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

Cybersecurity Information Sharing Platform Hosting Services 2023

Request for Proposal

Version 1.0
Date: 7 October 2022

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

Table of Contents

Contents

Summary

Cybersec Infohub is a partnership programme jointly administered by the Office of the Government Chief Information Officer (OGCIO) and the Hong Kong Internet Registration Corporation Limited (HKIRC) to promote closer collaboration among local information security stakeholders of different sectors to share cyber security information and jointly defend against cyber attacks under the platform "Cybersechub.hk".

This tender is to invite Proposals from eligible vendors for the hosting service of the "Cybersec Infohub" cybersecurity information sharing platform ("The Platform").

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

The scope of service is detailed in section 3 of this document.

Parties interested in providing this service shall submit **Proposal by no later than 12:00 noon, 24 October 2022 (Mon)**.

The service commencement date of this project is tentatively on **1 Dec 2022.**

1. 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”.

“The Services” means the hosting service for “Cybersec Infohub” cybersecurity information sharing platform with requirements stipulated in Section 3 of this document.

“RFP” means this Request for Proposal

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

2. About HKIRC

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

HKIRC 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).

3. Scope of Service

3.1 This Brief of Work Assignment (the "Brief") is to invite interested service providers to submit proposals for the Provision of Hosting Services (the "Services") for the "Cybersec Infohub" Cyber Security Information Sharing and Collaboration Platform (the "Platform").

3.2 The Contractor shall conduct the security risk assessment and audit ("SRAA") services for the Platform. The cost for conducting the SRAA shall be quoted under Contract Schedule 1 – Price Summary (a) in Appendix B.

3.3 The Contractor shall provide hosting services to host the Platform through public cloud service as well as other related services necessary for fulfilment of this Work Assignment. The cost for hosting services shall be quoted under Contract Schedule 1 – Price Summary (b) in Appendix B. The tentative start date of the hosting service is 1st February 2023 (or such a later date asspecified HKIRC). The subscription period of the hosting services shall take effect from the tentative start date and continue in force for a period of twelve (12) calendar months until 31 January 2024.

3.4 All requirements specified in Section 4 to Section 9 are essential requirements. Proposals which fail to meet any of the essential requirements in these sections shall be disqualified and shall not be considered further.

4. Project Requirements

4.1 Hosting Requirements

4.1.1 The Contractor shall comply with the following hosting requirements for the production environment of the Platform:

(i) Manage the hosting environment in MS Azure tailor for HKIRC and assign HKIRC to be the global admin of the environment

(ii) Backup the existing MS Azure Monitoring Resources e.g. Action Group and Metric alerts settings

(iii) Backup Setting on application gateway

(iv) Take snapshot on resources in existing subscription which including all VMs and MySQL DB

(v) Migrate Implementation from existing Azure Tenant to New Tenant

(vi) Provide at least eleven (11) dedicated instances of virtual machine (VM) running in Linux x86_64 (Kernel v4.4+) and meet with the requirements of hosting environment as specified in Appendix **C**;

(vii) Support hosting of the Platform developed in JavaScript and Python and supportMySQL, API interfacing, AI services and the like;

(viii) Host in data center in Hong Kong attained with ISO 9001 and ISO 27001

certification;

(ix) Support SSH access for cloud instances;

(x) Able to detect failed VM instances and automatically redeploy new instances to

replace. The newly deployed instances should have the same IP addresses of failed

instances;

(xi) Support sending of emails generated by the Platform to Internet and support receiving incoming Internet emails; and

(xii) Able to route all traffic of web servers to maintenance page to be provided by the Contractor during maintenance period.

4.2 Infrastructure Requirements

The Contractor shall comply with the following infrastructure requirements:

4.2.1 Provide and guarantee a dedicated network connectivity of at least 100Mbps to the Internet;

4.2.2 Provide dedicated static public IPv4 and IPv6 IP addresses to allow access to the Platform from the Internet;

4.2.3 Provide encryption for both data at rest and data in transit;

4.2.4 Support the use of Transport Layer Security (TLS) to establish secured sessions with web clients. The infrastructure shall support 2048 bit SHA256 digital certificate and support HTTP Strict Transport Security (HSTS). The Contractor shall install and configure the digital certificate to be acquired by HKIRC;

4.2.5 Provide, operate and maintain load balancers with necessary configuration to ensure that the serviceability shall meet the requirements as specified in Section 8 of the Brief;

4.2.6 Provide Content Delivery Network (CDN) services, with provision of necessary configuration, to support the delivery of web contents to Internet users at high service availability;

4.2.7 Provide virtual private network (VPN) connection between HKIRC or its authorized party, and the hosting environment;

4.2.8 Receive service calls / requests and to provide technical advice and support to resolve any technical and ongoing issues for the Services;

