Request for Information on Project on Training Packages for SME Cyber Security Staff Awareness

Information Due by
26 November 2021
(5:00pm Hong Kong Time)

Version 1.1
Date: 8 November 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 ROI become the property of HKIRC. We shall not be obligated to explain the results of the evaluation process to any Submission. Moreover, this ROI 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 submission(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 submission(s), to not award the contract to any service provider, or cancel this ROI.

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 Information by 26 November 2021 by email to HKIRC contacts (refer Appendix B – HKIRC Information Requirements, electronic copy).

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 information 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 consultancy services with requirements stipulated in Section 4 of this document.

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

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

"ROI" means this Request for Information

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.

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

Being one of the important internet infrastructures in Hong Kong, HKIRC is committed to promote a safe internet environment in Hong Kong and launched various cyber security public mission projects in past few years including “Cybersec Infohub”, “Free In-depth Website Security Scan Services”, “Cyber Youth Programme”, and more.

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 develop handy, easy-to-read, step-by-step training packages for the employees of SMEs.

This project will be part of public mission projects of HKIRC, where the training packages will be uploaded to HKIRC website and available for SMEs to view or download for free without login or membership registration.

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:

1. Online Training Packages for New Staff (general)
2. Online Training Packages for New Staff (sector specifics)
3. Online Training Packages for Different Job Duties
4. Online Training Packages for Other Circumstances

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.

4.2 Project Objective

- Assist SMEs with less IT resources to conduct cybersecurity staff awareness training to their staff
- Facilitate staff to relate the cybersecurity knowledge in corresponding job duties
- Foster cyber security level of Hong Kong by enhancing the awareness on cybersecurity among SMEs

4.3 Project Scope

There will be 3 project stages:

A. Preparation Stage
    1. Research for the project, which shall
        i. Identify and recommend sectors to cover in the project with justification
        ii. Identify and recommend job-duties to cover in the project with justification
        iii. Identify and recommend other circumstances 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
    2. (Optional) Propose engagement plan to deliver the staff training packages to the key stakeholders identified and general SMEs

B. Implementation Stage
    1. Prepare the Training Scripts of each training packages in Word Format
    2. Recommend the presentation of the training packages, which may include but not limited to videos, slides, MC questions, etc.
    3. Design and production of trail training packages for one of the sectors identified in 4.3A(i)
    4. UAT of trail training packages in B3
    5. (Optional) Pilot Run of the trail training packages in B3 with key industry stakeholder of corresponding sector
    6. Design and production of full sets of online training packages, including
        i. Online Training Packages for New Staff (general)
        ii. Online Training Packages for New Staff (sector specifics)
        iii. Online Training Packages for Different Job Duties
        iv. Online Training Packages for Other Circumstances
    7. UAT of all Training Packages
    8. Confirmation and launch of Training Packages

C. Post-implementation Stage
    1. (Optional) Execute the proposed engagement plan to deliver the staff training packages to the key stakeholders identified and general SMEs
    2. Maintenance of the Training Packages
    3. Final Report

4.4 Key Deliverables

1. Research Report
2. Training scripts in Word Format
3. Sets of online training packages in Traditional Chinese and English
4. Final Report
5. (Optional) Pilot Run Report
6. (Optional) Engagement Plan
7. (Optional) Engagement Report

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
	2. (Optional) Propose engagement plan	Engagement Plan	2 weeks after confirmation of service
B. Implementation Stage	1. Prepare the Training Scripts	Training scripts in Word Format	3 weeks after confirmation of service
	2. Recommend the presentation of the 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. (Optional) Pilot Run of the trail training packages in B3 with key industry stakeholder of	(Optional) Pilot Run Report	8 weeks after confirmation of service

Stage	Tasks	Key Deliverables	Tentative Schedule
	corresponding sector		
	6. Design and production of full sets of 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	Sets of online training packages in Traditional Chinese and English	20 weeks after confirmation of service
C. Post-implementation Stage	1. (Optional) Execute the proposed engagement plan	(Optional) Engagement Report	21-36 weeks after confirmation of service
	2. Maintenance of the Training Packages		21-36 weeks after confirmation of service
	3. Final Report	Final Report	21-36 weeks after confirmation of service

4.6 Quotation

In the information document, please provide the quotation with below format:

	Deliverables	Unit Cost	Committed Quantities	Total Cost ($HKD)
Core	1. Research Report			
	2. Training scripts in Word Format			
	3. Sets of online training packages in Traditional Chinese and English			
	• New Staff (general)			
	• New Staff (sector specifics)			
	• Different Job Duties			
	• Other Circumstances			
	4. Final Report			
Sub-Total Cost - Core				
Optional	5. (Optional) Pilot Run Report			
	6. (Optional) Engagement Plan			
	7. (Optional) Engagement Report			
Sub-Total Cost – Optional				
Total				
Additional	1 online training package for additional sector			
	1 online training package for additional job duty			

5. 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

6. Information Security

The company submitting the information ("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.

7. Ethical Commitment

7.1 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.

7.2 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).

7.3 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.

7.4 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 (a) to sign off a non-disclosure agreement (NDA) on all information to be provided and (b) to sign off a Compliance Statement where compliance requirements are specified in more details.

(A) Extract from the 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 Information Requirements

1.1 Information Attributes

The information 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 course & progress executed.

1.2 Information Requirements

Submission Deadline:	Please refer to P.4.
Delivery Address:	Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, HK
Electronic copy	Electronic copy is mandatory. It shall be sent by email to arktos.lam@hkirc.hk and cc kinson.leung@hkirc.hk
Information Format:	Specified in this document
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:	HKIRC 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: