香港珠海學院
HONG KONG
CHU HAI COLLEGE

CONFIDENTIAL
TEND/HKCHC/AS/2026

Tender Document

Second Tier Firewall for Network Security Optimization Project

for

Hong Kong Chu Hai College,
80 Castle Peak Road, Castle Peak Bay,
Tuen Mun, Hong Kong

Hong Kong Chu Hai College Limited

April 2026

香港珠海學院
HONG KONG
CHU HAI COLLEGE

CONFIDENTIAL
TEND/HKCHC/AS/2026

SECTION ONE: INFORMATION TO TENDERERS

a. Preambles

The purpose and intent of this "Information to Tenderers" is to facilitate the tenderers to submit tender for providing accounting system and after-sales service support at Hong Kong Chu Hai College (the "HKCHC"). in Hong Kong, Tuen Mun, New Territories.

The tender document consists of:

1. Information to Tenderers.
2. Technical Specification Requirements.
3. Scope of Work.
4. Tender Evaluation.
5. Terms and Conditions of Agreement

The tenderer shall check the number of pages of all the documents attached. Should there be any missing or indistinct pages, the tenderer shall inform the Employer at once and have the same rectified.

Should the tenderer for whatsoever reason be in doubt as to the precise meaning of any description or item, clarification shall be made for correct meaning before the closing time for tender submission.

b. The Site

The Site for the Works is located at the School Campus, Hong Kong Chu Hai College, 80 Castle Peak Road, Castle Peak Bay, Tuen Mun, New Territories, Hong Kong as confined within the building lot.

c. Tender Inquires

Any inquiries from tenderers concerning this tender shall be directed to the HKCHC and attention to procurement@chuhai.edu.hk

d. Tender Closing Date

All tenders must be submitted complete, entire, and in the required to HKCHC no later than **02:00 p.m. on 8 May 2026 (Fri)**. Tenders received after the closing time will NOT be accepted.

Please note that the closing time and date shall automatically be deferred to 3:00 pm on the next earliest possible working day if Tropical Cyclone Warning Signal No. 8 or above is hoisted or Black Rainstorm Warning is announced by the Government before and remains hoisted beyond the closing time. However, the closing time and date will remain unchanged should the Tropical Cyclone Warning Signal No. 8 or above or Black Rainstorm Warning be lowered or withdrawn two hours or more before the specified

closing time.

Should a tenderer discover a genuine error in the tender after it has been deposited, a written amendment submitted on or before the closing time of the tender submission may be accepted.

e. Delivery of Tenders

One set of original, **one set of copy** and **one soft copy via USB** must be submitted by hand, courier delivery, or registered mail. One set should be marked "Original" and the other one sets marked "Copy". In the event of any discrepancy between the copies, the "original" one will be taken as the true Tender.

The tender is to be submitted in a sealed envelope labeled "**Second Tier Firewall for Network Security Optimization Project**" and "**Private & Confidential**" and be addressed to the following:

Company	Hong Kong Chu Hai College Limited
Address	E701, 7/F, Hong Kong Chu Hai College, 80 Castle Peak Road, Castle Peak Bay, Tuen Mun, New Territories, Hong Kong
Contact	Finance Office
Tender Box Location	Cashier, Registrar's Office, 1/F, Hong Kong Chu Hai College, 80 Castle Peak Road, Castle Peak Bay, Tuen Mun, New Territories, Hong Kong

f. Confidentiality Provision

The terms of this tender and all other information provided by us in connection with this initiative are to be treated by your company as strictly confidential and proprietary. Such materials are to be used by your company solely to respond to this tender. Access to this information shall not be granted to third parties except on prior written consent of HKCHC and upon the written agreement of the intended recipient to treat the same as confidential. We may request at any time that any of our material be returned or destroyed at our election.

g. This Tender is NOT an Offer to Agreement

This tender is not an agreement offer, nor should it be construed as such. It is a definition of the specific requirements of HKCHC and an invitation to recipients to submit a responsive proposal addressing such requirements. The Company reserves the right to make no selection and enter into no agreement as a result of this tender. Only the execution of a written agreement between the Company and a Tenderer will obligate the Company by the terms and conditions contained in such agreement.

h. Your Response to this Tender Constitutes an Offer to do Business

It should be understood that your response to this tender constitutes an offer to do

business on the terms stated in your proposal and should an agreement be awarded to you, the Company may, at its option, incorporate all or any part of your proposal to this tender in the agreement. The Company reserves the right to accept your offer without further discussions and without any additional opportunity for you to amend, supplement, or revise your submitted offer after the Tender Closing Date.

i. Rights Of Hong Kong Chu Hai College Limited

The Company reserves the right to reject all proposals, to accept one which is not at the lowest cost or one which provides a lesser or larger range of services than indicated in this tender.