4.2.9 Provide, operate and maintain firewall and web application firewall (WAF), with provision

of customization to block malicious activities, including but not limited to malicious traffic, SQL injections, cross-site scripting, etc. and perform necessary actions for ensuring smooth operations of the Platform. It shall include Open Web Application Security Project (OWASP) ModSecurity core rule set in the WAF;

4.2.10 Carry out a stress test before production launch of the Platform to ensure the stability of the Platform subject to the advice given by the Platform Services Provider;

4.2.11 Configure, manage and regularly review the access control lists (ACL), firewall rules, web application firewall rules and other security policies for ensuring efficient and secure operations of the Platform;

4.2.12 Implement and carry out change management to ensure that such changes are properly analyzed, approved, documented and communicated to the appropriate parties where necessary; and

4.2.13 Provide Distributed Denial of Service (DDoS) protection service with at least 10Gbps mitigation of DDoS to stop illegitimate volumetric traffic.

4.3 Security Monitoring Services Requirements

4.3.1 The Contractor shall provide 24 x 7 (24 hours a day and 7 days a week) real time intrusion detection, monitoring and management, which shall include but not limited to network and host intrusion detection and monitoring, logs review and reporting.

4.3.2 The Contractor shall assure that all the necessary information is being logged and stored appropriately and be able to provide relevant operational event data and logs upon request.

4.3.3 The Contractor shall escalate any detected cyber security incident or abnormal activity according to pre-defined escalation procedure within 15 minutes of detection and take necessary actions to contain the situation and minimize the impact.

4.3.4 The Contractor shall provide an intrusion detection and monitoring report stating details of the incident should a security incident or abnormal activity be detected.

4.3.5 The Contractor shall provide continuous monitoring on the availability of the Platform, and utilization on the VMs and bandwidth (e.g. CPU utilization, disk-IO usage, storage usage and bandwidth) in maximum 5 minutes interval with alert features and notify HKIRC in case of any critical alert according to pre-defined procedure.

4.3.6 The Contractor shall provide weekly vulnerability scanning and carry out continuous monitoring on malicious code detection, defacement detection and security incident monitoring. The Contract shall alert HKIRC according to pre-defined procedure.

4.3.7 The Contractor shall prepare an "Operation and Incident Handling Procedure" to be mutually agreed with HKIRC before production launch of the Platform. In case of any service outage or incident, the Contractor shall follow the procedures for handling.

4.4 **Technical Support Services Requirements**

4.4.1 The Contractor shall assign a 24 x 7 telephone support hotline (including Saturday, Sunday and public holidays) for HKIRC and the Platform Service Provider to place service calls during the Contract Period.

4.4.2 The Contractor shall provide 24 x 7 support services and the Contractor shall be able to respond to service related incidents and/or requests submitted by HKIRC and the Platform Service Provider within one hour from the time when a service request is placed through the Contractor's hotline.

4.4.3 The Technical Support Services shall cater to an unlimited number of service calls/requests.

4.4.4 The Contractor shall carefully schedule system maintenance tasks to avoid/minimize service interruption and agree with user on the schedule, possible impact and fall- back/recovery procedure if such is inevitable. The Contractor shall work with the Platform Service Provider to devise the disaster recovery plan for the Platform.

4.4.5 The Contractor is responsible for ensuring the resilience and redundancy of cloud service, etc., such that the serviceability can meet the requirements as specified in this Brief.

4.4.6 The Contractor shall perform fine-tuning for the network configuration to ensure that the network traffic is smooth and is optimized.

4.4.7 The Contractor shall inform HKIRC of any software patch is available, and by HKIRC's approval, provide the software patch installation (including but not limited to security patches, software fixes and updates, major release) and firmware upgrade for the affected server/equipment to remove any new/known vulnerabilities identified by hardware/software manufacturers. The supply of these updates shall be applied to all the VMs as required in the

Brief and shall be made available to HKIRC within one month after the date of the release by the manufacturer/developer. In case there is critical vulnerabilities, the Contractor shall handle the vulnerabilities immediately to mitigate the risk.

4.4.8 HKIRC shall not be liable for any cost for any patches upgrade / installation / and related configuration services.

4.4.9 Around the end of the Contract Period or when the Contract is to be terminated for whatever reason, the Contractor shall co-operate with the next contractor engaged by HKIRC to ensure smooth migration of the Services.

4.4.10 The Contractor should provide a ticket system for tracking case.

4.5 **Backup Services Requirements for the Production Environment**

4.5.1 The Contractor shall be responsible for all necessary precautions to protect and recover the programs, data stored in the servers, the configuration of the servers, network equipment and system software provided by the Contractor.

