Schedule 17
14. Elements of a Strong Proposal 18
15. Service Agreement Negotiation and Signature 18
16. HKIRC Contacts 19
Appendix A – DNSSEC Practice Statement for the .HK and .香港 top level domain names, ...1
Appendix B – HKDNR Information Security Policy and Guidelines: An Extract Relevant to Outsourcing 1
Appendix C – Warranty 1
Appendix D – Declaration Form by Contractor on their compliance with the ethical commitment requirements 1
Appendix E – HKIRC Proposal Requirements 1
1.2 Proposal Content 2
1.3 Cover Page 3

1.4 Executive Summary 4
1.5 Conflict of Interest Declaration.....4
1.6 Company Background.....4
1.7 Methodology 4
1.8 Project Management Methodology 4
1.9 Understanding of our requirements.....4
1.10 Knowledge and Advices on Projects/Services 4
1.11 Deliverable and Services level 5
1.12 Proposed Costs of Service and Payment Schedule 5
1.13 Implementation Time Table.....5
1.14 Commercial and Payment Terms 5

1. Summary

HKIRC is going to commission an external Service Provider to implement DNSSEC for the .hk and .香港 and their sub-domains. The service shall provide complete design, building and integration of DNSSEC solution to HKDNR's existing system. The Service Provider shall provide all software, hardware and professional services in order to implement their DNSSEC solution in HKDNR environment.

HKIRC is looking for a service provider(s) ("the Contractor") to provide and setup for the above services.

The scope of service is detailed in section 4 and 5 of this document.

Parties interested in providing this service shall **submit prop osal** with the signed unilateral Non-Disclosure Agreement (NDA) (see Appendix D) to the Group **no later than 23:59pm on 20th Mar 2026**.

The Contractor should submit Expression of Interest by email to HKIRC contacts (refer to Appendix D - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix D, 1.3 Cover Page).

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 DNSSEC Implementation Service with requirements stipulated in Section 4 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 https://www.hkirc.hk .

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

4. Background of the Project

The DNS protocol can be vulnerable to attack due to an inherent lack of authentication and integrity checking of data that is exchanged between DNS servers or is sent to DNS clients. As originally designed, DNS itself does not offer any form of security and is vulnerable to spoofing and man-in-the-middle attacks. An attacker that has compromised a DNS server can gain access to all network communications that are sent by a targeted host. DNSSEC provides a way to mitigate again this.

DNSSEC includes changes to client and server DNS components that enable DNS data to be cryptographically signed and to enforce name validation policies that protect DNS communications. With DNSSEC, a DNS server can validate responses that it receives as genuine. By validating DNS responses, DNS servers and clients are protected against the single greatest vulnerability in DNS: DNS spoofing.

As the ccTLD for .hk and .香港, HKIRC is charter to provide accurate and secure Domain Name Resolution for these domains and their sub-domain. Hence it is critical that we can provide a DNSSEC supported DNS service.

Currently, HKIRC through it's fully own subsidiary HKDNR provide the following services:

- DNS for .hk and .香港 domain
- Register and registry service for provisioning of new subdomain name

It is the intend of this project to deployment DNSSEC for .hk and .香港 their sub-domain and also to offer this as an additional service to any third level domain.

5. The Required Services

The following defines the scope of service to be provided by the Contractor. There are three parts to the scope:-

- Designing of DNSSEC Solution based on the requirement of 5.1
- Build and implementation of the above solution
- Include first year support for the solution and continuous (renewable) support for the above solution for at least 48 month after the implementation

All vendors should propose for all parts any dependency for any part of the proposal.

5.1. System Requirement

5.1.1 Current Systems:

All services are provided from two Data Centres from two different geographical locations within Hong Kong. There are point-to-point connections connecting these two Data Centres

Top-level domain DNS Service:

Top-level domain DNS Service is provided by Open Sources based DNS software. Custom zone file generated from Domain Name registration system which are used to update DNS data. Full zones file generation and update once per day. Real-time Domain modification will update resource records in "stealth" master by nsupdate. Secondary DNS provider get latest zones by standard DNS zone transfer (AXFR/IXFR).

Currently there are multiple zone files of which there are some IDN domains.

Currently there are monitoring in place to monitor the DNS resolution:

- Serial Number checking for all zones
- Dig check on selected VIP domains

Domain Parking Service:

Domain Parking Service is provided by Open Sources based DNS and web server software. Subscriber's domain (must be domain served by above Top-level domain DNS Service) delegated name servers to HKIRC managed DNS servers which A and AAAA resource records

for that domain (and www.) pointed to a HKIRC managed web server which shows a simple webpage. Full zones file generation and update once per 2 hours.

DNS Hosting Service:

DNS Hosting Service is provided by Open Sources based DNS software. Subscriber's domain (must be domain served by above Top-level domain DNS Service) delegated name servers to HKIRC managed DNS servers.