The Company is not bound to give any explanation or reason for the rejection of any of the proposals or the award or non-award of the agreement to any or none of the tenderers.

j. Incurred Expenses & Property Rights

This tender does not commit or obligate the Company to pay any expenses incurred by you in the preparation of your proposal. All such expenses are solely at the risk of the tenderer. By submitting your tender you agree that all proposals to this tender shall become the property of the Company.

k. Non-Use of Hong Kong Chu Hai College Name

You shall not use the names, trademarks, or proprietary indicia of HKCHC nor its parent corporation, subsidiaries, or affiliates as a reference, or in any advertising, announcement, press release, or promotional materials, including testimonials, quotations, case studies, and other endorsements. No exceptions are granted without prior written consent from the Company.

l. Media Release

In addition to obligations under your existing confidentiality agreement with the Company, you will not make (or cause to be made) any public announcement relating to this tender or the Company evaluation process, and shall not otherwise publicize, confirm the existence of, or comment on this tender in any manner, without the express written consent of the Company.

m. Gifts or Payments

Tenderers shall not offer, agree to give or give any gift or consideration of any kind to any employee or representative of the Company or its affiliated enterprises as an inducement or reward for any act, including, without limitation, refraining from an act and showing favor or disfavor to any person or entity, about the evaluation and consideration of this proposal or award of this or any other agreement by HKCHC.

SECTION TWO: TECHNICAL SPECIFICATION REQUIREMENTS

General Architecture Requirements

The proposed firewall solution shall function as a second-tier security layer, operating in conjunction with an existing perimeter firewall infrastructure, to provide defence-in-depth and advanced threat prevention for an education network environment.

The solution shall be suitable for deployment in education institutions, supporting academic, administrative, research, and student access networks with differing security postures.

The firewall shall support deployment in inline (Layer 3), transparent (Layer 2), and virtual wire modes to enable flexible integration without requiring major network redesign.

1. Next-Generation Firewall Capabilities

1.1. **Performance Parameters**

1.1.1. Application Firewall performance(appmix) shall be greater than or equal to 8.5Gbps

1.1.2. Performance when application identification and IPS features enable (appmix) shall be greater than or equal to 4.5Gbps

1.1.3. Antivirus inspection throughput for all supported AV scanning modes (appmix) shall be greater than or equal to 4.5 Gbps

1.2. **Network Interfaces**

1.2.1. Configuration: at least 4 x 10GE optical interfaces, and at least 6 x GE optical interfaces, and at least 4x 5G POE interfaces, and at least 8 x GE electrical interfaces.

1.3. The firewall shall be a true Next-Generation Firewall (NGFW) that performs application identification, user identification, and content inspection at the network layer, rather than relying solely on port- or protocol-based controls.

1.4. Security enforcement shall be based on:

- Application identity
- User and group identity (directory-integrated)
- Device and location context
- Security risk profile

1.5. The firewall shall be capable of identifying and controlling encrypted applications and evasive applications, including those using non-standard ports or tunnelling techniques.

1.6. The proposed firewall solution shall have been positioned in the “Leaders” quadrant of the Gartner Magic Quadrant for Enterprise Network Firewalls for no fewer than 11 consecutive years and recognized as a “Leader” in The Forrester Wave: Enterprise Firewalls.

2. Application-Aware Security Controls

2.1 The solution shall provide granular application visibility and control, allowing administrators to:

- Permit, deny, restrict, or shape traffic based on specific applications and application functions
- Control educational, social media, collaboration, streaming, and cloud-based applications independently

2.2 Application identification shall remain effective even when applications are encrypted, fragmented, or dynamically port-mapped.

2.3 The firewall shall allow policy creation without dependency on static IP addresses or ports, supporting dynamic and cloud-based services commonly used in modern education environments.

3. User and Identity Integration

3.1. The firewall shall integrate with directory services (e.g., LDAP, Active Directory, Azure AD or equivalent) to enable user- and group-based security policies.

3.2. Policies shall be able to distinguish between:

- Students
- Academic staff
- Administrative staff
- IT administrators
- Guest or temporary users

3.3. The solution shall support dynamic user mapping, enabling enforcement even when users move between devices, networks, or locations.

