General Business Conditions
for Security Service

Related Parties:

Service Receiver (as stated in page with signature)

(hereinafter referred to as the **Client**)

DQS Management Systems Solutions (HK) Ltd

(hereinafter referred to as the **Provider**)

1. Purpose and Scope of the Service

1.1 The Provider will provide IT or data security service, according to the requested and agreed service scope.

1.2 A service may include part of or all below service items in an agreed service scope:

(a) Penetration Test **(Pen Test)**,

(b) Security Risk Assessment and Audit (or **SRAA** hereinafter),

(c) Privacy Impact Assessment (or **PIA** hereinafter),

(d) Cyber Resilience Assessment Frame (**CRAF**),

(e) Threat Intelligence Based Attack Simulation (**TIBAS**),

(f) Security Assessment for Critical Infrastructure,

(g) Incident Response Assessment,

(h) Red Team Assessment, and

(i) other IT or data security related services as specified.

1.3 The Penetration Test, SRAA and PIA services are defined in Annex A.

1.4 If the service personnel provide any information out of the above stated service scope, according to the requests by the Client or out of goodwill, such information shall be treated as reference only and doesn't constitute an outcome of this service.

1.5 Specially, consulting is not part of the service.

2. Obligations

2.1 The Client authorizes the Provider to conduct the IT or data security service on the systems designated by the Client, in accordance with this agreement.

2.2 Upon request, the Client agrees to provide the required authorizations and information, including those from any third parties, to enable the Provider to carry out the service.

2.3 Upon request, the Client agrees to obtain appropriate consent from its Internet Service Provider (ISP) and/or other associated parties, and to provide evidence of such consent.

2.4 The Client understands that the Provider may actively attempt to breach security controls, when applicable, to obtain access to the Client's systems and data.

2.5 The Client understands that the service may involve access to data and systems accessible via the Client's systems and there is a risk that the service may result in damage, loss, modification or impairment of these data and systems.

2.6 The Client warrants to the Provider that the requested service:

a) is not against any law or regulation applicable to the Client or its systems, and

b) has no harm to the interest of any other party.

2.7 The Client agrees that the Provider can exclude an activity in the service, which the Provider is not convinced lawful or of no harm to the interest of another party.

2.8 The Client shall notify affected parties, such as employees and customers, as applicable, that the test and that their activities in the systems may be monitored during the test.

2.9 The client agrees to arrange mutually convenient time with the Provider to carry out the service and to inform the ISP about it in advance.

2.10 The client agrees to ensure that no transaction, change or input will be made to the data and systems during the agreed test period.

2.11 The Client agrees to notify the Provider immediately if there is any period during the test when the Provider shall stop the service, such as due to impact to critical business processes or to other parties.

2.12 The Client agrees that the Provider may assign subcontractor(s) to carry out the service.

2.13 Addressing the inherent risks from the service, the Client agrees to ensure that:

(a) the data and systems accessible via the Client's systems are backed up regularly and right before the scheduled test service; and

(b) the back-ups can be promptly restored to the systems, when required.

2.14 The client shall assign personnel to support and provide credentials for the assessments.

2.15 The Client will make invalid the credentials provided to the Provider, right after receiving the vulnerability notification report after test, to prevent unauthorized access afterwards.

2.16 The Client agrees not to get IT or information security service from the Provider's assigned personnel or subcontractors for this service, in the following two years after completion of this service, unless otherwise agreed by the Provider in writing in advance.

3. Limitation

3.1 The Client understands that the service:

a) may not identify all true vulnerabilities within the Client's systems,

b) is limited to an assessment of the current state of the Client's environment.

3.2 The Client agrees to make own evaluation on the information and any findings provided by the Provider and on the appropriateness for any action on the basis of such information and findings.

4. Confidentiality

4.1 The information provided shall be used only for the purpose of the required service.

4.2 Neither party shall disclose or permit its employees, agents and sub-contractors to disclose any Confidential Information of the counterparty to any other parties, unless otherwise agreed in writing in advance or required by laws or regulations. This obligation also applies after termination of this contract.

4.3 For this service, the information provided by the Client may be provided to the Provider's subcontractor(s) carrying out the service for the Client. The Provider requires equivalent confidentiality terms with such subcontractor(s).

5. Service Fee

5.1 Unless otherwise specified in writing, the Client shall pay the service fee to the bank account designated by the Provider, within 7 days after receiving the invoice from the Provider.

