Ethical Phishing Email Campaign 2026

Request for Proposal
(Tender Ref.: RFP-CYBERSEC-2026-01)

Version 2.0
Date: 21 April 2026

Hong Kong Internet Registration Corporation Limited

Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Tel.: +852 2319 1313 Fax: +852 2319 2626
Email: enquiry@hkirc.hk Website: www.hkirc.hk

IMPORTANT NOTICE

This communication contains information which is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any distribution, copying or use of this communication or the information in it is strictly prohibited. If you have received this communication in error, please notify the sender immediately and then destroy any copies of it.

Table of Contents

Contents

IMPORTANT NOTICE 2
Summary 5
1. Definitions 6
2. About HKIRC 7
3. Background of the Project 8
4. The Required Services and System Functionalities 9
5. Limitation of Liability and Indemnity 15
5.1. Service Level Agreement (SLA), Service Credits and Contract Termination 15
5.2. Project Management Methodology and Review Meeting 16
5.3. Intellectual Property Rights 16
5.4. Software Source Code Escrow 16
6. Information Security 16
7. Project Acceptance 17
8. Anti-collusion 17
9. Offering Advantages 18
10. Compliance with law 18
11. Ethical Commitment 19
11.1. Prevention of bribery 19
11.2. Declaration of Interest 20
11.3. Handling of confidential information 20
11.4. Declaration of ethical commitment 21
12. Time Schedule 22
13. Payment Schedule 23
14. Elements of a Strong Tender 24
15. Service Agreement Negotiation and Signature 25
16. HKIRC Contacts 26
Appendix A – Warranty 27
Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements 30
Appendix C – HKIRC Proposal Requirements 32
Appendix D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing 38
Appendix E – SECURITY RISK ASSESSMENT AND AUDIT 40
Appendix G - PROFESSIONAL STAFF REQUIREMENT 47
Appendix H – TYPES OF PHISHING AND TOPICS OF PHISHING 48

Summary

Hong Kong Internet Registration Corporation Limited (HKIRC) is going to commission a Service Provider ("the Contractor") to provide a Phishing Email Awareness Solution for the upcoming Ethical Phishing Email Campaign 2026.

The scope of services and requirements are detailed in Section 4 of this document.

Parties interested in providing this service should **sign Non-disclosure Agreement (NDA)** and **submit proposal** (see Appendix C) to the Group **no later than 5:00pm on 8 May 2026 (Hong Kong time)**.

The Contractor should submit Proposal by email to HKIRC contacts (refer to Appendix C - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix C, 2 Cover Page).

1. Definitions

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

“The Contractor” ,“The Service Provider” and “Vendor” mean the company who will provide the Services after award of contract.

“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.

“The Services” and “The Project” means the comprehensive services with requirements stipulated in Section 4 of this document.

“RFP” means this Request for Proposal.

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

“The System” means the Vendor-owned and Vendor-managed environment on which the campaign software code and associated services are hosted, operated, and maintained.

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 endeavors 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. Background of the Project

Hong Kong Internet Registration Corporation Limited (HKIRC) is going to organise the "Ethical Phishing Email Campaign 2026", target to 160,000 staff across 80+ entities. The exercise aims to enhance staff awareness across participating organisations in identifying suspicious emails and to strengthen their overall cybersecurity resilience.

The exercise is expected to complete by December 2026. During this period, participating entities will receive simulated phishing emails at the provided email addresses to test their staffs' cybersecurity awareness. Upon completion, each entities will receive a detailed report summarizing their staffs' performance in handling suspicious emails.

HKIRC invites interested parties to provide the Phishing Email Awareness Solution with the detailed requirements below.

The campaign will be categorised into five major tasks

- Task 1 – Preparation
- Task 2 – Deployment, Hosting Environment, SRAA and PIA
- Task 3 – Email Dissemination for 2 rounds of phishing drill exercises
- Task 4 – Data Collection, Analysis, and Reporting for each phishing drill exercises
- Task 5 – Hybrid Seminars after each phishing drill exercises

4. The Required Services and System Functionalities

Task 1 – Preparation

- **Ethical Email, Website and Domain Preparation**
  - To establish a phishing simulation system (the System) for sending simulated phishing emails, tracking response and reporting.
  - To design **at least** 25 twenty-five customized pseudo phishing email templates tailored to seasonal topics relevant to the daily lives of staff across various entities, according to requirements of HKIRC (content language will be mainly in English and traditional Chinese and ensuring appropriateness and relevance for the audience.);
    - Upon HKIRC's request, your company shall customize the design or content of each pseudo phishing email to meet requirements of HKIRC in Task 1;
    - Any graphics or wordings used in those emails shall not infringe the copyright, patents or trademark of any organisation by possible means (such as altering original design or adding disclaimer);
  - To design **at least 25 twenty-five** landing pages according to requirements of HKIRC;
  - To provide, at its own cost, **at least 25 twenty-five Internet domains used for the pseudo-phishing websites** during the campaign period;
    - To arrange the auto-redirection to a page approved and agreed by HKIRC
  - To provide, at the contractor's own cost, **at least 25 Internet mailboxes using at least 25 different Internet domains with valid Mail Exchange (MX) record and related SSL / TLS certificates** for the campaign period. The System shall use such Internet mailboxes as "sender" addresses. Such Internet mailboxes shall be able to receive bounce back emails, if any. All the bounce back emails shall be forwarded to a provided mailbox. The emails stored in the senders' mailboxes shall be removed and shall not be kept;

- **User on-boarding and configuration**
  - To import target recipient lists around but not limit to 80 entities approximately (equivalent to 160,000 +5% email accounts);
    - Should any participating entity(s) be the subscriber or customer of your company and your associate partner(s), their eligibility of participating in the campaign shall not be affected.
  - To provide a configuration requirement and relevant guideline for the participating entities to apply (e.g. setup of technical connections for phishing email server in department environment, IP whitelist, Domain whitelist, etc)
  - To provide direct technical support and troubleshooting assistance to participating entities experiencing configuration issues (e.g. putting domains on their whitelist and conducting other necessary technical setup), via a dedicated telephone line (available during office hours from 9:00 AM to 6:00 PM) and a designated support email address
  - To provide 24x7 technical support contact for prompt troubleshooting during the dissemination of phishing emails (e.g. to support immediate suspension of email dissemination jobs of the System that cause abnormal loading and impact to the entities).