4. Threat Prevention and intrusion protection

4.1. Integrated Intrusion Prevention

4.1.1. The firewall shall include integrated intrusion prevention system capable of detecting and blocking in real time:

- Known exploits
- Zero-day threats
- Command-and-control traffic
- Lateral movement attempts

4.1.2. The proposed solution shall support real-time, inline deep learning–based detection and prevention to identify and block both known and unknown command-and-control traffic without reliance on signature-only mechanisms

4.2. Advanced Malware and Threat Analysis

4.2.1. The solution shall provide real-time malware analysis, leveraging either cloud-assisted and/or on-premises threat intelligence services, with seamless policy enforcement.

4.2.2. Unknown files and suspicious payloads shall be automatically analyzed in a sandboxed execution environment, with threat verdicts and protections dynamically distributed and enforced across the entire firewall deployment.

4.2.3. The proposed solution must support sandbox analysis for below file types:

- Portable Executable (EXE and DLL),
- Android Application Package (APK),
- Portable Document Format (PDF),
- Microsoft Office (doc/docx, xls/xlsx, and ppt/pptx),
- Java Applet (jar and java class),
- Flash,
- Mac OS X file types (Mach-O, DMG, PKG, and Application Bundles),
- Linux (ELF) files,
- Script (BAT, JS, VBS, PS1, Shell script, and HTA) files,
- Archive (RAR and 7-Zip) AND
- Email link

4.3. Deep Learning-Based Threat Detection

4.3.1. The firewall shall provide an in-box deep learning model capable of detecting common and advanced security risk techniques, including but not limited to:

- SQL injection
- Command injection
- Other application-layer attack techniques

4.3.2. Deep learning–based threat detection capabilities shall operate inline and in real time, without introducing latency or requiring traffic redirection to external devices.

4.4. The proposed solution shall provide post-quantum cryptography (PQC) threat signatures to identify and mitigate emerging cryptographic threats associated with quantum-resistant attack techniques.

4.5. All threat prevention, malware analysis, deep learning inspection, and cryptographic threat detection capabilities shall operate inline and in real time, without requiring separate appliances or out-of-band processing.

4.6. Phishing and Credential Protection

4.6.1. The proposed solution shall provide credential phishing prevention, enabling

administrators to block users from submitting corporate credentials to untrusted or malicious websites, while allowing credential submission to approved corporate and sanctioned sites.

4.6.2. The solution shall provide protection against advanced man-in-the-middle (MITM) phishing and SaaS-hosted phishing attacks, including attacks leveraging legitimate cloud platforms.

4.7. Anti-Evasion and Web Threat Detection

4.7.1. The proposed solution shall include anti-evasion mechanisms to protect against techniques such as:

- Website cloaking
- Fake CAPTCHA challenges
- HTML character encoding and obfuscation

4.7.2. The solution shall perform real-time web page analysis and classification using a combination of inline machine learning and cloud-based analysis to prevent:

- JavaScript-based malware exploits
- Phishing attacks embedded within web pages
- Emerging and unknown web-based threats

4.8. URL Categorization and Policy Control

4.8.1. The proposed solution shall support more than 60 URL categories for category-based URL filtering.

4.8.2. Each URL shall be assignable to up to four distinct categories to support flexible and granular policy enforcement.

4.8.3. URL filtering policies shall be enforced consistently for traffic over both IPv4 and IPv6 networks.

4.9. Translation and Search Protection

4.9.1. The proposed solution shall support URL filtering protection for website translation services, ensuring that tools such as Google Translate cannot be used to bypass URL filtering policies.

4.9.2. The solution shall support Safe Search enforcement for supported search engines.

4.10. Machine Learning and Visual Phishing Detection

4.10.1. The proposed solution shall provide machine learning models capable of analyzing images within web pages to determine whether they imitate brands commonly abused in phishing campaigns.

4.10.2. The solution shall provide advanced SaaS phishing detection models, incorporating:

- Webpage source code analysis
- Image and text analysis
- URL tokenization and pattern recognition

4.11. Privacy and Compliance

4.11.1. The proposed solution shall support selective SSL/TLS decryption, enabling compliance with data privacy and regulatory requirements while maintaining security inspection capabilities.

