Partnership Programme for

Cyber Security Information Sharing

Terms and Conditions

July 2024

PARTNERSHIP PROGRAMME FOR

CYBER SECURITY INFORMATION SHARING

TERMS AND CONDITIONS

These terms and conditions are the primary means by which information sharing, handling, confidentiality, liability and acceptable behaviour are established and managed by the Programme Management Committee.

These terms and conditions govern the exchange of cyber security information among the companies, organisations and legal entities who become members ("Members") of the Partnership Programme for Cyber Security Information Sharing – "Cybersec Infohub" (the "Programme").

By accessing Cybersechub.hk, the technical platform that enables sharing of cyber security information and collaboration in the Programme, you are indicating that you are a Representative as defined below and are acting on behalf of a Member of the Programme who agrees to comply with these terms and conditions.

1. OBJECTIVES

1.1 The objectives of the Partnership Programme for Cyber Security Information Sharing – "Cybersec Infohub" (the "Programme") are to:

1.1.1 establish a cross-sector, trusted collaborative network to share cyber security information;

1.1.2 provide a collaborative platform for sharing information to give a better visibility of cyber security situational awareness;

1.1.3 cultivate local collaborative culture among the industry for effective cyber security information sharing; and

1.1.4 enhance the overall cyber resilience of Hong Kong against territory-wide cyber attacks.

1.2 These terms and conditions aim to implement the Programme in an effective way through a highly participative, fair, open and transparent process in pursuit of the objectives of the Programme (the "Objectives").

2. SCOPE

2.1 These terms and conditions apply to any information (of whatever nature and whatever form or format) that is exchanged and shared among Members of the Programme and includes information which is received in writing, electronically or orally from or pursuant to discussions among Members.

3. DEFINITIONS

In these terms and conditions, the following definitions apply:

3.1 "**Anonymous Posting Facility**" is a function provided for Members to post cyber security information or responses on Cybersechub.hk without disclosing the identity of the Originator.

3.2 "**Cybersechub.hk**" is a uniquely hosted technical platform that enables online relationships and connections among Members (acting by Representatives) for sharing cyber security information, such as cyber threats and vulnerabilities. Cybersechub.hk is operated based on the principle of trust, respect, openness and transparency among Members.

3.3 "**Group**" means a voluntary organisation of two or more Members who have a common interest in sharing Information with one another as a result of their organisation or industry background or any other shared interest in cyber security. Creation and administration of Groups are defined in Clauses 4.5 and 4.6 respectively.

3.4 "**Information**" means any information (of whatever nature and whatever form or format) that is exchanged and shared among Members of the Programme and includes information which is received in writing, electronically or orally from or pursuant to discussions among Members. Information can be observations related to cyber security, vulnerabilities, alerts, cyber threat indicators, attack actors or campaigns, mitigation measures, best practices, etc.

3.5 "**Information Sharing Boundaries**" means the application of privacy control measures on Information which detail how the Information shall be handled within Cybersechub.hk. The boundaries are defined in the Traffic Light Protocol ("TLP") in Clause 7.

3.6 "**Member**" means a company, organisation or legal entity that meets the criteria and requirements for membership contained in Clause 4.1, and its application for membership has been approved by the Programme Management Committee.

3.7 "**Objectives**" means the objectives of the Programme as listed in Clause 1.1.

3.8 "**Originator**" means the Member or its Representative(s) that first discloses any particular Information in the Programme, including via Cybersechub.hk.

3.9 "**Personal Data**" has the meaning given in the Personal Data (Privacy) Ordinance (Cap. 486) of the Laws of Hong Kong.

3.10 "**Programme**" means the Partnership Programme for Cyber Security Information Sharing – "Cybersec Infohub" which includes the technical platform "Cybersechub.hk" and other related activities such as face-to-face meeting, workshop, etc. to facilitate cyber security information sharing and collaboration among Members.

3.11 "**Programme Management Committee**" is responsible for formulating and executing the business plan and resourcing decisions in pursuit of the Objectives. It comprises representatives appointed by the Digital Policy Office and the Hong Kong Internet Registration Corporation Limited.

3.12 **"Programme Manager"** means the team designated by the Programme Management Committee to deliver the defined Programme outputs and assure smooth operations of the Service Desk.

3.13 "**Recipient**" means a Member or its Representative(s) that receives Information pursuant to these terms and conditions from an Originator directly or indirectly via another party. A Member is still a Recipient for the purposes of these terms and conditions even when the Information is received by a Representative who acts on behalf of that Member under a marking contained in Clause 7 that prevents disclosure to a wider extent than that is accepted by the boundary of the marking.

3.14 "**Representative**" means an authorised individual within a Member who has been provided with personal access to Cybersechub.hk and acts on behalf of the Member.