- **User Acceptance Testing**
  - To send emails to participating entities (one or two contact person(s) or representative(s) only) for testing to ensure the reception of the prepared pseudo phishing emails;
  - Conduct initial distribution of test emails to HKIRC for verification, ensuring the accuracy and correctness of all twenty-five email templates prior to wider dissemination

- **Report Design**
  - To design a comprehensive analytical report template for the entire campaign outlining key findings and insights, and aligning with the standards and requirements specified by HKIRC.
  - To design an analytical report template for individual participating entities, fulfilling the qualities and requirements set out by HKIRC; and

- **Project Management**
  - To arrange regular report and meeting with HKIRC to update the project status;
  - To establish and maintain a co-host master list documenting the status of each participating entity. Including, but not limited to, whitelist status, testing progress, and current issues. The master list shall provide HKIRC's staff with both viewing and editing rights to facilitate effective oversight and collaboration.

Task 2- Deployment, Hosting Environment, SRAA and PIA

- To deploy the System in a hosting infrastructure owned by the vendor at the vendor's own cost. The hosting infrastructure **must be physically located within Hong Kong.** Such infrastructure shall be dedicated to serve the phishing email campaign and shall not host any out-of-scope systems and data.
- The vendor shall devise a solution and deploy components of the System to alternative hosting infrastructure as instructed by HKIRC, whenever necessary to accommodate the technical and security requirements and constraints in sending the phishing emails to the target recipient entities. The vendor shall provide support and perform necessary setup, configuration and customization at such alternative infrastructure, to ensure connectivity to the entities for sending the phishing emails and tracking response.
- The System and its operation shall strictly adhere to the **Security Requirements** set forth by HKIRC. These include compliance with the Baseline IT Security Policy (S17) and the IT Security Guidelines (G3) of the HKSAR Government, and any other instructions or standards specified by HKIRC. The Contractor must ensure confidentiality of all information, proper encryption and handling of system and user data, timely reporting of any security incidents, and full cooperation with auditors and assessors. Additionally, obligations extend to returning all related materials upon termination, maintaining compliance with the Personal Data (Privacy) Ordinance, preventing unauthorized disclosure or use of system materials, and implementing necessary technical safeguards such as security patches, firewall configurations, and X.509 digital certificates for encrypted transmission;
- Before the operation of the System, the vendor shall appoint an external independent third party as the Security Auditor, which has not been involved in the development life cycle of the System and the operation of the campaign, to conduct a Security Risk Assessment and Audit (SRAA) for the System, as well as follow up and resolve the findings identified by the Security Auditor. The SRAA shall cover the following:

- evaluate the security risk of the System and relevant services related to the use of information technology;
- identify and recommend measures with the aim of strengthening the level of security protection of the System and relevant services to an acceptable level; and
- review the compliance and effective implementation of security measures of the System and relevant services to ensure that all identified risks have been mitigated and solved;

(**Please Refer to Appendix E for the full requirements of SRAA**)

- Before the operation of the System, the vendor shall appoint an external independent third party as the Assessor, which has not been involved in the development life cycle of the System and the operation of the campaign, to conduct a Privacy Impact Assessment ("PIA") in relation to the System and the Phishing Email Campaign. The vendor shall follow up and resolve the findings identified and implement the recommendations accordingly. The PIA shall cover the following:
  - Identify the data privacy potential effect, actual effects, implication, issues and risks;
  - Perform data processing cycle analysis;
  - Perform privacy risk analysis
  - Provide recommendations on how the identified potential and actual effects upon personal data privacy can be mitigated;
  - Assess and ensure compliance with the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) and other relevant Ordinances, prevailing guidelines and recommendations from the Office of the Privacy Commissioner for Personal Data;
  - Provide recommendations on how to avoid or mitigate issues and risks;
  - Conduct the Privacy Compliance Audit with the objective of reassessing whether the recommendations of the Privacy Impact Assessment have been adequately addressed; and
  - Report and document the findings, recommendations, and privacy protective measures in addressing the privacy risks.

(**Please Refer to Appendix F for the full requirements of PIA**)

Task 3 – Email Dissemination for 2 rounds of phishing drill exercises

- To deliver approximate 2,500,000 emails during 2 rounds of phishing drill exercises. Each round shall be completed within 4 weeks' time.
- The System shall support pre-scheduling of email dissemination tasks and support email sending tasks in multiple sessions concurrently. The throughput of email dissemination shall be at least 5,000 emails per hour. The system shall be scalable to increase the throughput upon addition of extra hardware resources.
- Setup a random distribution mechanism
  - To ensure proper randomisation of template distribution and maintain variation among participants
  - A set of templates will be randomly selected from the 25 designated options for distribution to users in each round
  - Each participant will therefore receive a distinct set of ethical phishing emails within the two rounds of email dissemination, ensuring differentiation among users
  - Each participant shall not receive repeated template during the 2 rounds of phishing drill exercise

- The email disseminating pattern, frequency or/and period shall be adjustable and negotiable;
- To continue handling enquiries and providing technical supports to participating entities that encounter difficulties as stated in Task 1.
- Where feasible, provide HKIRC staff with access to the sending platform to monitor and review email delivery progress

Task 4 – Data Collection, Analysis, and Reporting for each phishing drill exercises

- **Data Collection and Analysis**
  - To collect and analyze the data generated during the entire campaign. Including, but not limited to:
    - Aggregating and analyzing user interaction data (e.g. email opens, timestamps, link clicks, credential submissions);
    - Segmenting results based on industry classification, organisational scale, and user role;
    - Identifying behavioural trends and risk patterns;
    - Providing actionable insights and visual reports to support awareness training and future campaign optimization; and
    - Identifying and flagging potential false positives by analysing the correlation between email delivery time and user click time, particularly instances where the time interval is unusually short and may indicate automated or non-human interaction

- **Production of Analytical Reports**
  - To provide raw data after each round of phishing drill exercises
  - To provide summary management report after each round of phishing drill exercises, i.e. 2 summary management reports in total
  - To produce individual analytical reports for each participating organisation, incorporating raw data and summarizing their respective performance;
    - Such report should include raw data such as who / when opened the pseudo phishing email(s), who / when clicked the embedded link(s) and / or attachment file(s),who scanned the QR code(s), etc;
  - To respond to enquiries from HKIRC and participating entities.