4.12. DNS Policy and Threat Classification

4.12.1. The proposed solution shall allow the creation of granular DNS security policies based on domain signature sources, including but not limited to:

- Command-and-control (C2) domains
- Dynamic DNS-hosted domains
- Malware domains
- Recently registered domains

4.12.2. DNS policies shall support severity-based logging and differentiated enforcement actions.

4.13. DNS Attack Detection and Prevention

4.13.1. The proposed solution shall support real-time detection and blocking of DNS hijacking attacks, including:

- Compromised DNS registrar attacks
- DNS injection attacks
- DNS cache poisoning
- DNS spoofing and man-in-the-middle (MITM) attacks

4.14. 4.2.2. The solution shall provide proactive detection and blocking of DNS misconfigurations, including:

- DNS record misconfigurations
- Claimable or non-resolvable domains

4.15. Advanced DNS Threat Techniques

4.15.1. The proposed solution shall protect against advanced DNS-based threats, including:

- Domain Generation Algorithm (DGA)–based attacks
- Directory-based DGA techniques
- DNS tunneling and ultra-slow tunneling
- Fast-flux network attacks

4.15.2. Detection of DGA-generated domains and DNS tunneling traffic shall rely on machine learning–based analysis, rather than static pattern-matching signatures.

4.15.3. The solution shall apply machine learning to DNS requests to identify and block

newly generated malicious domains in real time.

4.16. Visibility and Monitoring

4.16.1. The proposed solution shall be capable of identifying the original infected endpoint or user, rather than only reporting the internal DNS server as the source.

4.16.2. The solution shall support Passive DNS monitoring for historical analysis and threat investigation.

4.17. Deployment and Resilience

4.17.1. The proposed solution shall secure DNS traffic without requiring network reconfiguration and shall be designed to minimize opportunities for policy bypass.

4.17.2. The solution shall provide detection and protection against stockpiled domains and domain squatting attacks.

5. SSL/TLS and Encrypted Traffic Inspection

5.1. The proposed solution shall support SSL/TLS decryption and inspection for both inbound and outbound traffic, subject to institutional privacy and compliance policies.

5.2. Decryption policies shall be:

- Granular and rule-based
- User-, application-, and category-aware
- Capable of selective inspection to preserve performance

5.3. The proposed solution shall maintain full security inspection capabilities for encrypted traffic, including malware detection and data exfiltration prevention.

5.4. The proposed solution shall support authenticate certificates up to 8912-bit RSA keys from the destination server.

6. Centralised Management and Visibility

6.1. The firewall shall support centralised management, allowing multiple firewall devices to be administered from a single management platform.

6.2. The management system shall provide:

- Unified policy management
- Configuration versioning and rollback
- Centralised logging and reporting

6.3. The solution shall offer high-fidelity traffic and threat visibility, enabling security teams to:

- Quickly identify compromised devices or users
- Analyse application usage trends
- Support incident response and compliance audits

7. High Availability and Scalability

7.1. The firewall shall support high-availability (HA) configurations, including active/active and active/passive modes.

7.2. Failover shall be stateful, ensuring minimal session disruption during hardware or link failure.

7.3. The solution shall scale to support:
- Increasing student populations
- Remote and hybrid learning models
- Growth in cloud and SaaS adoption

8. Performance Requirements

8.1. The firewall shall deliver consistent throughput with full security services enabled, including threat prevention, application inspection, and SSL decryption.

8.2. Performance metrics shall be based on real-world traffic conditions, not solely on raw packet forwarding rates.

8.3. The solution shall be capable of handling peak academic periods without degradation of user experience.

9. Integration and Interoperability

9.1. The firewall shall interoperate seamlessly with existing network security infrastructure, including:
- Perimeter firewalls
- Network access control systems

9.2. The solution shall provide open APIs and standard logging formats to support automation, orchestration, and third-party integrations.

10. Education-Focused Security and Compliance

10.1. The firewall shall support content categorisation and policy enforcement suitable for educational institutions, including age-appropriate access controls.

10.2. The solution shall assist institutions in meeting data protection, cybersecurity, and acceptable-use policy requirements.

10.3. Reporting and logging shall support audit, compliance, and governance requirements commonly found in education environments.

11. Licensing and Subscription Model

11.1. The solution shall offer modular, subscription-based security services, allowing the institution to enable advanced features as required.