Custom zone file generated from Domain Name registration system which are used to update DNS data. Full zones file generation and update once per day. Real-time Domain modification will update resource records in "stealth" master by nsupdate and rndc. Secondary DNS provider get latest zones by standard DNS zone transfer (AXFR/IXFR) and custom scripts.

HKIRC Internal DNS

Domain Parking Service is provided by Open Sources based DNS. It's to hosting HKIRC internal infrastructure that supports all above services (say DNS to resolve name server names). Domain modification will update resource records in "stealth" master. Secondary DNS provider get latest zones by standard DNS zone transfer (AXFR/IXFR).

Details will be provided on the current system once the tenderee sign the NDA.

5.1.2 General Requirement

a) Tenderer should provide hardware, software licenses and professional services as a total solution. Partial solution offer will NOT be accepted.
b) Tenderer is required to guarantee the hardware model provided in this tender will not be end-of-support by the original at least five (5) years from the delivery date of that hardware.
c) All proposed equipment must be able to function properly and reliably under the following normal Controlled Environmental conditions:
   i. Temperature 10ºC to 40 ºC operating
   ii. Humidity 20%-80% non-condensing
d) All hardware proposed should comply with the Electrical Supply Characteristics list below; otherwise the successful tender is required to provide all necessary construction work in the Primary and Secondary Data Center of HKIRC for this tender:
   i. The equipment shall be suitable for use on 220 volts +/- 6% 50Hz single phase

ii. The quality and capacity of all electrical components and cabling shall be fully equivalent to that required by the latest applicable HKSAR Electrical and Mechanical Services Department specifications.

iii. All equipment shall be fitted with 3-core 13A (Live, Neutral, Earth) fused plug for single-phase industrial type supply cable of 3M in length.

e) All proposed features must be demonstrable during tender evaluation or the proposed equipment will not be accepted otherwise.

f) All equipment that has included battery operated component(s) must have a life expectancy of no less than 10 years from the manufacture date.

g) All equipment that has included battery operated component(s) that needed to be replace in regular period shall have manufacturer warranty (battery operation) for at least five years from the date of first use.

h) All equipment that has included battery operated component(s) shall state in the event of battery failure or expire, how the component can be replace. Vendor must provide process and procedure for the replacement of such equipment, without affect the whole of the system.

5.1.3 System Requirement

This project is to provide a solution and its' implementation to HKIRC for:

- DNSSEC for all DNS service mentioned in section 5.1.1 Current Systems.

The solution provided should:

- Adhere to the latest edition following DNSSEC RFC and any referring RFC:
  - RFC 2536 - DSA KEYs and SIGs in the Domain Name System (DNS)
  - RFC 2539 - Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
  - RFC 3110 - RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)
  - RFC 3226 - DNSSEC and IPv6 A6 aware server/resolver message size requirements
  - RFC 4033 - DNS Security Introduction and Requirements
  - RFC 4034 - Resource Records for the DNS Security Extensions
  - RFC 4035 - Protocol Modifications for the DNS Security Extensions
  - RFC 4398 - Storing Certificates in the Domain Name System (DNS)
  - RFC 4470 – Minimally Covering NSEC Records and Online Signing
  - RFC 4471 – Derivation of DNS Name Predecessor and Successor

- RFC 4509 - Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
- RFC 4956 – DNSSEC Opt-In
- RFC 5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
- RFC 5702 - Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
- RFC 5933 - Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSE
- RFC 6605 - Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC
- RFC 6781 - DNSSEC Operational Practices, Version 2
- RFC 6944 - Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status
- RFC 7583 – DNSSEC Key Rollover Timing Considerations
- RFC 7646 – Definition and Use of DNSSEC Negative Trust Anchors (NTAs)
- RFC 9364 (BCP 237) – DNS Security Extensions (DNSSEC) Canonical overview and index of DNSSEC RFCs
- RFC 9824 – Compact Denial of Existence in DNSSEC
- RFC 9904 – DNSSEC Cryptographic Algorithm Recommendation Update Process

- The solution should reference to DNSSEC Practice Statement for the .HK and .香港 top level domain names (HKDPS). Note that the Practice Statement is a draft version and could subject to changes during the project. When value or method is not defined in the HKDPS, the contract should propose value or method according to their implementation experience.
- Integration with HKIRC's existing domain registration system
  - Provide interface with the web interface for DS record input and integrated with the domain registration system
  - Provide an effective method to validate the syntax of DS record inputted by client
  - Zone file validation after signing and chain-of-trust validating from/towards the root
  - Provide system alert if misconfiguration/inconsistencies in the zone are found
- Inline Signer
  - Design and build a DNSSEC inline signing system based on a "bump in the wire" architecture. ie. the DNSSEC zone signing system will sit between our "stealth master" and our DNS authoritative slaves. Zone information is done through bind compatible zone transfer.
  - Support real time zone signing when zone information created, updated and deleted.
  - Support adding/delete zone on the fly without affecting operations.
  - Support DNSSEC algorithms that mentioned in DNSSEC RFCs. (Include but not limited to RSASHA1, RSASHA256, RSASHA1-NSEC3-SHA1, RSASHA512, ECDSAP256SHA256, ECDSAP384SHA384)

