Request for Proposal
On
Project on Training Packages for SME Cyber Security Staff Awareness

Proposal Due by

4 January 2022

(5:00pm Hong Kong Time)

Version 1.1

Date: 13 December 2021

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: info@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.

All responses to the RFP become the property of HKIRC. We shall not be obligated to explain the results of the evaluation process to any Tenderers. Moreover, this RFP is no way to commit HKIRC to award a contract, to pay any costs in preparation of a proposal, or to contract for goods and/or services offered or for oral presentations made by the tenderer(s). We reserve the right to accept or reject any or all proposals received as a result of this request, to negotiate with all qualified tenderer(s), to not award the contract to any service provider, or cancel this RFP.

Table of Contents

1. Summary

HKIRC is looking for a consultancy agency (the "Contractor") to provide consultancy service on the design, development, and production of Training Packages for SME Cyber Security Staff Awareness.

The Contractor must be capable in cybersecurity knowledge and with relevant experience for corporate staff awareness training.

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

Parties interested in providing this service shall submit Express of Interest (EOI) by 16 December 2021. For those who have submitted EOI, they should send proposals to HKIRC no later than 05:00pm (Hong Kong time) on 4 January 2022.

The party submitting the tender for the Services (the "Tenderer") should first submit Express of Interest by email to HKIRC contacts (refer Appendix B – HKIRC Proposal Requirements, electronic copy). The Tenderer must provide their information as required in the proposal cover page (Appendix B, 1.3 Cover Page).

2. Definitions

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

"The Contractor" means the consultancy agency who will provide the Services after award of contract. It is the company to provide Services and work in close collaboration with HKIRC in the project stated in this document.

"HKIRC" means Hong Kong Internet Registration Corporation Limited, the company requesting the proposal for "the Services".

"HKDNR" means Hong Kong Domain Name Registration Company Limited, a wholly-owned subsidiary of HKIRC. This company is also one of the registrars of HKIRC.

"Services" means the comprehensive services with requirements stipulated in Section 4 of this document.

"Tenderer" means the company sending the tender for the Services

"POBO" means the Prevention of Bribery Ordinance in Hong Kong

"RFP" means this Request for Proposal

3. About HKIRC

Hong Kong Internet Registration Corporation Limited (HKIRC) is a not-for-profit and non-statutory corporation designated by the HKSAR Government to administer the registration of Internet domain names under .hk and .香港 country-code top level domains. HKIRC provides registration services through its registrars for domain names ending with .com.hk, .org.hk, .gov.hk, .edu.hk, .net.hk, .idv.hk, 公司.香港, .組織.香港, .政府.香港, .教育.香港, .網絡.香港, .個人.香港, .hk and .香港.

HKIRC endeavors to be:

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

HKIRC's Vision:
.hk and .香港 are the most preferred top-level domains and the brand identity for Hong Kong residents, companies and organizations. In addition, Hong Kong is a leading city in inclusive, secure, innovative, and international Internet and e-Commerce centre.

HKIRC's Mission:
HKIRC is a not-for-profit organization that is committed to providing, and supervising the provision of .hk and .香港 Internet domain names registration, resolution and related services in an uninterrupted, effective, customer-centric and sustainable manner. In addition, HKIRC promotes Hong Kong as an inclusive, secure, innovative, and international city for the Internet and encourages the use of Internet and the related technologies.

3.1 HKIRC and HKDNR are public bodies under POBO

HKIRC and HKDNR are under POBO as public bodies. All the prescribed officers and employees, other than the ordinary members of HKIRC who are not vested with management responsibility, are public servants. In order to ensure that our contractors and service providers also observe a high integrity standard, please read and comply with Probity Clauses in Appendix C in this document and sign the warranty in Appendix D. **HKIRC will not consider proposals from companies which have not signed and sent to us on time the Warranty in Appendix D**

More information about HKIRC can be found on www.hkirc.hk.