11.2. Licensing shall be transparent, scalable, and suitable for multi-year education procurement cycles.

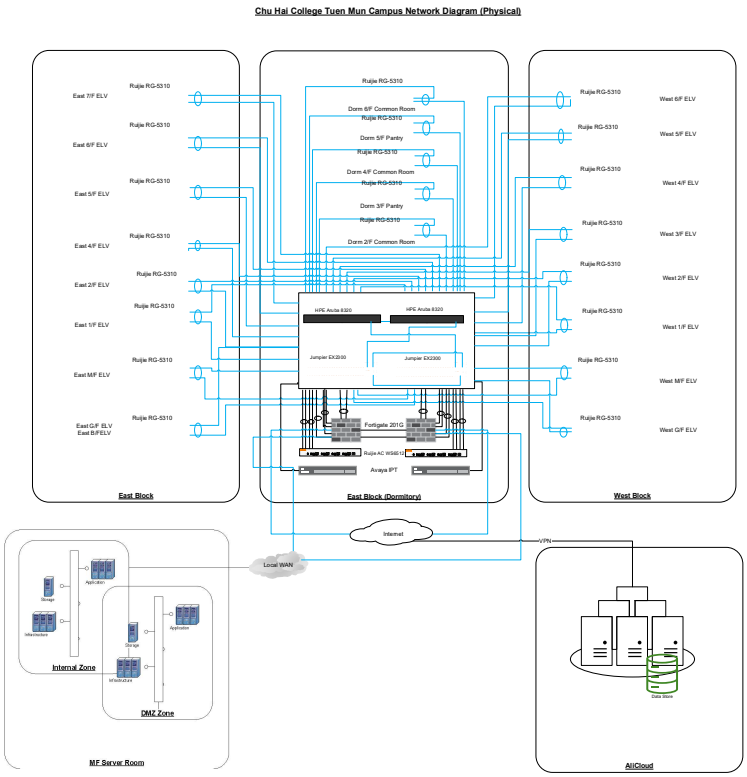
12. **Technical Support and Service**

12.1. Vendor Support: The solution shall provide comprehensive 7x24x4 technical support services（3 years）.

12.2. Software Updates and Patches: Ensure regular provision and updates of software and hardware patches to address security threats and improve performance.

SECTION THREE: SCOPE OF WORK

Current Overall Architecture



Please refer to ***Appendix 1 – CHC Network Diagram V0.4.pdf*** for details

Current Network Layer (M/F Server Room)

At the center of the network lies the Main Server Room, equipped with:

- HPE Aruba 8320 Core Switches (likely running as a core/aggregation pair)
- Jumpier EX2300 switches (management / auxiliary connectivity)
- Fortigate 201G Firewall (campus perimeter security)
- Ruijie AC WS6512 (wireless controller Gateway)
- Ruijie RG-5310 (Access Switches)
- Ruijie RG-S6110 (likely wireless APs Access Switches)
- Data Store / Storage Systems
- VPN Infrastructure
- DMZ Zone for public-facing services
- This is the heart of all routing, security, and server connectivity.

Project Management Services

Project planning and joining all stakeholders' meetings to assess the project implementation method, risk management and contingency plan

Implementation and Deployment

Work with Chu Hai College Education Technology Services Department to understand and confirm system requirements

The Contractor shall be fully and solely responsible for all design and build works, including but not limited to any reconfiguration, modification, integration, migration, or optimisation of the existing infrastructure environment, whether expressly stated or implied under this Agreement.

The Contractor shall adopt a structured, phased implementation methodology to ensure minimal disruption to academic and administrative services while maintaining network security integrity.

The implementation shall be designed to complement the existing perimeter firewall infrastructure, forming a layered security architecture that enhances visibility, control, and threat prevention within the internal network.

All deployment activities shall follow industry best practices, change-management principles, and the Institution's internal IT governance policies.

The firewall solution shall be deployed as a second-tier security layer, positioned logically behind the perimeter firewall to provide:

- Deep application-level inspection
- User-centric policy enforcement
- Advanced threat detection within internal and east-west traffic

The solution shall support deployment in:

- Layer 3 (routed) mode
- Layer 2 (transparent) mode
- Virtual wire or equivalent modes

allowing flexibility to align with the Institution's existing network design.

The architecture shall support future scalability, including additional segments, campuses, or remote learning infrastructure.
The Contractor shall implement security policies based on application, user identity, and security risk, rather than solely on IP address or port.

Initial policies shall be developed using a progressive enforcement approach, including:

- Visibility and monitoring mode
- Alert-only or partial enforcement
- Full enforcement after validation

Policies shall be aligned with the Institution's:

- Acceptable Use Policy

- Data protection and privacy requirements
- Educational content access guidelines

The firewall shall be integrated with existing directory and identity services to enable user- and group-based policy enforcement.
Integration shall support:

- Academic staff
- Administrative staff
- Students
- Guest or temporary users

Where required, the firewall solution shall be deployed in a high-availability configuration to ensure service continuity.