Task 5 –Seminars after each phishing drill exercises

- **Seminars Design**
  - The Contractor shall design and provide two seminars after each round of phishing drill exercises;
    - Each session is around 2 hours;
    - The seminars shall be conducted in either online or hybrid mode (i.e. at physical venue with online streaming), subject to decision of HKIRC. Hybrid seminars shall be for around 200 – 300 sitting in participants per session with on-line broadcasting around 5000 participants; The contractor is not responsible for the acquisition of the physical venue, but shall be responsible for the setup of equipment at the venue.
  - Topics of the hybrid seminars agenda shall be proposed by the Contractor and for agreement by HKIRC;
  - Topics shall be related to phishing and related cybersecurity threats, and a presentation on the findings and insights of the phishing campaigns.
  - The content of the two (2) hybrid seminars shall be 80-90% the same and the topics shall be related to phishing. The difference in content shall be according to the phishing drills situation. Phishing topics shall include but are not limited to those mentioned **Appendix F**:

- **Preparation**
  - The Contractor shall provide and arrange the equipment and other relevant materials logistic, if needed, in the hybrid seminars and webinars. Such as on-site equipment and setting (site-visit maybe required), on-line broadcasting equipment/software and etc.;
  - The Contractor shall provide on-line participants' attendant list for HKIRC's record; and
  - HKIRC would arrange the on-line registration, training venue and attendant list for reception sign-off.
  - The Contractor shall prepare education materials and presentation slides in English

- **Delivery**
  - The Contractor shall provide and arrange manpower in the hybrid seminars, such as trainers, the emcee, supporting staff and etc.;
  - The Contractor shall provide the emcees and trainers at Contractor's own cost (i.e. no extra cost to the HKIRC)
  - Trainers shall conduct the training in Cantonese.

- **Post Seminars**
  - Hybrid seminars shall be recorded, and the Contractor shall remove the videos from any format of storage after HKIRC acknowledges receiving the copies; and
  - The Contractor shall provide video capture and editing for the key points of the two (2) hybrid seminars.

Summary of the Campaign

Preparation (Task 1)

Deployment, Hosting Environment, SRAA and PIA(Task 2)

Phishing Dill Exercise 1

- Email Dissemination 1 (Task 3)
- Summary management Report 1 (Task 4)
- Seminar 1 (Task 5)

Phishing Drill Exercise 2

- Email Dissemination 2 (Task 3)
- Summary management Report 2 (Task 4)
- Seminar 2 (Task 5)

Overall Report (Task 4)

Reports for Individual Entities (Task 4)

5. Limitation of Liability and Indemnity

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

5.1. Service Level Agreement (SLA) Service Credits and Contract Termination

All services provided by the Service Provider shall be sized and scaled to meet the agreed SLA, including but not limited to implementing the Project according to the agreed project schedule without significant deviation; delivering project deliverables up to industrial standards and quality levels; protecting data integrity and confidentially; and maintaining system availability at the agreed level. All planned activities which would affect the Production environment and daily operations shall be notified to and agreed with HKIRC four weeks in advance.

In case of the Service Provider's service level does not meet with the proposed SLA, the Service Provider shall, as part of the SLA, include a Service Credit scheme or any applicable remedial actions (at the Service Provider's own cost) for compensation for the service which did not meet the SLA. Service Provider may propose detail scheme during the contractual negotiation stage, but will need to outline the proposed scheme within the tender for HKIRC to evaluate.

HKIRC also reserves the right to terminate the contract based on a "3-strike" principle; the Service Provider shall not break the SLA for more than three times during the project period. HKIRC also reserves the right to terminate the service if the service provided:

- Causes disruption and/or losses to HKIRC business and operation.
- Causes service downtime without notices.

5.2. Project Management Methodology and Review Meeting

Please propose the project management methodology the Service Provider would adopt for governing the implementation of the Project. Review meetings, on monthly basis, should be arranged for the purposes including but not limited to:

- Monitor and review the overall project progress, quality of project deliverables.
- Discuss and propose action plans for any project-level issues.
- Manage any project-related risks and incidents.

5.3. Intellectual Property Rights

The Service Provider's proposed solution, and its components, shall not infringe the intellectual property rights of any third party. The Service Provider shall bear the liability or consequence for any intellectual property rights infringement made by the Service Provider and/or in its solution for the Project.

5.4. Software Source Code Escrow

It is required to use open source frameworks for the development of the System and release the source code to HKIRC/ HKDNR without additional cost incurred. If this arrangement cannot be made, the Service Provider is required to make software source code escrow arrangement to allow HKIRC/ HKDNR to retrieve and use the software source code of the System for any circumstances in which the Service Provider no longer supports and maintains its solution.

6. 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 D). The company shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

The company shall be provided with a set of NDA after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA shall be signed and returned to HKIRC before the scheduled deadline. HKIRC will only consider proposals from companies which have 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 the HKIRC's staff and Board of Directors of HKIRC.

7. Project Acceptance

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

1. Acceptance of Task 1
2. Acceptance of Task 2
3. Acceptance of Task 3
4. Acceptance of Task 4
5. Acceptance of Task 5

8. Anti-collusion

(1) The Tenderer shall not communicate to any person other than HKIRC the amount of any tender, adjust the amount of any tender by arrangement with any other person, make any arrangement with any other person about whether or not he or that other person should or should not tender or otherwise collude with any other person in any manner whatsoever in the tendering process. Any breach of or non-compliance with this sub-clause by the Tenderer shall, without affecting the Tenderer's liability for such breach rules and laws or non-compliance, invalidate his tender.

(2) Sub-clause (1) of this Clause shall have no application to the Tenderer's communications in strict confidence with his own insurers or brokers to obtain an insurance quotation for computation of tender price and communications in strict confidence with his consultants/sub-contractors to solicit their assistance in preparation of tender submission.