4. The Required Services

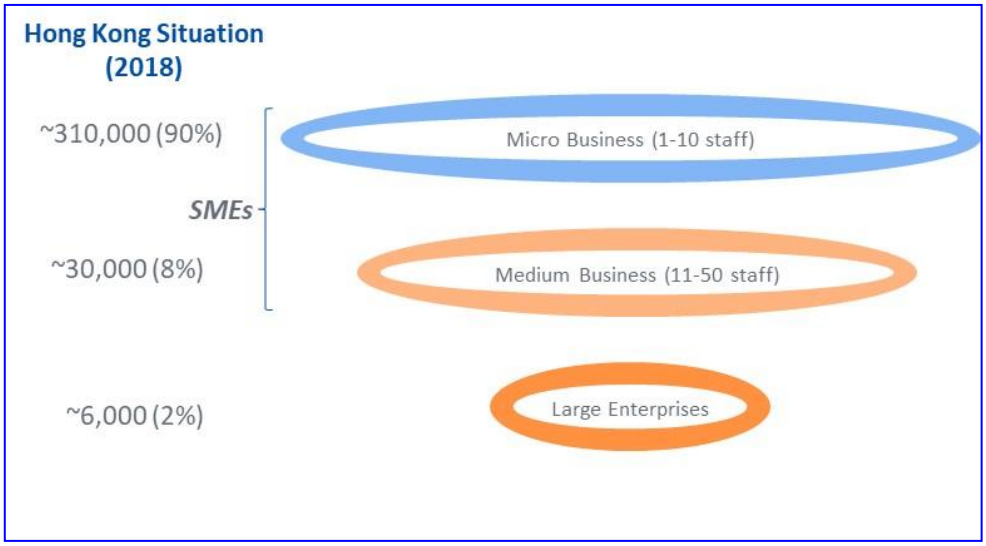
The following defines the scope of service to be provided by the Contractor. The scope is as follows:-

Project Title: Project on Training Packages for SME Cyber Security Staff Awareness

4.1. Project Background

According to First Quarter Economic Report 2018 of Hong Kong Economy, HKSAR, around 98% of Hong Kong companies are small and medium-sized enterprises (SMEs) which generally refer to enterprises engaging less than 50 persons. Among the SMEs, the number of the "micro business" with less than 10 staff, representing 90% of all companies. These micro businesses are expected to be with less IT or technical resources.

Hong Kong Business Situation by Number of Staff



Source: First Quarter Economic Report 2018 of Hong Kong Economy, HKSAR

In this digital era, cybersecurity staff awareness is important to all companies, however, it is found that the current resources on cybersecurity materials are

- Mostly focus on individual Cyber Security Topics
- Too many information that staff do not know where to start with
- Generalized to all situation, staff may not be able to relate the application to their real-life working environment
- "Top-Down" approach - materials target IT manager or technical staff, and rely on them to digest and deliver the message back to their staff
- For a micro business without IT resources, they are difficult to adopt the materials as internal training

With this background, to further enable SMEs, in particular those with less resources, to equip their employees with essential cyber security hygiene practices and enhance their cyber security awareness, this project titled "Project on Training Packages for SME Cyber Security Staff Awareness" aims to assist the digest of individual cybersecurity materials and develop handy, easy-to-read, step-by-step training packages for the employees of SMEs.