3.15 "**Service Desk**" means the team that provides helpdesk service and acts as the point of contact for all Members associated with the operation of the Programme. The Service Desk administers these terms and conditions and answers enquiries from Members.

4. MEMBERSHIP

4.1 Any Hong Kong company or organisation with its business address in Hong Kong, which owns a .hk Internet domain name and manages an electronic communications network and has operational needs for cyber security information, is eligible to become a Member provided that it confirms that it complies and is willing to continue to comply with these terms and conditions. In case of dispute, the decision will be made at the discretion of the Programme Management Committee.

4.2 Members must have appropriate measures in place to protect the confidentiality and integrity of any information received via the Programme.

4.3 Membership of the Programme is exclusive to the entity to whom it is granted and does not extend to any related or associated company. Companies that are a holding company or a subsidiary of a Member are required to apply separately for membership if they intend to participate in the Programme.

4.4 A Member can nominate one or more Representatives to join Cybersechub.hk. The Programme Management Committee reserves the right to determine the maximum number of Representatives for Members according to the operation of the Programme.

4.5 Members are able to join Groups on Cybersechub.hk. Groups are for facilitating communication among Members with common interests. Communication in a Group is accessible to the members of that Group only. A Member can suggest to the Service Desk the creation of a new group with justifications of the focus areas of the proposed group and the criteria of joining the group. The list of Groups and other related information of groups such as membership criteria and focus area, etc. can be searched on Cybersechub.hk.

4.6 A Group shall have at least two Representatives with one as the administrator of the Group. The Group operations and logistics, such as invitation, admission and removal of members, are managed by the Group administrator and are bound by these terms and conditions. Members can apply to the relevant Group administrator to join a particular Group.

4.7 Membership of Cybersechub.hk is dependent on participation. One condition of continued membership is that the Representative is using its account regularly.

4.7.1 After 30 calendar days of inactivity (defined as the Representative not logging in Cybersechub.hk), a notification email will be sent to the Representative, prompting a return to Cybersechub.hk.

4.7.2 If the inactivity continues for another 30 calendar days, a notification email will be sent to the Representative and the primary contact of the Member.

5. MEMBER RESPONSIBILITIES

5.1 A Representative put forward by a Member must:

5.1.1 have a role within the Member's organisation that their participation in the Programme promotes the Objectives;

5.1.2 consent to the processing of their Personal Data in accordance with Clause 13;

5.1.3 agree to comply with these terms and conditions; and

5.1.4 neither transfer the use of an account to another person, disclose the account credential to another person, nor use another person's account.

5.2 A Member must inform the Service Desk as soon as possible if it wishes to change its Representative(s) or their personal details, or if any Representative ceases to be an employee or a member of the organisation.

5.3 A Member shall only share information through Cybersechub.hk when the Member considers that sharing the information can further the Objectives. Members shall only use and disclose Information shared by other Members for the Objectives and in a manner consistent with the information sharing as in Clause 7.

5.4 Members shall ensure that their supply and receipt of Information through the Programme and their use and disclosure comply with any applicable legal obligation, including those contained in these terms and conditions.

5.5 Members shall stay on topics of discussion that are related to the Objectives.

5.6 Members shall not solicit or advertise a product or service in the Programme for any commercial gain for themselves, another Member or any third party.

5.7 Members shall not use Cybersechub.hk as a tool for recruitment, business lead generation, political lobbying or any other purposes not related to the Objectives.

5.8 Members shall respect other fellow Members and participants of the Programme. Members shall not use offensive, provocative, threatening, harassing, defamatory and other inappropriate languages in discussions. Members or Representatives reserve the right to request the Service Desk to remove such discussions. The Service Desk will remove that Information without prior notice and notify the Originator.

5.9 Members shall minimise the exposure of Personal Data and sensitive information related to Members' organisation(s) on Cybersechub.hk.

5.10 Members shall ensure that Information shared on Cybersechub.hk relates to cyber security, cyber threat indicators and mitigation measures. Members are advised not to publish sensitive information such as financial losses suffered by or other damages done to a named organisation.

5.11 Members shall endeavour to ensure that any Information shared on Cybersechub.hk is safe for sharing as stated in Clause 9.

5.12 Members shall endeavour to ensure that any Information shared on Cybersechub.hk is accurate. However, all Members understand and accept that the Information is provided in the Programme in good faith. The Originator excludes all liability as stated in Clause 14.2.

5.13 Members shall ensure that their profiles and the profiles of their Representatives on Cybersechub.hk are accurate and kept up-to-date.

5.14 Members shall ensure that their Representatives are fully conversant and comply with the requirements of these terms and conditions.