High-availability implementation shall include:

- State synchronisation
- Automatic failover
- Link and device health monitoring

The implementation shall be tested to verify seamless failover with minimal impact to active sessions.

Testing

Prior to production cut-over, the Contractor shall conduct comprehensive testing, including:

1. Connectivity and routing validation
2. Application identification accuracy
3. Security policy enforcement
4. Threat prevention effectiveness

Testing shall be performed during agreed maintenance windows to minimise disruption to teaching and learning activities.

A formal User Acceptance Testing (UAT) process shall be conducted, with documented sign-off from the Institution.

Documentation and Knowledge Transfer

The Contractor shall provide complete implementation documentation, including:

- Network and security architecture diagrams
- Configuration summaries
- Policy design rationale
- Operational procedures

Knowledge transfer sessions shall be conducted for the Institution’s IT staff, covering:

- Day-to-day operation
- Policy management
- Monitoring and troubleshooting

Maintenance and Support
Post-Deployment Support: Offer support and maintenance after the equipment goes live.

System Updates and Adjustments: Make necessary system updates and configuration adjustments based on feedback within the equipment valid life time.

Issue Response (7*24*4): Provide phone or online support within 10 minutes for any faults or assistance requests. If unresolved, on-site support should be provided within 4 hours.

Data Security and Compliance
Compliance with Regulations: Ensure the system adheres to all relevant data protection and privacy regulations.
Security Measures: Implement security measures to protect data from unauthorized access.

香港珠海學院
HONG KONG
CHU HAI COLLEGE

CONFIDENTIAL
TEND/HKCHC/AS/2026

SECTION FOUR: AGREEMENT OF CORE SWITCH AND FIREWALL INFORMATION INNOVATION REPLACEMENT PROJECT

Only the main terms of the agreement (contract type, buyer, supplier, contract period, project content and price, payment method) are specified here, and the specific contract content will be negotiated separately by both parties.

This agreement is entered into on the date outlined in Part 4 hereto (the "Effective Date"), by and between the party outlined in Part 2 hereto (the "Purchaser") and the party outlined in Part 3 hereto (the "Vendor") in the following Property according to the Terms and Conditions mentioned hereinafter:

Part 1 – Type of Agreement

Second Tier Firewall for Network Security Optimization Project for Hong Kong Chu Hai College Limited

Part 2 – The Purchaser

Hong Kong Chu Hai College Limited, a company with a principal place of business at Hong Kong Chu Hai College, 80 Castle Peak Road, Castle Peak Bay, Tuen Mun, New Territories, Hong Kong

Part 3 – The Vendor

Company Name	:	_____
Contact Person	:	_____
Contact No.	:	_____
Business Registration Certificate No.	:	_____
BR Date of Expiry	:	_____
Registered Address	:	_____
		_____

Part 4 – Agreement Period (Effective Date)

Thirty-six (36) months commencing from project kick start.

Part 5 – Services Charges

The brief description given hereunder is to be read in conjunction with the whole Tender and Agreement document.

Item	Description of item	Price
1.		HK$
2.		HK$
3.		HK$
4.		HK$
5.		HK$
	Total Contract Sum	**HK$**

Part 6 – Payment Term

The Vendor shall submit to the Company ("Hong Kong Chu Hai College Limited") an original invoice upon order confirmation. The settlement of payment will only be proceeded by the Company upon the receipt of the original invoice.

Payment Methods

1. 40% Payment upon Acceptance of Delivered Equipment: Upon the arrival and acceptance inspection of the required equipment, meeting the specified standards, and after being audited and approved, 40% of the total contract amount will be paid.

2. 40% Payment after Final Project Acceptance and Going Live: Once the project completes all stages of acceptance and all functions meet the predetermined requirements, 40% of the total contract amount will be paid after the project acceptance and goes live.

3. 20% Stable Operation Fee after Two Months of Steady Running Post-Launch: The final stable operation fee, accounting for 20% of the total contract amount, will be paid after the project has been launched and has been running stably for two months.