4.5.2 The Contractor shall provide backup service of the Platform, including virtual machine instances, snapshots and related configurations. Backup shall be performed according to the following schedule:

Backup Type	**Frequency**	**Retention Period**
Daily Full Backup	Daily	7 days
Weekly Full Backup	Weekly	4 weeks

4.5.3 The backups of the Platform should be kept securely.

4.5.4 The Contractor shall provide ad hoc manual backup and restore services on HKIRC's request.

4.5.5 The Contractor shall provide integrity checking of backup data to ensure data integrity.

4.6 **Reports Requirements for the Production Environment**

4.6.1 The Contractor shall produce the following performance figures for the regular monitoring of the utilization of the Platform, to be included in a report ("Monthly Consumption and Usage Report"):

(i) CPU utilization;

(ii) Memory utilization;

(iii) Bandwidth utilization;

(iv) CDN, load balancer, firewall, and web application firewall related statistics;

(v) Service availability for the month; and

(vi) Configuration/ Application changes made.

4.6.2 The Contractor shall produce regular reports based on the statistics and related information of service activities, security alerts, and changes of ACL or ruleset, to be included in the Monthly Consumption and Usage Report.

4.6.3 The Contractor shall provide ad-hoc reports if any security incidents / cyber attacks occurred or upon request by HKIRC Representative.

4.7 **Requirements on SRAA for the Platform**

4.7.1 The Contractor shall conduct the SRAA for the Platform before its production launch if there are hosting migration.

4.7.2 The Contractor shall reference the documents as mentioned in Section 7.2 (e) when performing the SRAA. The requirements listed in these reference documents together form the "Security Baseline" for the assessment and audit.

4.7.3 The Contractor shall gather all relevant information such as security requirements and objectives, system and network architecture and infrastructure, applications and servers information, access controls, identification and authentication mechanisms, documented or informal policies and guidelines, operational processes, etc. of the Platform by performing multi-level interviews, group discussions, surveys, equipment and configuration checking etc., where appropriate. The Contractor shall perform general control review to identify any inadequacies in general controls being put in place for the current environment by examining the systems manually for their control and procedures which may include, but is not limited to, the following:

(i) Management responsibilities;

(ii) IT security policies;

(iii) Human resource security, including security awareness training;

(iv) Asset management;

(v) Access control, such as access privileges;

(vi) Cryptography;

(vii) Physical and environmental security;

(viii) Operations security;

(ix) Communications security;

(x) System acquisition, development and maintenance;

(xi) Outsourcing security;

(xii) Security incident management;

(xiii) IT security aspects of business continuity management; and

(xiv) Compliance

A checklist to conduct the general control review should be prepared and be agreed upon by HKIRC before the assessment or audit commence.

The checklist must include tasks to check against

i) Security Regulations;
ii) Baseline IT Security Policy (S17), in particular the 14 areas listed in section 2.1 of S17;
iii) Security Checklist for iAM Smart-enabled Online Services;
iv) IT Security Guidelines (G3);
v) OGCIO IT Security Policy;
vi) Practice Guide for Information Security Incident Handling (ISPG-SM02);
vii) Practice Guide for Cloud Computing Security (ISPG-SM04);
viii) Practice Guide for Internet Gateway Security;
ix) Practice Guide for Website and Web Application Security;
x) Practice Guide for Penetration Testing; and
xi) HKIRC Information Security Policy; and

that are relevant to and are within the scope of the assessment or audit. The audit follow the Practice Guide for Security Risk Assessment & Audit (ISPG-SM01) published by OGCIO

After assessment or audit, result of the checklist should be submitted to HKIRC. Reasons for not performing any tasks in the checklist must be provided.

4.7.4 The Contractor shall perform vulnerability scanning at network, hosts and systems which should at least cover the following where appropriate:

(i) Network level probing/ scanning and discovery

(ii) Host vulnerability tests and discovery, including but not limited to password audits and identification of database mis-configurations

(iii) Web application and API vulnerability scanning, including but not limited to Open Web Application Security Project (OWASP) Top 10 vulnerabilities and OWASP API Top 10 vulnerabilities

(iv) Penetration testing, including but not limited to OWASP Top 10 vulnerabilities, input validation, injection, session manipulation, brute-force password attacks and exploiting vulnerabilities, etc.

(v) Code review, including but not limited to examine written application codes

(vi) Configuration review, including but not limited to examine configuration settings within the system and application.

(vii) System/application (including web system/application) scanning;

and prepare a vulnerability scanning detailing the tests conducted and the test results upon completion of the tests. The system/application scanning shall also cover scanning of web systems and applications via the Hyper Text Transfer Protocol (HTTP), including HTTP Secure (HTTPS).

4.7.5 The Contractor shall perform web penetration testing which should at least cover the following:

(i) Conduct manual penetration testing which covers the latest version of the top ten most critical web application security risks of the OWASP, logical flaws, error handling and system information leakage, file uploading and execution and input validation issues;

(ii) Bring in all tools for the use of the testing and ensure that all hardware/firmware/software used in the testing is legal and properly licensed;

(iii) Log the actions taken with evidence (such as screen capture or program logs), clean up and restore any changes that are made during the testing;

(iv) Explain and analyze the identified vulnerabilities for its likelihood and impact to the

website/web application; and

(v) Prepare a web penetration testing report detailing the test progress, the test results, and recommendation upon completion of the tests.