5.15 In the event that a Member's organisation is split up into two or more organisations, it is the responsibility of the Member to inform the Programme Management Committee through the Service Desk, so that details can be reviewed and amended accordingly and the new organisations can become Members if appropriate.

6. PRIVACY CONTROLS

6.1 Members are able to set privacy controls and Information Sharing Boundaries on the sharing of cyber security information within and outside Cybersechub.hk in accordance with the rules for information sharing in Clause 7.2.

6.2 Members shall not disclose other Members' Information except in accordance with the applicable Information Sharing Boundaries or with the prior written consent of the Originator.

6.3 Members are able to share Information within the Group(s) they belong to ensure that the shared information stays within the specific Group(s).

6.4 Members are able to use the Anonymous Posting Facility to hide their identities when sharing cyber security information or responding on Cybersechub.hk. This facility should be used sensibly because posting with real names is the best approach to build trust.

6.5 The identities of Members who respond to anonymous polling of Cybersechub.hk shall not be disclosed.

6.6 Members understand and accept that the Programme Management Committee, the Programme Manager and the Service Desk may collect and access the Personal Data of their Representatives. Such access to the Personal Data is strictly intended for performing their duty of work for maintenance, administration, support and statistical analysis purposes, subject to Clause 13.

7. INFORMATION SHARING

7.1 Members and their Representative(s) who post Information on Cybersechub.hk must use the Traffic Light Protocol ("TLP") set out below.

7.2 The Originator can assign one of the four Information Sharing Boundaries to a piece of Information shared within Cybersechub.hk. The Recipients of the Information shall not disclose the Information to a wider extent than that is accepted by the boundary to which the piece of Information is attached.

The four Information Sharing Boundaries are as follows:

Information Sharing Boundary		**How Information can be Shared**
TLP:RED	Not for disclosure, restricted to the Representatives that have been explicitly identified and named by the Originator	• The Originator may use TLP:RED when the Information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation or operations if misused. • Recipients may not share TLP:RED information with any parties outside Cybersechub.hk in which it was originally disclosed.
TLP:AMBER	Limited disclosure, restricted to the organisations of the Representatives	• The Originator may use TLP:AMBER when the Information requires support to be effectively acted upon, and yet carries risks to privacy, reputation or operations if shared outside the organisations involved. • Recipients may only share TLP:AMBER information with the staff members within the same Representative's organisation. • The Originator are at liberty to specify additional intended limits of the sharing.

Information Sharing Boundary		How Information can be Shared
TLP:GREEN	Limited disclosure, restricted to Cybersechub.hk	• The Originator may use TLP:GREEN when the Information is useful for the awareness of all Recipients as well as peers within Cybersechub.hk. • Recipients may share TLP:GREEN information with other Members within Cybersechub.hk, but not via publicly accessible channels. • TLP:GREEN information may not be released outside Cybersechub.hk.
TLP:WHITE	Disclosure is not limited	• The Originator may use TLP:WHITE when the Information carries minimal or no foreseeable risk of misuse in accordance with applicable rules and procedures for public release. • Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

7.3 If a piece of Information on Cybersechub.hk has not been attached to any Information Sharing Boundary, TLP:GREEN is assumed (by default).

7.4 Information marked as TLP:AMBER or TLP:GREEN may, additionally, be disclosed by a Member to its security service provider(s) provided and only to the extent that it is necessary for the Member to make such disclosure in order to improve its cyber security capability and the Originator does not explicitly disallow such disclosure.

7.5 Information posted within a specified Group is targeted at the Members of that Group(s) only and should not be released outside the Group unless agreed by the Originator.

7.6 The Originator's identity in anonymous postings and anonymous polling shall not be disclosed.

7.7 In any sharing or discussions in the Programme, be it online or offline, neither the identity or affiliation of the Originator of the Information nor that of any other participants may be revealed.

8. HANDLING CONFIDENTIALITY

8.1 In consideration of the Information being made available by an Originator, each Member hereby irrevocably undertakes with the Originator and with the other Members, both for itself and on behalf of its Representatives, that all personnel shall:

8.1.1 only use the Information for the Objectives;

8.1.2 not store in any medium, copy, reproduce or reduce to writing any material part of the Information except as may be reasonably necessary for the Objectives;

8.1.3 use the same care and discretion as it uses with its own proprietary information, but no less than reasonable care, to avoid disclosure, publication or dissemination otherwise than in accordance with these terms and conditions; and

8.1.4 ensure that their Representative(s) and security service provider(s) as stated in Clause 7.4, who are permitted to access the Information, are aware of the Information Sharing Boundary that the Originator has attached to it and comply with any confidentiality and non-disclosure obligations which apply.