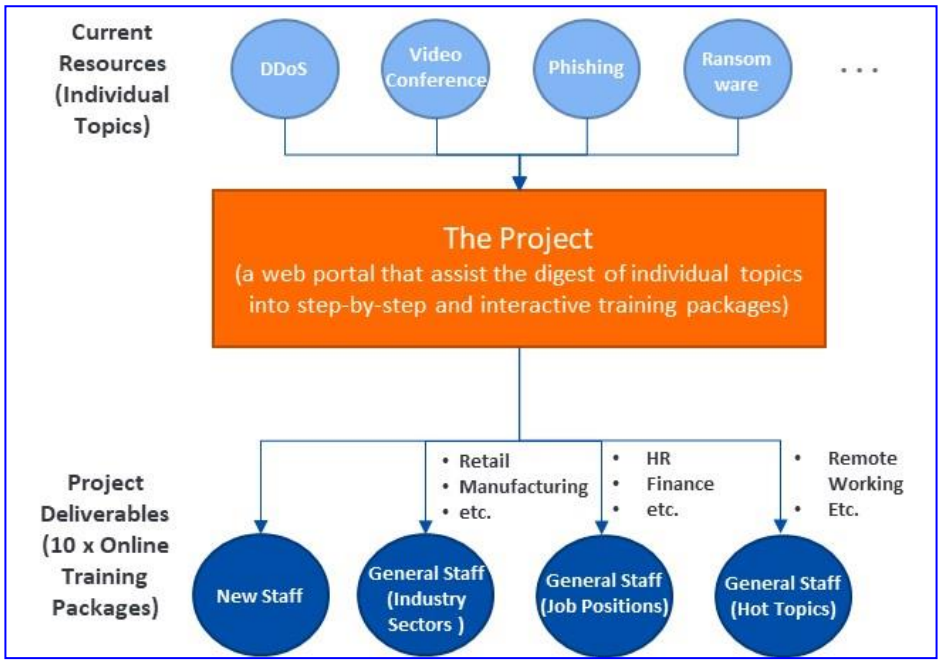
This will enable SMEs to educate their even non-technical personnel about cyber security knowhow using such handy materials and in turn enhance the cyber security level of SMEs themselves.

The training packages will not only cover common security topics for all general employees, but also cover specific topics for employees taking different roles and job natures, including the below areas:

i. Online Training Package for New Staff
ii. Online Training Package for General Staff (Industry Sectors) (e.g. Retail/ Manufacturing/ School/ etc.)
iii. Online Training Package for General Staff (Job Positions) (e.g. HR/ Finance/ Marketing/etc.)
iv. Online Training Package for General Staff (Hot Topics) (e.g. Remote working)

The training packages will be uploaded to HKIRC website and open to public for free to view without login or membership registration.

Illustration of the Project



4.2. Project Objective

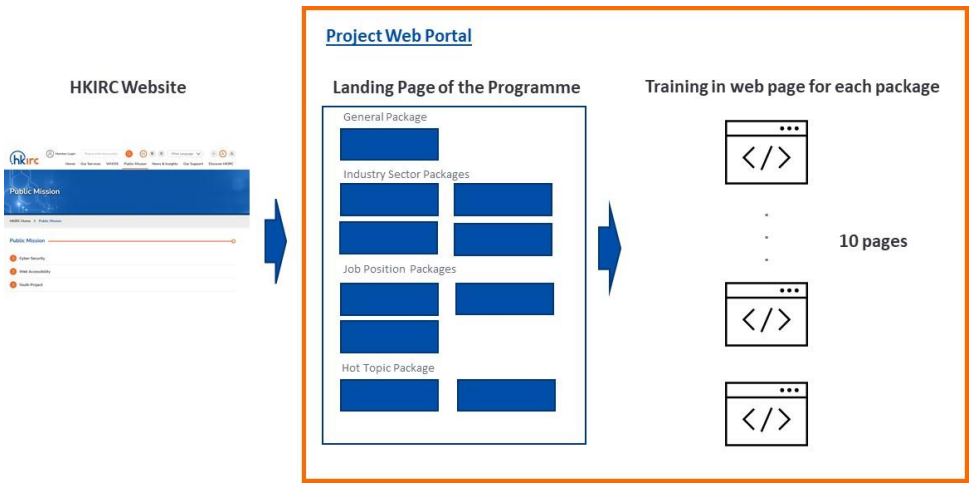
- Assist SMEs with less IT resources to provide cybersecurity staff awareness training to their staff via the training packages developed in the project, especially during new staff on-board
- Facilitate staff to relate the cybersecurity knowledge in corresponding sectors or job positions via the industry sector-specific or job position-specific training packages developed in the project
- Foster cyber security level of Hong Kong by enhancing the awareness on cybersecurity among SMEs