Before conducting the vulnerability scanning and/or web penetration testing, the Contractor should agree with HKIRC on the scope, possible impact and fallback/recovery procedure.

4.7.6 The Contractor shall perform risk analysis on every aspect which shall include, but is not limited to, the following:

(i) Human resource security;
(ii) Asset management;
(iii) Access control;
(iv) Cryptography;
(v) Physical and environmental security;
(vi) Operations security;
(vii) Communications security;
(viii) System acquisition, development and maintenance;
(ix) Outsourcing security; and
(x) IT security aspects of business continuity management

to determine the value of the assets and their associated risks through the following processes:

(i) Asset identification and valuation;
(ii) Threat analysis;
(iii) Vulnerability analysis;
(iv) Asset/threat/vulnerability mapping;
(v) Impact and likelihood assessment; and
(vi) Risk results analysis.

4.7.7 The Contractor shall identify and recommend safeguards based on the results of risk analysis in order to reduce the likelihood and impact of identified threats and vulnerabilities to an acceptable level.

4.7.8 The Contractor shall document the findings and results of the security risk assessment and vulnerability tests in a report (“Security Risk Assessment and Audit Report”).

4.7.9 The Contractor shall conduct a presentation to HKIRC to report the findings of the security risk assessment.

4.7.10 The Contractor shall identify and review relevant statutory, regulatory and contractual requirements.

4.7.11 The Contractor shall check for conformance to existing security policies, standards, guidelines and procedures.

4.7.12 The Contractor shall document the findings and results of the security audit in the Security Risk Assessment and Audit Report.

4.7.13 The Contractor shall conduct a presentation to HKIRC to report the findings of the security audit.

4.7.14 The Contractor shall verify the security status after implementation of safeguards to ensure that all risks identified have been mitigated or reduced to an acceptable level with regard to the recommendations provided in the Security Risk Assessment and Audit Report.

4.7.15 The Contractor shall document the details, findings and results of the verification in a report ("Verification Report").

4.7.16 The Contractor shall ensure that the services provided have minimum impacts on the daily operation of HKIRC and related parties.

4.7.17 The Contractor shall carefully schedule all activities (in particular for vulnerability tests) to avoid/minimize service interruption and agree with user on the schedule, possible impact and fallback/recovery procedure.

4.7.18 The Contractor shall provide the software and equipment, if necessary, for carrying out the tasks free of charge to HKIRC.

4.7.19 The Contractor shall ensure that the security level of the system and network is not affected due to the installation and configuration of any necessary software and equipment. Remove those software and equipment and restore any necessary system and network configuration upon termination or completion of the Work Assignment such that the security level and the operation of the system and network is not affected.

4.7.20 The Contractor shall ensure that no malicious software (e.g. computer malware, worm, Trojan horse program), backdoor or anything which would disrupt the operation or lead to compromise of any system is embedded in either the information or its storage media (e.g. in the form of data file, database, document, program code, e-mail, hard disk, CD/DVD-ROM) when they are disseminated and/or exchanged with HKIRC.

4.8 Other Requirements

4.8.1 HKIRC shall not be liable for any cost for any software / tools / equipment necessary for fulfillment of this Work Assignment.

4.8.2 The Contractor shall cover all labor charges incurred for fulfillment of this Work Assignment.

4.8.3 The Contractor shall exercise all due and reasonable skill, care and diligence in its delivery of the Services and in a professional manner in accordance with the time schedule stipulated in the Contract.

4.8.4 The Contractor shall comply with all reasonable instructions of HKIRC Representative in so far as they are applicable to the responsibility of the Contractor.

4.8.5 The Contractor shall, through HKIRC Representative, keep HKIRC informed of all matters related to the Services within the knowledge of the Contractor and shall answer all reasonable enquiries received from HKIRC Representative.

4.8.6 The Contractor shall, upon request by HKIRC Representative, attend all meetings convened by HKIRC Representative and shall advise and assist HKIRC Representative on all matters relating to the duties of the Contractor.

5. Manpower Requirements

5.1 The composition of the Contractor's assignment team ("Project Team") shall include at least the following roles meeting the requirements specified in the table below. The role of Service Manager and Service Specialist shall not be taken up by the same person.