- The signing process should be transparent to both the "stealth master" and the DNS authoritative slaves.
- The zone signing system should be able to replace by "dropin" replacement, without reconfiguration to "stealth master" nor the DNS authoritative slave.
- Provide interface to notify on status of the signing process, ie. success or failure
- Provide a method to validate the KSK and ZSK in all distributed zone after key roll-over
- Provide traceable logging for all signing process.
- Provide planning of switch DNSSEC algorithms without affecting operations.
- Support NSEC and NSEC3 with opt-out, random salt, iterations
- Rational zone/record update signaling to DNS authoritative slave (ie. minimize on notification to DNS authoritative slave).
- Signer should has a minimum performance of:
  - 4000 signed record per second
  - Handle more than one million zones
  - Handle more than one million records per zone
  - Scalable performance with addition hardware within the same box to at least 5 times current performance
- High availability with data replication for key management system as well as DNSSEC signer function include active/passive standby within site and site over different geological location
- Rational handling of Zone file serial number
  - Handle any zone serial number update either transparently or a rational serial numbering scheme.
  - Handle serial number change issue by "stealth master"
- Role based system administration according to DNSSEC Practice Statement of HKIRC including segregation of duty.
- Support full suite of performance and system state/statistic monitoring matrix, eg. CPU loading, RAM usage, zone/record signed, current record per second etc.
- If the proposed architecture of the singer is not inline signer, please specific how the architecture require to be change and include all the necessary hardware, software and professional cost for consideration.

- Provide robust and executable disaster recovery facility and procedures to perform emergency recovery actions to resume service within shortest possible time.
- Support Key Management through either HSM or equivalent:
  - Support all key generation standards as stated above RFCs.
  - Support full key lifecycle, ie. create, publication, activation, de-activation and deletion. Please give details in your proposal on how your solution supports the key lifecycle, eg. different key publication method, key generation method, key

publication timeline control etc.

- Support schedulable key lifecycle for KSK and ZSK using both absolute and relative days and actual date.
- Provide method(s) to perform KSK ceremony.
- Support schedulable NSEC3 random salt (re)generation.
- Support secure importing and exporting of keys for backup and restoring.
- Validated to Security Standard eg. FIPS, RSA, Common Criteria etc.
- High availability with data replication for key management system, include active/passive failover within site and site over different geological location.
- Key generation and management according to DNSSEC Practice Statement of HKIRC including segregation of duty.
- Key generation minimum performance:
  - 4,000 signature per second
  - Scalable performance with addition hardware within the same box to at least 5 times current performance
- Support full suite of performance and system state/statistic monitoring matrix, eg. CPU loading, RAM usage, signature generated, current signature per second etc.
- Support secure online/offline storage of keys.
- Support Emergency Key Rollovers:
  - Support rollover keys out-of-schedule
  - Support emergency regeneration of keys

- Provide process and procedure that does not affect the operation of the system for replacement of any battery operated component that is for:
  - Failure before life expectancy of battery as stated in Section 5.1.2 f)
  - After warranty as stated in Section 5.1.2 g)

5.2. Professional Services

HKDNR is looking for partner that has previous successful experience in implementing DNSSEC solution in ccTLD level. The partner should be able advice on any operation and design consideration for implementing DNSSEC system for .hk and .香港.

The professional services for this Project should cover the following:

- Operational and design advice/recommendation
- Design and build an DNSSEC system based on the requirement of HKDNR
- Procurement and delivery of all system component for this project based on the above design
- Equipment commission service, including equipment mounting, software installation and configuration.