4.3. Project Scope

Develop a web portal with 10 training packages, including

- Online Training Package for New Staff
- Online Training Package for General Staff (Industry Sectors)
- Online Training Package for General Staff (Job Positions)
- Online Training Package for General Staff (Hot Topics)

Illustration of the Project Web Portal with 10 Training Packages



There will be 3 project stages:

A. Preparation Stage

1. Research for the project, which shall

i. Identify and recommend industry sectors to cover in the project with justification
ii. Identify and recommend job positions to cover in the project with justification
iii. Identify and recommend hot topics to cover in the project with justification
iv. Identify and recommend cybersecurity elements in each training packages with justification
v. Identify the key stakeholders of proposed sectors and general SMEs in the project
vi. Expected to be in Microsoft Word format (.DOCX) and Microsoft PowerPoint format (.PPTX), no less than 15 pages in English

B. Implementation Stage

1. Design of the web portal of training packages
    i. 1 x Landing Page
        - In webpage HTML format
        - Hosted in the hosting environment to be specified by HKIRC
        - Responsive web design and mobile friendly
        - Support multi-media
        - Static and dynamic content support
        - Support multi-language, including English and Traditional Chinese
        - W3C Web Content Accessibility Guidelines (WCAG) 2.0 Level AA standards
        - Fully compatible with the prevailing versions of popular web browsers such as Microsoft Edge, Google Chrome, Mozilla Firefox, Safari, etc.
    ii. 10 x Webpages for training packages
        - 1 webpage for each package
        - Hosted in the hosting environment to be specified by HKIRC
        - Each package shall contain
            - Animation-based video with no less than 3 minutes, include
                - Professional voice over in Cantonese
                - Sub-title in English and Traditional Chinese
                - Transcripts in English and Traditional Chinese
            - Graphical and text-based introduction and tips
            - Case scenario-based multiple-choice question and answer
            - and/or other interactive elements
        - Each package is estimated to be finished in 15-20 minutes
        - Each package shall cover at least 4 cybersecurity topics
        - The packages will be in both English and Traditional Chinese
2. Prepare the storyboards of the training packages
3. Design and production of 1 trail training package for one of the sectors identified in 4.3A(i)
4. UAT of the trail training package in B3
5. Pilot Run of the trail training packages in B3 with key industry stakeholder of corresponding sector
6. Design and production of the web portal and all online training packages, including
    - Online Training Package for New Staff
    - Online Training Package for General Staff (Industry Sectors)
    - Online Training Package for General Staff (Job Positions)
    - Online Training Package for General Staff (Hot Topics)

7. UAT of web portal and all online training packages
8. Confirmation and launch of Web Portal with the Training Packages

C. Post-implementation Stage

1. Maintenance of the Web Portal and Training Packages, including but not limited to
    i. Bug fix
    ii. Minor interface adjustment or textual update
2. Final Report
    i. Summarize the project, including but not limited to introduction, methodology, implementation and findings of the Project
    ii. Suggestions on way forward of the Project
    iii. Expected to be in Microsoft Word format (.DOCX) and Microsoft PowerPoint format (.PPTX), no less than 15 pages in English

4.4. Key Deliverables

1. Research Report in DOCX format and PPTX format
2. 10 Sets of Online Training Packages in HTML format
3. Web Portal in HTML format
4. Final Report in DOCX format and PPTX format

4.5. Project Schedule

- A kick-off meeting will be arranged after confirmation of service.