Role	**Responsibilities**	**Requirements**
Service Manager	Overall management of the project	• Shall have at least **ten (10)** years of IT experience including at least **three (3)** years of project management
Service Specialist	Technical review, design, recommendation of areas in servers, storage, networks and security infrastructure of the Platform	• Shall have at least **six (6)** years of IT experience including at least **two (2)** years' working experience in cloud infrastructure/services
Web Application Security Advisor **(This role <u>may or may not</u> be taken up by one of the team members who act as the Service Manager / Service Specialist)**	Providing advice on web application security aspects to the Platform Service Provider	• Shall have at least **six (6)** years of IT experience including at least **two (2)** years' working experience in web application security
Security Consultant **(This role <u>shall not</u> be taken up by any team members who act as the Service Manager / Service Specialist / Web Application Security Advisor)**	Conducting the SRAA for the Platform (Shall not involve in any tasks related to the provision of hosting services for the Platform)	• Shall have at least **six (6)** years of IT experience including at least **three (3)** years of working experience in IT security risk assessment and audit • Shall possess at least one **valid** qualification / certificates related to IT security risk assessment audit (e.g. CISSP, CISA, CISM, etc.)

5.2 The cut-off date for counting the experience of the members of the Project Team is the closing date for proposal submission.

5.3 The submitted proposal should describe how the assignment team would be structured in providing the Services, and should provide a full description of the experience of all designated team members and their proposed roles in the Work Assignment.

6. General Requirements

6.1 Service providers and their offered services will comply with or exceed the general requirements, security requirements, manpower requirements, and technical requirements. The following general requirements shall be satisfied in fulfillment of this Work Assignment:

6.2 The Services offered shall include but not be limited to the following set-up measures:

6.2.1 Be a secure and reliable 24 x 7 non-stop service.

6.2.2 Built-in with the resilience that the switch-over operation be performed in an automatic manner and be transparent to HKIRC.

6.2.3 Built-in with the business continuity capability and be resided in a minimum of two different geographic sites to avoid service outage during disaster situations.

6.2.4 Provide usage management capability where service usage can be monitored, controlled and/or reported.

6.3 The Services offered shall include but not be limited to the following implementation measures:

6.3.1 Be designed for business use and be interoperable and compatible with the existing hardware, software, networking devices mentioned in the Specifications document provided by HKIRC.

6.3.2 Built-in with the capability that no user data loss or loss of user data access after service disruption.

6.3.3 Support rapid and elastic service provisioning and de-provisioning, such that the service being provisioned or de-provisioned often appear to be unlimited and can be purchased in any

quantity at any time.

6.3.4 Provide dedicated support resources to HKIRC in relation to the provisioning of hosting service.

6.3.5 Provide an exit plan to HKIRC within one month after the implementation of the service.

6.3.6 Report any critical incident to HKIRC within four hours after it has occurred.

6.3.7 Complete any non-critical incident or provide reasonable explanations within five working days after it has occurred.

6.3.8 Provide a solution or work-around in response to a helpdesk enquiry within 24 hours after it has been raised by HKIRC.

6.4 The Services offered shall include but not be limited to the following additional implementation measures:

6.4.1 Support provisioning of practically scalable storage, network bandwidth, computing power and memory.

6.4.2 Provide documented procedures, Application Programming Interfaces (APIs) or other electronic means for the HKIRC Representative to export or extract their corresponding user data any time.

6.4.3 Have the capability for the HKIRC Representative to perform the corresponding user data migration, and data destruction upon expiry, completion or termination of the Contract, or requested by HKIRC.

6.5 All HKIRC data, information, drawings, specifications, documents, contracts, plans, design materials, data and other materials furnished by or on behalf of HKIRC in connection with this Contract shall be treated as confidential information. The Contractor shall not, during the continuance of this Contract or at any time thereafter, disclose to any person the terms and conditions of this Contract, or any confidential information.

7. Security Requirements

7.1 The service providers and their offered services will comply with or exceed the general

requirements, security requirements, manpower requirements, and technical requirements. The following security requirements shall be satisfied in fulfillment of this assignment:

7.2 The Services offered shall include but not be limited to the following set-up measures:

a) Store all user data processed by the Services in data centres accredited with one or more International standards in information security management like ISO/IEC 27001, or audited with the Statement on Standards for Attestation Engagements (SSAE) No. 16 or equivalent, where applicable.

b) Enable password protection on per user, user group or role basis to protect the access to the Services with one or more of the following measures to be implemented:

- Anti-password guessing mechanism
- Configurable timeout period
- Password aging

c) Have the anti-malware service enforced to protect HKIRC against malware, worms, trojan horses, spyware and malicious code, etc., wherever applicable.

d) Ensure the anti-malware service to be run with the most appropriate or up-to-date list of malware signatures.

e) Comply with the Security Regulations. The following OGCIO policy and guidelines shall also be followed as appropriate:

- Baseline IT Security Policy (S17)
- OGCIO IT Security Policy
- Security Checklist for iAM Smart-enabled Online Services
- Practice Guide for Security Risk Assessment & Audit (ISPG-SM01)
- Practice Guide for Information Security Incident Handling (ISPG-SM02)
- Practice Guide for Cloud Computing Security (ISPG-SM04)

These policies and guidelines are accessible through the following URL:
(https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/)

f) Comply with all security, confidentiality and data protection principles of the Personal Data (Privacy) Ordinance requirements.

g) Be processed under an end-to-end encryption environment and/or as required by the Specification on IT security.