(3) The Tenderer shall submit to the HKIRC a duly signed warranty in the form set out in Appendix 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

9. 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.

10. Compliance with law

Notwithstanding anything to the contrary under the Agreement of this Project, HKIRC reserves the right to disqualify the Service Provider on the grounds that the Service Provider has engaged, is engaging, or is reasonably believed to have engaged or be engaging in acts or activities that are likely to cause or constitute the occurrence of offences endangering national security or otherwise the exclusion is necessary in the interest of national security, or is necessary to protect the public interest of Hong Kong, public morals, public order or public safety.

HKIRC may immediately terminate the Agreement of this Project upon the occurrence of any of the following events:

(a) the Service Provider has engaged or is engaging in acts or activities that are likely to constitute or cause the occurrence of offences endangering national security or which would otherwise be contrary to the interest of national security; or

(b) the continued engagement of the Service Provider or the continued performance of the Services is contrary to the interest of national security; or

(c) HKIRC reasonably believes that any of the events mentioned above is about to occur.

11. Ethical Commitment

11.1. Prevention of bribery

(A) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, except with permission of Hong Kong Internet Registration Corporation Limited (hereafter referred to as the Organisation) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organisation. The Contractor shall also caution his directors, employees, agents and sub-contractors against soliciting or accepting any excessive hospitality, entertainment or inducements which would impair their impartiality in relation to the business of the Organisation. The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors are aware of the aforesaid prohibition and will not, except with permission of the Organisation, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organisation.

(B) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, offer any advantage to any Board member or staff in relation to the business of the Organisation.

11.2. Declaration of Interest

(C) The Contractor shall require his directors and employees to declare in writing to the Organisation any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract. In the event that such conflict or potential conflict is disclosed in a declaration, the Contractor shall forthwith take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(D) The Contractor shall prohibit his directors and employees who are involved in this Contract from engaging in any work or employment other than in the performance of this Contract, with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(E) The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors who are involved in this Contract are aware of the provisions under the aforesaid sub-clauses (C) and (D).

11.3. Handling of confidential information

(F) The Contractor shall not use or divulge, except for the purpose of this Contract, any information provided by the Organisation in the Contract or in any subsequent correspondence or documentation, or any information obtained when conducting business under this Contract. Any disclosure to any person or agent or sub-contractor for the purpose

of the Contract shall be in strict confidence and shall be on a "need to know" basis and extend only so far as may be necessary for the purpose of this Contract. The Contractor shall take all necessary measures (by way of internal guidelines or contractual provisions where appropriate) to ensure that information is not divulged for purposes other than that of this Contract by such person, agent or sub-contractor. The Contractor shall indemnify and keep indemnified the Organisation against all loss, liabilities, damages, costs, legal costs, professional and other expenses of any nature whatsoever the Organisation may suffer, sustain or incur, whether direct or consequential, arising out of or in connection with any breach of the aforesaid non-disclosure provision by the Contractor or his directors, employees, agents or sub-contractors.

11.4. Declaration of ethical commitment

(G) The Contractor shall submit a signed declaration in a form (see Appendix B) prescribed or approved by the Organisation to confirm compliance with the provisions in aforesaid sub-clauses (A) (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and confidentiality. If the Contractor fails to submit the declaration as required, the Organisation shall be entitled to withhold payment until such declaration is submitted and the Contractor shall not be entitled to interest in that period. To demonstrate compliance with the aforesaid sub-clauses (A), (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and handling of confidential information, the Contractor and the sub-contractors employed for the performance of duties under this Contract are required to deposit with the Organisation a copy of the internal guidelines issued to their staff.

12. Time Schedule

High-level Schedule

#	Items	To be Completed by
1	Publish RFP	21-Apr-2026
2	Sign Non-disclosure Agreement (NDA)	08-May-2026
3	Deadline for vendors to submit proposal	08-May-2026, 5:00pm
4	Sign service agreement contract with the appointed vendor	May 2026
5	Kick-start of the project	May/Jun 2026
6	Project completion	Dec 2026

Project Schedule

#	Items	Tentative Schedule
1	Kick-start of the project	May/Jun 2026
2	Preparation (Task 1)	May-Jul 2026
3	Deployment, Hosting Environment, SRAA and PIA (Task 2)	May-Jul 2026
	Phishing Dill Exercise 1	
4	Email Dissemination 1 (Task 3)	By Aug 2026
5	Summary management Report 1 (Task 4)	By Sep 2026
6	Seminar 1 (Task 5)	By Sep 2026
	Phishing Drill Exercise 2	
7	Email Dissemination 2 (Task 3)	By Oct 2026
8	Summary management Report 2 (Task 4)	By Nov 2026
9	Seminar 2 (Task 5)	By Nov 2026
10	Overall Report (Task 4)	By Dec 2026
11	Reports for Individual Entities (Task 4)	By Dec 2026
12	Project completion	Dec 2026

13. Payment Schedule

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

Milestone	Items	Payment
1	Kick-start of the project	10%
2	Acceptance of Task 1	20%
3	Acceptance of Task 2	20%
4	Acceptance of Task 3	20%
5	Acceptance of Task 4	20%
6	Acceptance of Task 5	10%

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

Deliverables	Total Cost ($HKD)
1. Task 1 – Preparation	
2. Task 2 – Deployment, Hosting Environment	
3. Task 2 – SRAA	
4. Task 2 – PIA	
5. Task 3 – Email Dissemination for 2 phishing drill exercises	
6. Task 4 – Data Collection, Analysis, and Reporting for each phishing drill exercises	
7. Task 5 – Hybrid Seminars after each phishing drill exercises	
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.