SECTION FIVE: TENDER EVALUATION

The following evaluation system applies to all bids:

Criteria	**Percentage**
- Price	60%
- Technical Solution	30%
- After Sales Service and Support	5%
- High Education Project Experience	5%
Total	100%

SECTION SIX: TERMS AND CONDITIONS OF AGREEMENT

In consideration of the mutual promises in the Agreement including these Terms and Conditions ("this Agreement"), the Vendor and the Purchaser agree as follows:

1 Confidential Information

1.1 Neither Party shall disclose to any third party any Confidential Information of the other Party, or use the other Party's Confidential Information except in the proper performance of its obligations under this Agreement (or, in the case of Purchaser, its use of the Services performed under this Agreement). "Confidential Information" means any information that relates in any way whatsoever to any research, development, trade secrets, customers, technology, systems, proprietary products, or business affairs of a Party, but does not include information which (a) is at the time of its disclosure publicly known. or (b) was rightfully known by the receiving Party at the time of disclosure. or (c) is lawfully received from a third party not bound by any confidentiality obligations to the owner of such Confidential Information. Each Party will share the other Party's Confidential Information on a "need to know" basis and must give its personnel (including but not limited to employees, officers, agents, and contractors) notice of the confidentiality obligations in this Agreement and the requirement to be bound by them. If there is a breach or threatened breach of this Section, remedies at law may be inadequate and the injured Party will have the right, without proof of special damages (in addition to its other legal rights) to seek an injunction or other equitable relief to enforce this Section.

1.2 Vendor may only disclose Purchaser's Confidential Information to the Vendor's Personnel who are directly involved in the provision of the Services and who need to know the information. Vendor shall ensure that such Vendor's Personnel are aware of, and comply with, the confidentiality obligations in this Agreement.

1.3 Vendor shall not and shall procure that Vendor's Personnel do not, use any of Purchaser's Confidential Information received otherwise than for this Agreement.

1.4 Vendor shall notify Purchaser immediately upon discovery of any unauthorized use or disclosure of Confidential Information, or any other breach of this Section 16 by Vendor, and shall cooperate with Purchaser in every reasonable way to help Purchaser regain possession of the Confidential Information and prevent its further unauthorized use or disclosure.

1.5 Upon the expiry or termination of this Agreement or at Purchaser's request, whichever is the earlier, Vendor shall forthwith return to Purchaser (or at Purchaser's option, destroy and certify the destruction of) all originals, copies, reproductions, notes, summaries, and extracts of, containing or relating to Confidential Information which are in Vendor's possession, custody or control.

1.6 All Confidential Information is and shall remain the property of Purchaser. By disclosing Confidential Information to Vendor, Purchaser does not grant any express or implied right to Vendor to or under any of Purchaser's patents, copyrights, design rights, trademarks, trade secrets, or other intellectual property or other proprietary rights.

1.7 The provisions of this Clause 1 shall survive the expiry or termination of this Agreement.

2 Intellectual Property Rights

Subject to Clauses 2.3 and 2.4:

2.1 Purchaser shall not acquire any right, title, or interest in or to the Intellectual Property Rights of Vendor or its licensors, including:

a) the Intellectual Property Rights relating to the Vendor's Software.

b) the Intellectual Property Rights relating to the Third Party Software. and

c) Vendor's Background Intellectual Property Rights.

2.2 Vendor shall not acquire any right, title, or interest in or to the Intellectual Property Rights of Purchaser or its licensors, including:

a) the Intellectual Property Rights relating to the Purchaser's Software.

b) the Intellectual Property Rights relating to the Purchaser's documentation, processes, and procedures.

c) the Intellectual Property Rights relating to the Purchaser's know-how.

d) the Intellectual Property Rights relating to the Purchaser's Data.

e) the Intellectual Property Rights relating to the Database.

f) Purchaser’s Background Intellectual Property Rights. and

g) the Intellectual Property Rights relating to the Work Product.

2.3 Where either party acquires, by operation of law, title to Intellectual Property Rights of the other referred to in Clauses 2.1 or 2.2, and such acquisition is inconsistent with the allocation of title set out in Clauses 2.1 or 2.2, such Intellectual Property Rights shall be assigned by it to the other party on the request of the other party, whenever that request is made.

2.4 Purchaser hereby grants to Vendor a royalty-free, non-exclusive, non-transferable license during the term of this Agreement to use:

a) the Purchaser's Software.

b) the Purchaser's documentation, processes, and procedures. and

c) the Purchaser's Data and the Database, including the right to grant sub-licenses to its Sub-Contractors, provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with Vendor in a form reasonably acceptable to Purchaser.

2.5 The license granted in Clause 2.4 is granted solely to the extent necessary for performing the Services by this Agreement. The vendor shall not use such licensed materials ("Purchaser Materials") for any other purpose. Vendor will not, and will not permit any Vendor's Personnel to use any Purchaser Materials for the benefit of any person or entity other than Purchaser without the prior written approval of Purchaser, which may be withheld at Purchaser's sole discretion.