7.3 The Contractor shall include but not be limited to the following implementation measures:

a) Not disclose any data or information relating to the Services to any external parties and not use those data or information for other purposes.

b) Report any vulnerability, its resolution and/or any workaround to HKIRC, if security vulnerability is reported on the Services.

c) Resolve the vulnerability as soon as technically feasible, without any charges to HKIRC.

d) Support the Platform Service Provider engaged by HKIRC to install, configure and test the Platform in the hosting environment.

e) Support the Platform Service Provider engaged by HKIRC to perform system update and patching for the Platform.

8. Service Level Requirement

8.1 The Contractor shall warrant that the hosting cloud services shall achieve at least the minimum service availability for the month of **99.5%.**

9. Project Deliverables and Implementation Schedule

9.1 The tentative start date of this Work Assignment is **1 December 2022**. The ImplementationSchedule is as follows. The Contractor shall complete the service to the satisfaction of theHKIRC in accordance with the required tasks and deliverables listed.

No.	Major Task	Deliverable(s)	Tentative Completion Date	No. of calendar months for subscription of hosting services
Stage 1: Pre-production setup and related tasks (for Dec 2022 to January 2023)				
1	Prepare Project Plan for the Work Assignment	Project Plan, Operation and Incident Handing Procedure	10 Dec 2022	2
2	Setup, configure, migrate and provide hosting services for the Platform		20 Dec 2022	
3	Perform SRAA for the Platform			
3.1	Carry out SRAA for the Platform	Security Risk Assessment and Audit Report	20 Jan 2023	
3.2	Review the security status after implementation of safeguards	Verification Report	25 Jan 2023	
4	Rollout of the Platform for Production		31 Jan 2023	

Stage 2: Hosting services for the Platform (for Feb 2023 to Jan 2024)*				
5	Provide hosting services for the Platform	Monthly Consumption and Usage Report	31 January 2024	12

*The subscription period of the hosting services shall take effect from the tentative start date (1 December 2022) and continue in force for a period of fourteen (14) calendar months until 31 January 2024.

10. Payment Schedule

10.1 Payment for this Work Assignment should be made as follows:

Payment Milestone (PM)	Implementation State (as stipulated in Section 9.1 of the Brief)	Service Period	Payment
PM1	Stage 1	Dec 2022 – Jan 2023	(A) + (B) x 2
PM2	Stage 2	Feb 2023 – Jul 2023	(B) x 6
PM3	Stage 3	Aug 2023 – Jan 2024	(B) x 6

where:
(A) refers to the total price of SRAA as quoted in Contract Schedule 1 – Price Summary; and
(B) refers to the total price of hosting services per month as quoted in Contract Schedule 1 – Price Summary.

10.2 Upon completion of the deliverables submitted by the Contractor to the satisfaction of HKIRC Representative, HKIRC will issue a written notice to the Contractor. Payment will be made to the Contractor upon completion of each payment milestone. The Contractor shall produce an invoice for the sum becoming payable to the named person to be informed by HKIRC.

10.3 Should the Contract be terminated for whatever reason, HKIRC will be obligated to pay for only the pro rata portion of the work that has been completed by the Contractor before such termination. The Contractor shall bear at its own cost arising from the early termination of the Contract and shall not be entitled to claim for whatever compensation from HKIRC.

11. Acceptance Criteria

11.1 HKIRC will only accept the delivered services if:

(a) All implementation services and associate deliverables as specified in Section 4 above are completed in accordance with the required schedule and adhere to HKIRC standards stipulated in Section 12 below and are with acceptable quality; and
(b) All the project objectives as well as requirements as specified in Section 3 and Section 4 above are met satisfactorily.

11.2 HKIRC will require in general up to 14 days to consider each required deliverable and, if itdeems appropriate, to confirm the acceptance of the deliverable.

11.3 For the approval of acceptance of the last assignment deliverable of Stage 1 – Pre-production setup and SRAA, the Contractor should assure HKIRC that all assignment
deliverables, including the Platform, should have been delivered satisfactorily and is acceptable to HKIRC.

11.4 HKIRC will only accept the on-going Hosting services for the Platform (Stage 2-3)if:

(a) the Contractor produces all agreed deliverables for the services required and are with acceptable quality; and (b) the Contractor complies with the requirement as specified in Section 4 above.