- Interface specification to HKDNR registration system
- Performance benchmarking for proposed system.
- Documentation on design, setup guide and operational/administration procedures including:
  - System design guide
  - System installation and configuration guide
  - System operational/administration guide:
    - Daily operation guide
    - Recurring task guide
    - System Failover/Recovery guide based on different failure mode/scenario, impacts and estimate of Time to Recover.
- Perform complete failover and recovery drill before system commission.
- Preform DNSSEC Infrastructure Audit based on but not limited to DNSSEC Infrastructure Audit Framework, NLnet Labs Document 2013-002 Version 1.0. Section 4, 5, 6, 8, 9 and 10.
- Deployment plan for system in phases with fallback plan for each phase.
- Support for system during deployment phases (multiple phases). Tentative deployment schedule for HKDNR DNSSEC System are as follows:
  - Phase 1 Signing of .hk and .香港 root zone with IANA. Within nursing period.
  - Phase 2 Signing of zones, eg. .idv.hk, .net.hk etc. Within 3 months from ending of nursing period.
  - Phase 3 Signing of zone, eg. .com.hk, gov.hk. Within 3 months from ending of nursing period.
  - Phase 4 Signing of remaining zones, eg. .org.hk, IDN. Within 3 month from ending of nursing period.
- Nursing period for the system will be 3 month after system goes into production.
- Continuous system support for 12 month after system commission.
- Standby real time failover drill support 6 month after system commission.
- Standby real time for first top and second level KSK key rollover (within 6 month after commission)
- All equipment and service supplied shall come with 24x7 service support contract.

5.3. Information Security

- The Contractor shall follow HKIRC Information Security Policy and Guidelines set out by HKIRC on personal and co-operation data security.
- Contractor's Information Security Policy is subject to HKIRC review if needed.

5.4. Service Acceptance

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

1. Delivery, setup of equipment
2. Services provided by professional service
3. Functionality of the integrated system
4. System Performance
5. Documentation, knowledge transfer and training
6. Performance of monitoring system & reporting system
7. Quality of service provided

Under this acceptance framework, the vendor should fulfill the scope of services described in section ”The Required Services”. In addition, interested vendors may provide additional acceptance criteria and the related plan in detail in their proposals.

5.5. Contractual Consideration

Contract should include all requirements from this RFP. All vendors should propose for all parts of the scope in the RFP. HKIRC reserve the right to take up any part or parts of the each proposal.

5.6. Cost Breakdown

The vendor should breakdown all cost by Capital Expenditure (CapEx) and Operational Expenditure (OpEx). Vendor should justify the cost of OpEx, if it exceeded 10% of CapEx.

6. Limitation of Liability and Indemnity

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

7. 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.

8. Project Acceptance

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

1. Delivery, setup of equipment
2. Services provided by professional service
3. Functionality of the integrated system
4. Performance of monitoring system & reporting system
5. System Acceptance Test
6. User Acceptance Test
7. Documentation, knowledge transfer and training
8. System Failover/Recovery Drill
9. System commissioning
10. Ending of nursing period

9. 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.

10. 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.

11. Ethical Commitment

11.1. 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.

11.2. 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).

11.3. 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.

11.4. 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.

12. Schedule

	Project schedule		
	Tasks	*To be Completed by*	*Remark*
1	Publish RFP	27/2/2026	
2	Sign NDA and InfoSec Compliance Statement with all interested vendors	27/2/2026 to 20/3/2026	
3	Deadline for vendors to submit proposal and quotation	20/3/2026, 23:59pm	
4	Selection of vendor by panel	16/4/2026	
5	Conclude final decision and appoint the vendor	11/6/2026	
6	Prepare service agreement contract	26/6/2026	
7	Sign service agreement contract with the appointed vendor	26/7/2026	
8	Service implementation	26/7/2026	
9	Service commencement	30/10/2026	
10	Nursing period	31/10/2026	
11	Project Complete	31/1/2027	

13. Payment Schedule

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

	Milestone/Acceptance	**Payment**
1	Delivery of Hardware & Software	30%
2	Hardware & Software Installation and configuration Acceptance	20%
3	System performance and SAT/UAT Intergation Acceptance	30%
4	End of nursing period	20%
	TOTAL	**100%**

14. Elements of a Strong Proposal

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

15. 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.

16. HKIRC Contacts

HKIRC Contacts information

Cntacts	
Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong +852 23192303 – telephone +852 23192626 – fax https://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**Senior IT Manager** John Lam +852 23193811 john.lam@hkirc.hk

Appendix A – DNSSEC Practice Statement for the .HK and .香港 top level domain names,

Provide after signing of NDA

Appendix B – 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 C – 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 tender of Domain Name System Security Extensions (DNSSEC)" Implementation Project:

(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 D – 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.:
Title:

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 E – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 12 - 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	Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong http://www.hkirc.hk
Electronic copy	Electronic copy is required, by email to john.lam@hkirc.hk; and cc to it-procurement@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.

1.2 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 Advices on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Time Table
- Commercial and Payment Terms. e.g. Compensation for delay.

1.3 Cover Page

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

Cover Page		
Project Title		
		Domain Name System Security Extensions (DNSSEC) Implementation Project
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

1.4 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

1.5 Conflict of Interest Declaration

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

1.6 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.

1.7 Methodology

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

1.8 Project Management Methodology

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

1.9 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 on the requirements listed in the scope of service section; and briefly explain how they are achieved.

1.10 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.

1.11 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.

1.12 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.

1.13 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.

1.14 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.