Stage	Tasks	Key Deliverables	Tentative Schedule
A. Preparation Stage	1. Research for the project	Research Report	2 weeks after confirmation of service
B. Implementation Stage	1. Design of the web portal of training packages		3 weeks after confirmation of service
	2. Prepare the storyboards of training packages		3 weeks after confirmation of service
	3. Design and production of trail training packages for one of the sectors identified in 4.3A(i)		4 weeks after confirmation of service
	4. UAT of trail training packages in B3		5 weeks after confirmation of service
	5. Pilot Run of the trail training packages in B3 with key industry stakeholder of corresponding sector		8 weeks after confirmation of service
	6. Design and production of the web portal and all online training packages		15 weeks after confirmation of service
	7. UAT of all Training Packages		18 weeks after confirmation of service
	8. Confirmation and launch of Training Packages	• Web Portal • 10 sets of online training packages	20 weeks after confirmation of service
C. Post-implementation Stage	1. Maintenance of the Training Packages		21-36 weeks after confirmation of service
	2. Final Report	Final Report	21-36 weeks after confirmation of service

5. Fee Arrangements

The tenderer should provide fixed fee quote on project basis but with breakdown by item:

Deliverables	**Total Cost ($HKD)**
1. Research Report	
2. 10 Sets of Online Training Packages in HTML format	
3. Web Portal in HTML format	
4. Final Report	
Total	

To ensure mutual understanding, the method of billing, rates for additional works, third-party costs, and out-of-pocket expenses, as well as payment terms with any interest charges for late payment should be fully detailed in the proposal.

6. Service Period

The tenderer will provide Services after signing service contract till the end of the project, but it is expected that the programme will be completed not more than 10 months. Reasonable explanation is to be given if the project delay is caused by the tenderer. Tentative service timeline is stated in Session 4.5.

7. Elements of a Strong Proposal

All submitted proposal must follow the format as stated in Appendix B – Proposal Requirement.

HKIRC will evaluate all proposals with following criteria.

Evaluation Criteria	Weighting
Ability to Meet the Scope of Work • Understanding our requirements with the proposed work plan • Demonstrating the understanding on the trend of cybersecurity and needs of SMEs • Demonstrating the ability to deliver cybersecurity knowledge to SMEs	30%
Qualifications, Experience and Knowledge • Qualifications and expertise of staff involved in this project • Direct experience in delivering corporate cybersecurity trainings • Work samples showing the quality in performing staff cybersecurity training materials design and implementation • Put forward proposal with professional opinions	30%
Proposed Costs and Payment Schedule • Reasonable breakdown costs and payment schedule	40%

8. Schedule

A tender briefing will be held on 17 December 2021 5:00pm, interested parties please email the attendance list to Arktos LAM (arktos.lam@hkirc.hk) and Kinson LEUNG (kinson.leung@hkirc.hk) during the Expression of Interest.

	Tasks	**To be completed by**
1	Publish of RFP	13 December 2021
2	Expression of Interest	16 December 2021
3	Tender Briefing	17 December 2021, 5:00pm (HKT)
4	Sign Non-Disclosure Agreement (NDA), the Warranty in Appendix D and the Declaration Form on the compliance with the ethical commitment requirements in Appendix E by all interested Tenderers	24 December 2021
5	Deadline for Tenderers to submit proposal and quotation	4 January 2022, 5:00 pm (HKT)
6	Conclude final decision and appoint the Contractor	Mid-January 2022
7	Sign service contract with the appointed Contractor	Mid-January 2022
8	Commencement of Service	Late January 2022

The above schedule may change. In case of the change, HKIRC will notify the Tenderers of the change accordingly.

We may require any tenderers providing more information after submitting proposals or may invite them for face-to-face presentations during the evaluation process, and/or before the contract signed off by HKIRC.

In any case, HKIRC reserves the right to award a contract without going through the presentation and discussion process with the tenderer(s).

9. Service Agreement Negotiation and Signature

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

The service agreement must be signed by both parties within 14 days from the project award date. If the agreement is not signed within the said period, HKIRC will start the negotiation with the next qualified Tenderer on the selection list.

10. Service Completion

The Service Agreement shall be terminated forthwith by either party by giving 1-month prior written notice to the other or if either party is in breach of its obligations and fails to take any reasonable steps to remedy such breach within ten (10) days of receiving a written notice.