12. Information Security

The Tenderer shall acknowledge and agree that, if the Tenderer is selected as the Contractor, it shall be bounded by our Non-Disclosure Agreement (NDA) and Information Security Policies. The Tenderer shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

The Tenderer shall be provided with a set of NDA and Information Security Compliance Statement after HKIRC received The Tenderer'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 the NDA and 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 HKIRC's staff and Board of Directors of HKIRC.

The Tenderer shall comply with the following HKIRC security policy and guidelines, to the extent that match with their roles and responsibilities. Nonetheless, the Contractor hereby refers to all relevant staff members of Contractor and those of any other subcontractors under the Contractor's purview.

1. Information Security Policy;
2. Information Security Guideline; and
3. Information Security Classification Guideline.
4. Other regulations, OGCIO policy and guidelines mentioned in Section 7.2 e).

Herein, HKIRC would also set the expectation of the Tenderer 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.

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

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

14. 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.

15. Ethical Commitment

15.1. 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.

15.2. 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).

15.3. 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.

15.4. Declaration of ethical commitment

(g) The Contractor shall submit a signed declaration in a form (see Appendix F) 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.

16. Schedule

	Project schedule	
	Tasks	*To be Completed by*
1	Publish RFP	7 October 2022
2	Express of Interest	14 October 2022
3	Sign NDA and InfoSec Compliance Statement with all interested vendors	19 October 2022
4	Deadline for vendors to submit proposal and quotation	24 October 2022, 12:00 noon
5	Selection of vendor by panel	Nov 2022
6	Conclude final decision and appoint the vendor	Nov 2022
7	Prepare service agreement contract	Nov 2022
8	Sign service agreement contract with the appointed vendor	Nov 2022
9	Service commencement	1 Dec 2022
10	Service implementation - SRAA	Jan 2023
11	Service implementation - Hosting	Last until 31 Jan 2024

17. Elements of a Strong Proposal

All submitted Proposal must following the format as stated in Appendix A - 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
- 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

18. Service Agreement Negotiation and Signature

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

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

19. HKIRC Contacts

HKIRC Contacts information

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong +852 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.*	**Cybersecurity Manager** Arktos LAM +852 2319 3863 arktos.lam@hkirc.hk **Project Manager** Kinson Leung +852 2319 3851 kinson.leung@hkirc.hk

Appendix A – HKIRC Proposal Requirements

A1. Proposal requirements

Submission deadline	Please refer to Schedule section, 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 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Hard copies	Sending hard copies is **not** mandatory. For sending hard copies, 2 copies of the full Proposal are required. The Proposal shall be sent to the attention of Arktos LAM (Cybersecurity Manager).
Electronic copy	Electronic copy is mandatory. It shall be sent by email to arktos.lam@hkirc.hk and kinson.leung@hkirc.hk
Proposal format	Specified in this document
Font	Electronically published or typed. Times New Roman 12 point font.

A2. 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
    - Migration
    - Hosting
    - SRAA
- 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
- Sample Report generated from services
- Proposed Payment Terms
- Commercial and Payment Terms. e.g. Compensation for delay.

A3 Cover Page

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

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

A4 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

A5 Conflict of Interest Declaration

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

A6 Company Background & Financial Situation

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.

A7 Methodology

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

A8 Project Management Methodology

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

A9 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.

A10 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.

A11 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.

A12 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/deliverables. 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.

A13 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.

A14 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 B – Contract Schedules

Schedule 1 – Price Summary

(a) Cost of SRAA

Suppliers shall quote below the cost for conducting the SRAA.

Description	Price (HK$)
Total price of SRAA (A)	_____

(b) Cost of Hosting Services for 14 Calendar Months (from 1 Dec 2022 to 31 Jan 2024)*

Suppliers shall quote below the Unit Subscription Fee **per month** for hosting services. The total price of hosting services for **14 calendar months** shall be quoted.

Item No.	Description of Services	Net Subscription Fee Per Month (HK$)
1	Hosting services of the production environment	(b1) _____
2	Other services, if any (please specify)	(b2) _____
Total price of hosting services per month (B)		(b1 + b2) _____
Total price of hosting services for 14 calendar months (C)		(b1 + b2) x 14 _____

* The subscription period of the hosting services shall take effect from the tentative start date (1 Dec 2022) and continue in force for a period of 14 calendar months until 31 Jan 2024.

(c) Total Price of the Work Assignment

Suppliers shall quote below the total price of the Work Assignment. The total price of the Work Assignment (D) shall equal the total price of SRAA (A) plus the total price of hosting services for **14 calendar months** (C). Price comparison during proposal evaluation will be based on the total price of the Work Assignment.