14. Elements of a Strong Tender

All submitted tender must follow the format as stated in Appendix C - HKIRC Proposal Requirements

Evaluation Criteria	Weighting
Ability to Meet the Scope of Work • Understanding our requirements with the proposed work plan (e.g. random distribution mechanism, 2 phishing exercises, summary management report and seminar after each exercise) • Demonstrating the understanding of the trend of phishing attacks • Demonstrating the robust work plan to design and implement quality phishing email templates • Demonstrating the robust work plan to deliver 2,500,000+ emails on schedule • Demonstrating the ability to provide secure deployment and hosting environment • Demonstrating the ability to provide quality seminars • Demonstrating the ability to provide quality reports on schedule • Any other innovative approach	40%
Qualifications, Experience and Knowledge • Company size and length of business in Hong Kong • Qualifications and expertise of staff involved in this project • Direct experience in delivering phishing drill exercises for public sector or the Government • Direct experience in delivering phishing drill exercises for massive scale	30%
Proposed Costs and Payment Schedule • Reasonable breakdown costs and payment schedule	30%

The vendor selection criteria consist of 2 parts: Technical (accounting for 70% of the total score), based on submitted proposal and technical evaluation, and Price (accounting for 30% of the total score).

Proposal not passing the technical assessment will not be further considered.

The Price score is calculated based on the following formula:

Lowest price among qualified tenders / Offered price of the tenderer x 30%

15. 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.

16. 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 2319 2303 telephone +852 2319 2626 fax https://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**Head of Public Mission - Cybersecurity** Horace MA +852 2319 3863 horace.ma@hkirc.hk **Project Manager** Kinson LEUNG +852 2319 3851 kinson.leung@hkirc.hk

Appendix A – Warranty

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

DearSir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the Request for Proposal of Ethical Phishing Email Campaign 2026 (Ref.: RFP-CYBERSEC-2026-01):

(i) it has not communicated and will not communicate to any person other than the HKIRC the amount of any tender price;
(ii) it has not fixed and will not fix the amount of any tender price by arrangement with any person;
(iii) it has not made and will not make any arrangement with any person as to whether it or that other person will or will not submit a tender; and
(iv) it has not otherwise colluded and will not otherwise collude with any person in any manner whatsoever in the tendering process.

(2) In the event that the Tenderer is in breach of any of the representations and/or warranties in Clause (1) above, the HKIRC shall be entitled to, without compensation to any person or liability on the part of the HKIRC :

(i) reject the tender;
(ii) if the HKIRC has accepted the tender, withdraw its acceptance of the tender; and
(iii) if the HKIRC has entered into the contract with the Tenderer,
terminate the contract.

(3) The Tenderer shall indemnify and keep indemnified the HKIRC against all losses, damages, costs or expenses arising out of or in relation to any breach of any of the representations and/or warranties in Clause (1) above.

(4) Clause (1) shall have no application to the Tenderer's communications in strict confidence with its own insurers or brokers to obtain an insurance quotation for computation of the tender price, or with its professional advisers, and consultants or
sub-contractors to solicit their assistance in preparation of tender submission. For the avoidance of doubt, the making of a bid by a bidder to the HKIRC in public during an auction will not by itself be regarded as a breach of the representation and warranty in Clause (1)(i) above.

(5) The rights of HKIRC under Clauses (2) to (4) above are in addition to and without prejudice to any other rights or remedies available to it against the Tenderer.

Authorized Signature & Company Chop :

Name of Person Authorized to Sign (in Block Letters) :

Name of Tenderer in English (in Block Letters) :

Date :

Appendix B – Declaration Form by Contractor on their compliance with the ethical commitment requirements

[start in next page]

To: Hong Kong Internet Registration Corporation Limited (HKIRC)
Contract No.: RFP-CYBERSEC-2026-01
Title: Ethical Phishing Email Campaign 2026

In accordance with the Ethical Commitment clauses in the Contract:

1) We confirm that we have complied with the following provisions and have ensured that our directors, employees, agents and sub-contractors are aware of the following provisions:

   a) prohibiting our directors, employees, agents and sub-contractors who are involved in this Contract from offering, soliciting or accepting any advantage as defined in section 2 of the Prevention of Bribery Ordinance (Cap 201) in relation to the business of HKIRC except with the permission of HKIRC;

   b) requiring our directors, employees, agents and sub-contractors who are involved in this Contract to declare in writing to their respective company management any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract, and in the event that a conflict or potential conflict is disclosed, take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed;

   c) prohibiting our directors and employees who are involved in this Contract from engaging in any work or employment (other than in the performance of this Contract), with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract and requiring our agents and sub-contractors to do the same; and

   d) taking all measures as necessary to protect any confidential/privileged information or data entrusted to us by or on behalf of HKIRC from being divulged to a third party other than those allowed in this Contract.

Signature
(Name of the Contractor)
(Name of the Signatory)
(Position of the Signatory)
(Date)

Appendix C – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 12 – Time Schedule, item no. 4 for the proposal submission deadline.
Hard copies	No Hard Copy is required
Electronic copy	Electronic copy is mandatory. It shall be sent by email to pm-procurement@hkirc.hk
Proposal format	Specified in this document
Page count	40 pages or fewer
Font	Electronically published or typed. Times New Roman 12-point font.

1 Proposal Content

The proposal should contain the following:

- Cover Page
- Executive Summary
- Conflict of Interest Declaration
- Company Background
  - Financial Situation
  - Track Records
  - Organization and management team
  - Project team with credentials
  - Company credentials
  - Staff credentials
- Approach and Methodology
- Project management methodology
- Understanding of our requirements
- Knowledge and Advice on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Timetable
- Commercial and Payment Terms. e.g. Compensation for delay

2 Cover Page

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

Cover Page		
Project Title		
		Ethical Phishing Email Campaign 2026 (Tender Ref.: RFP-CYBERSEC-2026-01)
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

3 Executive Summary

The executive summary provides a brief synopsis of the commercial and technical solution the vendor proposed for the project/service. This summary must be non-confidential. It should fit on a single page.

The executive summary should be constructed to reflect the merits of the proposal and its feasibility. It should also clearly specify the project/service's goals and resource requirements. It should include:

- Rationale for pursuing the project or service, the methodology/technology needed and the present state of the relevant methodology/technology.
- Brief description of the vendor's financial situation.
- Brief description of the vendor's facilities and experience on similar projects or services

4 Conflict of Interest Declaration

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

5 Company Background

The vendor must describe its company background. Major activities, financial situation, organizational structure, management team and achievements in similar projects/services or service outsourcing of the company should be elaborated. Track records are preferred.