Creative concepts, work plan, tactics and all related materials developed during implementation of the Contract shall be property or intellectual property of HKIRC. Upon completion or termination of the Contract, the contractor shall transfer, assign, and otherwise make available to all property and materials belonging to HKIRC and paid for by HKIRC, in the best and most practical format, as agreed upon in advance by both the Contractor and HKIRC.

11. HKIRC Contacts

Hong Kong Internet Registration Corporation Limited

Unit 501, Level 5, Core C, Cyberport 3,
100 Cyberport Road, Hong Kong

Tel: + 852 2319 2303
Fax: + 852 2319 2626
If you are not sure about the appropriate person to call, the receptionist can help you

Cyber Security Manager
Arktos LAM
+852 2319 3863
arktos.lam@hkirc.hk

Assistant Project Manager
Kinson LEUNG
+852 2319 3851
kinson.leung@hkirc.hk

12. 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 Tenderer shall be provided with a set of NDA after HKIRC received the company's Express-of-Interest before the stipulated time. The NDA shall be signed and returned to us before the scheduled deadline. **HKIRC will not consider proposals from companies which have not signed the NDA.**

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

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

13. Ethical Commitment

13.1 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.

13.2 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).

13.3 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.

13.4 Declaration of ethical commitment

(G) 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 the ethical commitment clauses. The company shall submit a signed declaration in a form (see Appendix E) 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 company fails to submit the declaration as required, the Organisation shall be entitled to withhold payment until such declaration is submitted and the company 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 company 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.

Appendix A
HKIRC Information Security Policy and Guideline (An extract relevant to Outsourcing)

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

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

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

(A) Extract from the HKIRC Information Security Policy

8.1 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 organisation'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 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 organisation'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 organisational 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 in

accordance with established policies and procedures of the organisation.

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

8.3 Termination or change of employment

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

8.3.2 All employees, contractors and third party users shall return all of the organisation'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 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 organisation.

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 to be taken.

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 HKIRC Information Security Guidelines

6. ORGANISING INFORMATION SECURITY

6.2 EXTENRNAL PARTIES

6.2.1 Identification of Risks Related to External Parties

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

6.2.3 Addressing Security in Third Party Agreements

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

7. Asset Management

7.1.3 Acceptance 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 resources 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 organisation's information security policy.

8.1.2 Screening

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 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 organisation's responsibilities for information security.

8.2.1 Management Responsibilities

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

12. Information systems acquisition, development and maintenance

12.5.5 Outsourced Software Development

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

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 to be taken.

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.

Appendix B

HKIRC Proposal Requirements

1.1 Proposal Attributes

Successful Tenderer is the one who submitted a clear proposal. The proposal should include but not limited to the following attributes:

- Executive Summary (1-2 page)
- Company Background, for example:
  - Financial situation
  - Company and team credentials
  - Track records
  - Organization and management team
  - Others like Conflict of Interest Declaration
- Methodology and Workplan
- Understanding of Our Requirements
- Knowledge and Advice on Ad hoc issues
- Deliverables and Measurable Result
- Proposed Costs of Service and Payment
- Implementation Timetable
- Other optional items

Tenderer should recommend ways to measure the effectiveness of the project & progress executed.

1.2 Proposal Requirements

Submission Deadline:	Please refer to Section 8– Schedule for the proposal submission deadline.
Delivery Address:	Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, HK
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 (Cyber Security Manager)
Electronic copy	Electronic copy is mandatory. It shall be sent by email to arktos.lam@hkirc.hk and cc kinson.leung@hkirc.hk
Proposal Format:	Specified in this document
Page Count:	30 pages or less. Stapled. Do not bind
Font:	Electronically published or typed. Times New Roman 12 point font.

1.3 Cover Page

Prepare a non-confidential Cover Page with following information and Table of Content in the order given.

Cover Page	
Project Title:	Project on Training Packages for SME Cyber Security Staff Awareness
Project Manager:	Name: Title: Phone: Fax: Email: Mailing Address:
Company:	Company Name: Contact Person: Title: Phone: Fax: Email: Website: Mailing Address:

Appendix C
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 D

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 E

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: _____