Total price of the Work Assignment (D)	(A) + (C) _____

Name and Signature of Authorised Representative (with Company Chop) _____

(Name:)

Name of Organisation/Company _____

Date _____

Appendix C – Requirements of Hosting Environment

i. Hosting platform

Microsoft Azure

ii. Hosting specification

Platform (Production environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in two virtual machines)	2	2 vCPU cores 8 GB RAM 64 GB Storage	Production environment for the Platform
Database Server (utilise Azure Database for MySQL service)	1	4 vCore 320 GB Storage	Storage of Platform database
Object Storage (utilise Azure Blob Storage service)	1	1 TB Storage	Storage of Platform data (for images, documents, etc.)

Platform (UAT environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in one virtual machine)	1	2 vCPU cores 4 GB RAM 64 GB Storage	UAT environment for Platform
Database Server (utilise same Azure Database for MySQL service of Platform but another database)	-	4 vCore 320 GB Storage	Storage of Platform database

Server	Quantity	Specification	Objectives
Object Storage (utilise Azure Blob Storage service)	1	1 TB Storage	Storage of Platform UAT data (for images, documents, etc.)

AI – Automated Tagging (Production environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in two virtual machines)	2	4 vCPU cores 14 GB RAM 64 GB Storage	Production environment for AI – Automated Tagging

AI – Automated Tagging (UAT environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in one virtual machine)	1	2 vCPU cores 4 GB RAM 64 GB Storage	UAT environment for AI – Automated Tagging

AI – Correlation and Summarisation (Production environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in two virtual machines)	2	4 vCPU cores 16 GB RAM 64 GB Storage	Production environment for AI – Correlation and Summarisation

AI – Correlation and Summarisation (UAT environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in one virtual machine)	1	2 vCPU cores 8 GB RAM 64 GB Storage	UAT environment for AI – Correlation and Summarisation

Machine-to-machine service (Production environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in 1 virtual machine)	1	4 vCPU cores 16 GB RAM 64GB Storage	Hosting production environment for the M2M Restful API

Machine-to-machine service (UAT environment):

Server	Quantity	Specification	Objectives
Web Application Server (installed in one virtual machine)	1	2 vCPU cores 8 GB RAM 64GB Storage	Hosting UAT environment for the M2M Restful API

iii. Monitoring component

Component	Description	Coverage
Azure Monitor	- Collect metrics and logs - Show metrics in chart form	Production and UAT environment of both Platform and AI
Log Analytics	- Retrieval of log data via log queries	Production environment of both Platform and AI
Security Center	- Service health monitoring - Threat detection for networks, VMs/servers, Azure services and web application (the Platform) - Alert on security risk and vulnerabilities	Production environment of both Platform and AI
Alert	- Alert on metrics, logs and portal user operation - Alert with email notification	Production environment of both Platform and AI

iv. Other Service

Component	Description
SendGrid	Provide email sending service for the Platform via SendGrid API for the plan Pro or above

v. Email accounts

Five email accounts of O365 services are provided.

vi. Network component

Component	Quantity	Description
Anti-DDoS	1 (for prod)	DDoS mitigation from Cloudflare - Mitigate attack up to 15 Tbps of capacity - Identify and block threats
CDN	1 (for prod)	Support custom caching options to cache web content across globally distributed network (provided by Cloudflare)
Application Gateway – Web Application Firewall (WAF)	2 (1 x prod, 1 x UAT)	Provide centralised protection of the Platform from common exploits and vulnerabilities based on rules from the OWASP core rule set 3.0 (provided by Azure)
Load Balancer	2 (1 x prod, 1 x UAT)	Manage traffic to the Platform & AI (provided by Azure)

Appendix D Probity Clauses

Probity Clauses in Tender/ Quotation Invitation Documents

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.

Anti-collusion

(1) The Tenderer shall not communicate to any person other than the Hong Kong Internet Registration Corporation Limited ("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 D 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 contractor.

Appendix E Warranty

To: Hong Kong Internet Registration Corporation Limited ("HKIRC")

Dear Sir/Madam,

(1) By submitting a tender, _____[the name of your company] (the "Tenderer") represents and warrants that in relation to the tender of Project on Training Packages for SME Cyber Security Staff Awareness:
   (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, HKIRC shall be entitled to, without compensation to any person or liability on the part of the HKIRC:
   (i) reject the tender;
   (ii) if HKIRC has accepted the tender, withdraw its acceptance of the tender; and
   (iii) if HKIRC has entered into the Service Agreement with the Tenderer, terminate the contract.

(3) The Tenderer shall indemnify and keep indemnified HKIRC against all losses, damages, costs or expenses arising out of this Warranty 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 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.

Signature:
Name of the Company: _____
Name of the Signatory: _____
Position of the Signatory: _____
Date: _____

Appendix F Declaration Form on the Compliance with the Ethical Commitment Requirements

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

We, _____ ("the company") shall acknowledge and agree that, if the company is selected as the Contractor, it shall be bounded by the Ethical Commitment clauses:

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 Company: _____
Name of the Signatory: _____
Position of the Signatory: _____
Date: _____