List the key technical and management personnel in the proposal. Provide a summary of the qualifications and role of each key member. Please indicate where the key members station, i.e. local or non-local.

6 Approach and Methodology

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

7 Project Management Methodology

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

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

9 Knowledge and Advices on Projects/Services

The vendor should describe their knowledge and advice to ensure the success of this project/service

or projects/services with similar nature.

10 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.

11 Proposed Costs of Service and Payment Schedule

The cost shall be broken down by each tasks. The payment shall be scheduled based on the milestones and/or deliverables.

12 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.

13 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 D – HKIRC Information Security Policy: An Extract Relevant to Outsourcing

This document provides an extract of the HKIRC Information Security Policy (the "Policy") 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 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 refers 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.

<-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><-><->

7. HUMAN RESOURCES SECURITY

7.1 PRIOR TO EMPLOYMENT

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.

7.1.1 Security roles and responsibilities of employees, contractors and third-party users shall be defined and documented in accordance with the Organization's information security policy.

7.1.2 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.

7.1.3 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 Organization's responsibilities for information security.

7.2 DURING EMPLOYMENT

Security objective: To ensure that all employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

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

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

7.3 TERMINATION AND CHANGE OF EMPLOYMENT

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

7.3.2 All employees, contractors and third-party users shall return all of the Organization's assets in their possession upon termination of their employment, contract or agreement.

7.3.3 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.

14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

14.2.7 The organization shall supervise and monitor the activity of outsourced system development.

16. INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

Security objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.3 Employees and contractors using the Organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

Appendix E – SECURITY RISK ASSESSMENT AND AUDIT

- The Security Auditor shall conduct the SRAA for the System before its production launch.
- The Security Auditor shall reference the documents as mentioned in the below Section when performing the SRAA. The requirements listed in these reference documents together form the "Security Baseline" for the assessment and audit.
- The Security Auditor 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 System by performing multi-level interviews, group discussions, surveys, equipment and configuration checking etc., where appropriate. The Security Auditor 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:
    - Management responsibilities;
    - IT security policies;
    - Human resource security, including security awareness training;
    - Asset management;
    - Access control, such as access privileges;
    - Cryptography;
    - Physical and environmental security;
    - Operations security;
    - Communications security;
    - System acquisition, development and maintenance;
    - Outsourcing security;
    - Security incident management;
    - IT security aspects of business continuity management; and
    - 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 The policies provided by HKIRC such as IT Security Policy and Baseline IT Security Policy (S17) that are relevant to and are within the scope of the assessment or audit. 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. An example of the checklist can be found in Annex D of Practice Guide for Security Risk Assessment & Audit (ISPG-SM01) (https://www.govcert.gov.hk/doc/ispg-sm01-v2.1_EN.pdf). This checklist is not intended to cover all aspects, but rather acts as a preliminary reference.
- The Security Auditor shall perform vulnerability scanning at network, hosts and systems which should at least cover the following where appropriate:
    - Network level probing/scanning and discovery;
    - Host vulnerability tests and discovery;
    - System/application (including web system/application) scanning;
    - Password audit;

  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).
- The Security Auditor shall perform web penetration testing which should at least cover the following:

- Conduct manual penetration testing which covers the latest version of the top ten most critical web application security risks of logical flaws, error handling and system information leakage, file uploading and execution and input validation issues;
    - 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;
    - 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;
    - Explain and analyse the identified vulnerabilities for its likelihood and impact to the website/web application; and
    - 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 Security Auditor should agree with HKIRC on the scope, possible impact and fallback/recovery procedure.
- The Security Auditor shall perform risk analysis on every aspect which shall include, but is not limited to, the following:
    - Human resource security;
    - Asset management;
    - Access control;
    - Cryptography;
    - Physical and environmental security;
    - Operations security;
    - Communications security;
    - System acquisition, development and maintenance;
    - Outsourcing security; and
    - IT security aspects of business continuity management

  to determine the value of the assets and their associated risks through the following processes:
    - Asset identification and valuation;
    - Threat analysis;
    - Vulnerability analysis;
    - Asset/threat/vulnerability mapping;
    - Impact and likelihood assessment; and
    - Risk results analysis.
- The Security Auditor 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.
- The Security Auditor shall document the findings and results of the security risk assessment and vulnerability tests in a report ("Security Risk Assessment and Audit Report").

- The Security Auditor shall conduct a presentation to HKIRC to report the findings of the security risk assessment.
- The Security Auditor shall identify and review relevant statutory, regulatory and contractual requirements.
- The Security Auditor shall check for conformance to existing security policies, standards, guidelines and procedures.
- The Security Auditor shall document the findings and results of the security audit in the Security Risk Assessment and Audit Report.
- The Security Auditor shall conduct a presentation to HKIRC to report the findings of the security audit.
- The Security Auditor shall ensure that the services provided have minimum impacts on the daily operations of HKIRC and related parties.
- The Security Auditor shall carefully schedule all activities (in particular for vulnerability tests) to avoid/minimise service interruption and agree with user on the schedule, possible impact and fallback/recovery procedure.
- The Security Auditor shall provide the software and equipment, if necessary, for carrying out the tasks free of charge to the HKIRC.
- The Security Auditor shall ensure that no malicious software (e.g. computer virus, 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, email, floppy diskette, hard disk, CD-ROM, Internet web page) when disseminate and/or exchange with the participants.
- The external independent Security Auditor assigned to conduct SRAA shall meet the requirements specified in the table below:

Role	**Job Duites**	**Requirements #**
Security Auditor (SRAA)	Conduct the SRAA for the System (Shall not involve in any tasks related to the provision of the Services for the System except the SRAA)	• Shall not be the direct employee of the Contractor and shall be independent to the Contractor • Shall have at least fifteen (15) years of IT experience • Shall have at least four (4) years working experience in security risk assessment and audit related projects • Shall have valid certification of Certified Information Security Auditor (CISA) or Certified Information Security Professional (CISP) or Certified Information System Security Professional (CISSP)