5.2 Unless otherwise specified in writing, the service prices quoted by the Provider don't cover any local taxes or surcharges to pay out of Hong Kong. The Client is responsible for such taxes or surcharges, if any.

5.3 If the Client fails to pay any service fee when due, the Provider, at its discretion, may enforce its rights or pursue remedies to collect or recover any outstanding amount. the Provider is entitled to employ agents or service providers for such purposes. The Client is required to indemnify and reimburse the Provider for all reasonable amounts of costs (including legal fees) and expenses reasonably incurred by the Provider for such purposes.

6. For the privacy related information provided to the Provider, the Client understands and agrees with the Provider's Privacy Policy posted at the webpage of https://www.dqsglobal.com/en-hk/legal-aspects/privacy-policy/.

7. Liability

7.1 The Client will indemnify the Provider against all claims, cost, loss or liability which may arise from:

a) carrying out the service requested by the Client, or

b) the Client's subsequent actions on the basis of the information and findings from the service.

7.2 The direct and indirect compensation in total to either party, due to the fault of the counterparty, will not exceed the amount of the agreed service fee. The potential costs and expenses defined in Clause 5.2 are excluded from it.

8. Validity of Contract

8.1 The contract shall take effect after being signed by the authorized representatives of both parties and stamped with the Provider's seal, on this contract or a quotation with reference to this contract.

8.2 This contract replaces any formerly agreed contract or terms, orally or in writing, between both parties, when applicable.

8.3 If a party materially breaches the agreement and does not remedy that breach within 7 days of receiving a notice to do so, then the other party may cancel the affected service, in whole or in part.

8.4 The contract will end after the required service is completed and the service fee is fully received by the Provider.

8.5 The termination of this contract, no matter in which way, shall neither affect any liability of either party constituted before the termination, nor reduce any service fees that shall be paid by the Client to the Provider.

9. Disputes

The dispute related to this contract is subject to friendly negotiation by both parties. If the negotiation fails, both parties agree that the dispute will be resolved according to the applicable laws in Hong Kong.

Annex A – Definition of Service Items

A.1 Penetration Test (Pen Test)

A Penetration Test Service is to identify the vulnerabilities within the Client's systems, to the extent possible by the assigned service personnel with reasonable efforts.

The service includes:
(a) a simulated cyber-attack or similar threat detection simulation on the Client's computer systems, to identify their vulnerability, and
(b) a vulnerability notification report.

A.2 Security Risk Assessment and Audit (SRAA)

A Security Risk Assessment and Audit service is to identify the vulnerabilities within the Client's IT systems, to the extent possible by the assigned service personnel with reasonable efforts.

A SRAA service includes IT related Security Risk Assessment (or **SRA** hereinafter in this document), Security Audit (or **SA** hereinafter in this document SA).

(a) The Provider's **SRA** process is to identify, analyse and evaluate the security risks, with a report of findings about risks, to support the client's decisions on the establishment of security program, and taking mitigation measures to reduce the risks to an acceptable level.

(b) The Provider's **SA** process is an audit on the level of compliance with the client's established security policy and standards, with a report of findings of compliance or non-compliances, to determine the overall state of the existing protection and to verify whether the existing protection has been performed properly.

A.3 Privacy Impact Assessment (PIA)

A Privacy Impact Assessment Service is to analyse a program's impact on individuals' information privacy.

The assessment will address the privacy, confidentiality and security issues associated with the processing of personal data, against the principles of the **selected regulations** associated with personal data protection, to the extent possible by the assigned service personnel with reasonable efforts.

The service includes:
(a) identification of assessment scope,
(b) personal data flow analysis,
(c) privacy analysis,
(d) identification of privacy risks,
(e) conclusions, and
(f) an assessment report, covering above items.

Notes for A.1, A.2 and A.3:

- The Pen Test, SRAA or PIA service does NOT include fixing the findings from the assessment.
- Unless otherwise specified in writing, for a Pen Test, SRAA, or PIA service, **one** follow-up assessment can be offered, when required, to verify the Client's implemented improvement actions to address the findings from initial assessment.
  For this follow-up service, the Client shall implement the improvement actions within 3 months after the initial test, assessment or audit.
- An additional Follow-up Assessment can be provided with a separate quotation.
- It is NOT guaranteed that the final report will have no findings, even after the follow-up.