2.6 In the event of the termination or expiry of this Agreement, the licenses referred to in Section 2.4 shall terminate automatically and Vendor shall deliver to Purchaser all Purchaser Materials licensed to Vendor under Clause 2.5 in its possession or control.

3 Publicity

Vendor must not use the name, trademarks, service marks, logos, domain names, Websites, or any other identifiers of Purchaser or any of Purchaser's Affiliates in any way without prior written approval of Purchaser.

4 Entire Agreement

This Agreement is the entire agreement between the Parties concerning the subject matter of this Agreement. The appendix and schedules attached to or referred to in this Agreement are incorporated by reference. If there is a conflict between these Terms and Conditions and any Schedule, the provisions of these Terms and Conditions (as they may be amended by mutual agreement of the Parties) will prevail. No change or amendment to this Agreement will be valid unless it is in writing and signed by an authorized representative of both Parties.

5 Governing Law

This Agreement shall be construed by the laws of Hong Kong and both Parties agree to submit to the non-exclusive jurisdiction of the courts of Hong Kong.

6 Time is of the Essence

The vendor acknowledges that time is of the essence concerning the performance of its obligations hereunder.

7 No Waiver

The failure of either Party to insist upon or enforce strict performance by the other Party of any part of this Agreement or to enforce any right under this Agreement shall not be construed as a waiver or a relinquishment of such Party's right to assert or rely upon such provision or any other provision of this Agreement.

8 Counterparts and Electronic Signatures

This Agreement, and all agreements executed hereunder, may be executed in counterparts, with the same effect as if the Parties had signed the same document. Each counterpart so executed shall be deemed to be an original, and all such counterparts shall be construed together and shall constitute one Agreement. The counterparts of this Agreement and any agreement executed hereunder may be executed and delivered by facsimile or other electronic signature by any of the Parties to any other Party and the receiving Party may rely on the receipt of such document so executed and delivered by facsimile or other electronic means as if the original had been received.

9 Conditions Affecting the Maintenance Services

The Vendor shall satisfy himself as to the nature of the systems and their general location within the site. Any failure on the part of the Vendor to obtain reliable information as to the conditions under which the maintenance services are to be carried out shall not relieve him from any risks or responsibility for the performance of his obligation under this Agreement.

10 Compliance with laws

10.1 The Parties hereto mutually agree, for themselves and their employees, agents, and intermediaries, that they will not pay, and will not permit or suffer any agent, intermediary, or employee to pay, directly or indirectly, any money or thing of value, to any official of the government of any nation or political subdivision thereof, or any of their agencies, instrumentalities, corporations or ventures, or any political party, official thereof, or any candidate, to influence the acts, omissions or decisions, in an official capacity, of such official, party or candidate in violation of his/her or its lawful duty or inducing him or it to exercise his/her or its influence to affect or influence any act or decision of such government or instrumentality or to obtain or retain business for Vendor or Purchaser.

10.2 Moreover, before making payment of any money or thing of value on behalf of,

or with funds directly or indirectly received from Vendor or Purchaser, the Parties hereto will make such inquiry as the circumstances may indicate is prudent into whether the immediate recipient and any ultimate recipient or beneficiary of such payment may have any official status with the government of any nation or political subdivision thereof, or any of their agencies, instrumentalities, corporations or ventures, or with any political party, official thereof, or any candidate for political office.

10.3 Should either Party become aware of a possible violation of Section 10.1 and/or 10.2, or of the facts and circumstances from which a prudent person could conclude that further inquiry is necessary to determine whether such a violation has occurred, is occurring or is likely to occur, such Party will give representatives designated by the other Party immediate notice of such violation, facts or circumstances, and will cooperate fully, and direct all agents, employees and other person(s) the other Party may retain or direct in connection herewith, to cooperate fully, with any inquiry or investigation the other Party may conduct.

11 Exclusion of Rights

Notwithstanding any other provisions of this Agreement, a person who is not a party to this Agreement shall not have any right under the Contracts (Rights of Third Parties) Ordinance to enforce any provisions of this Agreement. This does not affect any right or remedy of such third party which exists or is available apart from that Ordinance.

12 Disputes

This agreement and the rights and obligations of the parties hereunder shall be governed by the construed in all respects by the laws of Hong Kong Special Administrative Region and the parties hereto submit to the non-exclusive jurisdiction of the Hong Kong Courts.