- All designated team members shall be able to read and write English and Chinese as well as communicate in Cantonese.
- Additional team members may be proposed by the Contractor if considered appropriate. The submitted proposal shall describe how the Project Team will be structured in providing the services, and provide a full description of the experience of all designated team members and their proposed roles in the Work Assignment. Each designated team member cannot assume more than one (1) role.
- In case of staff resignation, replacement staff shall have the same or more experience and qualification as the resigned staff.
- The proposed PM and SA are considered to be the key project team members. In case of staff resignation, replacement staff shall have the same or more experience and qualification as the resigned staff and proper skill transfer shall be provided to the new staff to ensure competence on the support level. All members shall provide non-resident services for this Work Assignment. For the avoidance of doubt, off-shore service is NOT acceptable for this Work Assignment.
- HKIRC may request the Contractor to provide relevant information to substantiate the qualifications, experience and past performance of all the designated team members on need basis. The Contractor shall provide the required relevant information within three (3) working days upon receipt of HKIRC's request.
- The Contractor shall ensure sufficient manpower to be allocated to the Work Assignment at various project stages. If delay of project activities caused by the Contractor happens during the course of the Work Assignment, the Contractor shall provide additional manpower resources at no extra cost upon request from HKIRC to meet the project schedule.
- HKIRC reserves the right to require replacement of the members of the Project Team. Any proposed addition or change of members of the Project Team initiated by the Contractor shall obtain the HKIRC's prior written approval

- # Appendix F – PRIVACY IMPACT ASSESSMENT (PIA)
  - The Assessor shall conduct the PIA for the System before its production launch.
  - The PIA shall include the following:
    - Data processing cycle analysis;
    - Privacy risk analysis;
    - Recommendations or measures in avoiding or mitigating privacy risks; and
    - Compile a PIA report.
  - The Assessor shall assess and ensure compliance with Personal Data (Privacy) Ordinance (Cap. 486) and other relevant Ordinances, prevailing guidelines and recommendations from the Office of the Privacy Commissioner for Personal Data, and make reference to prevailing industry and international practices.
  - The Assessor shall identify the data privacy potential effect, actual effects, implication, issues and risks, and provide recommendations on how the identified potential and actual effects upon personal data privacy can be mitigated.
  - The Assessor shall work with all stakeholders in conducting the PIA.
  - The Assessor shall conduct the Privacy Compliance Audit with the objective of reassessing whether the recommendations of the Privacy Impact Assessment have been adequately addressed.
  - The Assessor is required to produce an assessment report (refer to "TABLE OF CONTENTS OF PRIVACY IMPACT ASSESSMENT REPORT (SAMPLE)" paragraph) in concluding the PIA, which document the findings, recommendations, and privacy protective measures in addressing the privacy risks, to the satisfaction and endorsement of HKIRC within the agreed timeframe. The report shall be completed within 3 weeks after the commencement of the PIA.
  - The Assessor will be required to present its recommendations and reports.
  - Upon request of the HKIRC, the Assessor will also be required to attend regular working meetings to keep track of progress and to discuss issues relating to the assessments. Draft reports should be sent to HKIRC for comment as soon as practicable, to facilitate early consideration.
  - The Assessor shall, within 3 working days after the completion or termination of the Service Contract for any reason whatsoever, confirm in writing the destruction / return of all related materials belonging to / collected from any stakeholders. The confirmation should be supplemented by a full list of the materials destroyed / returned.
  - The Assessor shall comply with the following regulations and policy:
  - Baseline IT Security Policy [S17], IT Security Guidelines [G3] and all related documents issued by the Digital Policy Office of the HKSAR Government;
  - Other prevailing Government regulations, standards, guidelines and procedures requested by HKIRC

The Assessor's assignment team as a whole, and each individual within the team, should have the experience of conducting studies of similar nature and scope of those required in this work assignment. The composition of the Assessor's assignment team ("Project Team") for the Services shall include one project manager and at least one system analyst and they shall meet the related requirements specified in the table below:

Role	Job Duties	Requirements
Project Manager (PM)	• Overall project management on the Services • Be a single contact point for HKIRC • Coordinate with third parties including any stakeholders for the necessary arrangement	• Shall have at least eight (8) years of post-qualification IT experience • Shall have at least four (4) years' experience in consultancy study and privacy and data protection services; • Shall have at least one reference project in leading Privacy Impact Assessment for IT project in HKSAR Government or public organisations
Systems Analyst (SA)	• Support PM on the Services • Conduct the PIA • Compile documentations	• Shall have at least 4 years of post-qualification IT experience; • Shall have at least 2 years of working IT experience in consultancy study and privacy and data protection services; • At least one reference project in performing Privacy Impact Assessment for IT project in HKSAR Government or public organisations

- Additional team members may be proposed by the Assessor if considered appropriate. The submitted proposal shall describe how the Project Team will be structured in providing the services, and provide a full description of the experience of all designated team members and their proposed roles in the Work Assignment. Each designated team member cannot assume more than one (1) role.
- In case of staff resignation, replacement staff shall have the same or more experience and qualification as the resigned staff.
- The proposed PM and SA are considered to be the key project team members. In case of staff resignation, replacement staff shall have the same or more experience and qualification as the

resigned staff and proper skill transfer shall be provided to the new staff to ensure competence on the support level. All members shall provide non-resident services. For the avoidance of doubt, off-shore service is NOT acceptable.

- HKIRC may request the Assessor to provide relevant information to substantiate the qualifications, experience and past performance of all the designated team members on need basis. The Assessor shall provide the required relevant information within three (3) working days upon receipt of HKIRC's request.
- The Assessor shall ensure sufficient manpower to be allocated to the Services at various project stages. If delay of project activities caused by the Assessor happens during the Service, the Assessor shall provide additional manpower resources at no extra cost upon request from HKIRC to meet the project schedule.
- HKIRC reserves the right to require replacement of the members of the Project Team. Any proposed addition or change of members of the Project Team initiated by the Assessor shall obtain the HKIRC's prior written approval

TABLE OF CONTENTS OF PRIVACY IMPACT ASSESSMENT REPORT (SAMPLE)

The PIA report shall, as a minimum, include the following sections:

- Executive Summary
- Introduction
  - Background
  - Objectives
  - Scope of PIA
- The Aspect of Assessment (Confidentiality, Integrity, Continuity and Auditability)
- The Requirements (derived from the Ordinance)
- Reference Documentation
- Consideration of Privacy Principle / Legislation and Policies
- Date of Assessment and Status Update
- Glossary and Terms Used (if applicable)
- Project Proposal / Approach for Assessment
- Data Flow Analysis
  - Business Flow Diagram and Description
  - Data Flow Table
- Privacy Analysis
  - Data Collection Process
  - Use, Disclosure and Retention of Data
- Privacy Risk Management Plan
  - Privacy Risk Mitigation
  - Privacy Risk Management Plan - Summary
- Compliance / Monitoring Mechanisms
- Assessor's Opinion
- Detailed Findings and Recommendations

Appendix G - PROFESSIONAL STAFF REQUIREMENT

The composition of the Contractor's assignment team ("Project Team") for the Services shall include one project manager and at least three system analysts and they shall meet the related requirements specified in the table below:

Role	Job Duties	Requirements #
Project Manager (PM)	• Overall project management on the Services for the System • Be a single contact point for HKIRC • Coordinate with third parties including the SRAA/PIA vendor for the necessary arrangement	• Shall have at least ten (10) years of IT experience • Shall have at least four (4) years' experience in managing web-based and database application
Systems Analyst (SA)	• Support PM on the System • Implement necessary program change to the System • Perform installation, configuration and system hardening for the System • Conduct load test, system test and functional test • Prepare test plan, specifications and test cases • Provide the Internet mailboxes and Internet domains to support the Phishing Drill • Work with SRAA/PIA vendor to follow up and resolve their findings • Compile documentations	• Shall have at least five (5) years of IT experience • Shall have at least two (2) years' experience in the capacity of SA on system analysis and design • Shall have completed at least two (2) projects related to email integrated solution and/or phishing simulation in the role of SA • Shall have completed at least two (2) projects related to web-based application development project • Shall have completed at least two (2) projects implemented under virtualised environment using Linux or Microsoft Windows; and database system using MySQL or Microsoft SQL Server

Appendix H – TYPES OF PHISHING AND TOPICS OF PHISHING

Prevailing Types of Phishing

1. Deceptive Phishing

   The most common type of phishing scam, deceptive phishing refers to any attack by which fraudsters impersonate a legitimate company and attempt to steal people's personal information or login credentials. Those emails frequently use threats and a sense of urgency to scare users into replying to the email as soon as possible.

2. Spear Phishing

   Fraudsters customise their attack emails with the target's name, position, company, work phone number and other information to make the emails appear as legitimate and convincing as possible. Similar to deceptive phishing, spear phishing is to lure the victim into clicking on a malicious URL or email attachment to download malware or steal the victim's money or sensitive data.

3. Watering Hole Phishing

   It seeks to compromise some websites, say by injecting malicious code, which are mostly visited by a specific group of users. Once users visit the compromised websites and are deceived into loading infected files, malware can be installed onto user's computer to perform malicious actions without users' knowledge.

4. Vishing (Voice Phishing)

   It involves verbal scams by phishers to trick an individual or organisation into performing actions that are in the best interests of the phishers. The verbal scams can be carried out in various ways such as making a phone call with a falsified caller ID to obfuscate the users, or using an interactive voice response system to redirect users to chat with the phishers directly in order to lure the users into disclosing personal information, etc.

5. Smishing (SMS Phishing)

   It involves phishers sending unsolicited mobile phone SMS text messages mimicking trusted third party to trick users into clicking a malicious link that may redirect the users to a malicious website to lure individuals into providing sensitive data, or providing personal information by replying to the SMS messages, etc.

6. Pharming

   Pharming is an attack that redirects a user's web access from a legitimate website to a fraudulent website for the purpose of stealing user's login credentials or sensitive data. The attack can be conducted through the following ways:

   - Malware-based pharming - Install malware on users' computers to modify the computers' local host files and redirect users to malicious websites.
   - Domain Name System (DNS) server poisoning - Exploit vulnerabilities in DNS servers alter DNS records and redirect users to malicious websites.

7. Wi-Fi Phishing

It attempts to steal sensitive data by convincing wireless network users to connect their mobile devices to the malicious Wi-Fi access point (AP) in the following ways:

- Malicious rogue AP - Phishers install a malicious wireless AP to provide wireless network connection to trick users into entering login credentials, or the phishers perform man-in-the-middle (MITM) attack through the malicious AP.
- Evil Twin - Phishers create malicious Wi-Fi AP pretending to be a legitimate Wi-Fi hotspot with same Wi-Fi service set identifier (SSID), basic service set identifier (BSSID), captive portals, etc. to trick users into disclosing login credentials or sensitive data.

8. Quick Response (QR) Code Phishing

It is a type of scam where phishers hide the malicious links in QR codes and take advantages of the implicit trust of users to perform thoughtless action in scanning the QR codes so as to carry out malicious actions on mobile devices. For instance, the actions can be redirecting user to a malicious website to capture user's sensitive data, connecting the device to a compromised Wi-Fi network or making a payment automatically, etc.

9. Malware Based Phishing

Fraudsters send an email attachment or downloadable file that once clicked, will infect a computer with a virus, ransomware or other malicious programmes. This is exactly what happened in the infamous WannaCry attack that affected more than 200,000 victims in 150 countries after their computers were infected with the malicious software.

10. File Sharing Scams

Fraudsters sent fake Dropbox/Google emails to victims, tried to lure them into entering their login credentials on a fake Dropbox/Google Drive sign-in page hosted on Dropbox / Google Drive itself.

11. Social Media Phishing

There has been a steep increase in the number of phishing scams carried out on social media. Fraudsters use social media sites such as Facebook, LinkedIn or Twitter, to trick users into clicking on malicious links or revealing personal information.

12. Pop-up Phishing

It involves "pop-up" windows with fraudulent messages for users when they are surfing the web. A fake "pop-up" are designed to entice users into clicking on the "pop-up" windows that redirect them to malicious websites to steal sensitive data.