8.2 Where a Member stores, copies or reproduces Information in accordance with Clause 8.1.2, the Member shall ensure that the copy or reproduction has the same Information Sharing Boundary as the original.

9. HANDLING CYBER THREAT INDICATORS

9.1 A cyber threat indicator means information that is able to describe or identify a variety of cyber threats and of which may include Indicators of Compromise (IOCs), malware samples, malicious code, malicious active content, etc. The Originator should redact fields / contents containing Personal Data or sensitive information that are not relevant to analysis, investigation or addressing threats. To ensure that Information on Cybersechub.hk would not infect the users' computers inadvertently, the Originator should exercise due diligence and apply proper safeguards to protect Members from possible malicious contents.

9.1.1 For malware samples and files with malicious active content, the Originator should use an alternate text format that is safe to share, for example, file hash of a malware sample, or a password protected zip file; and

9.1.2 for malicious Uniform Resource Locators (URLs), the Originator should add a bracket in front of and right after every dot as '[.]' of each URL to be shared as http://www[.]example[.]com.

9.2 If Members or Representatives discover that any Information on Cybersechub.hk contains malicious content without proper safeguards, they may notify the Service Desk immediately. The Service Desk would remove that Information with reference to Clause 9.1 above without any prior notice. The Originator of the Information shall then be notified.

10. DISCLOSURE

10.1 Non-Disclosure to Third Parties

10.1.1 Unless it is expressly permitted in these terms and conditions, no Member shall at any time without the relevant Originator's prior written consent disclose Information otherwise than:

10.1.1.1 in accordance with the applicable Information Sharing Boundary as stated in Clause 7; or

10.1.1.2 being required to do so by law or by the order or ruling of a court, a tribunal or a regulatory body.

10.1.2 Where disclosure is contemplated in accordance with Clause 10.1.1.2, the disclosing party shall to the extent allowed by law, notify the relevant Originator promptly in writing of such disclosure to allow the Originator to seek relief to prohibit or limit such disclosure or use of the disclosed Information and to mitigate any damage arising. In any event, the relevant Member shall only disclose such Information to the extent as necessary under the court order or other ruling.

10.2 Unintended Disclosure

10.2.1 In the event that Information is disclosed or used by a Member without authorisation, the Member shall notify the relevant Originator of the unauthorised use or disclosure promptly and take steps (including, in particular, any steps which the Originator reasonably requires the Member to take) to prohibit or limit further disclosure and unauthorised use of the disclosed Information and to mitigate any damage arising.

10.2.2 The obligation to notify the Originator of any unauthorised disclosure and to mitigate any damage arising from the unauthorised use or disclosure remains in effect regardless of the termination of any other rights and obligations under these terms and conditions.

11. FEEDBACK

11.1 Members shall be able to provide qualitative feedback on Information received from other Members. Any feedback made or provided by Members or Representatives shall be subject to the same limitations and exclusions of liability as set out in Clause 14.2.

12. INTELLECTUAL PROPERTY RIGHTS

12.1 The intellectual property rights, including copyright, of all information, data and materials published in any channel of the Programme remain with the Originator. The disclosure of Information by any Originator does not imply any kind of transfer of rights or grant of licence connected with the Information, including without limitation, any intellectual property rights, patent, copyright, trademark or trade secret.

12.2 Members shall not publish another person's copyrighted work without his/her written and express consent. Members shall not infringe or misappropriate another person's intellectual property rights.

12.3 The Recipient shall not remove any proprietary, patent, copyright, trademark, trade secret or other legend from any Information. The Recipient shall add to any Information any proprietary, patent, copyright, trademark, trade secret or other legend reasonably requested by the Originator in writing to protect its intellectual property rights of the Information.

13. DATA PROTECTION

13.1 The operation of the Programme shall comply with the Personal Data (Privacy) Ordinance (Cap. 486) of the Laws of Hong Kong.

13.1.1 Data Collection

13.1.1.1 The Programme Management Committee and the Programme Manager may collect any Personal Data provided by Members or Representatives that are necessary but not excessive for the Objectives of the Programme, such as:

- their contact information for maintaining communication with them;
- their organisation background and interests in cyber security for providing access to and administration of Cybersechub.hk;

- their Internet Protocol addresses when accessing Cybersechub.hk to support session maintenance and user experience;
- their preference settings in their profiles to support service provision;
- cookies to improve website experience; and
- other Personal Data that are strictly used for providing services for the Objectives and for administration, support and statistical analysis purposes.

13.1.1.2 The Service Desk may access Personal Data contained in:

- posts on Cybersechub.hk, including posts in Groups, posts using anonymous posting and responses to polling facilities, regardless of privacy controls and Information Sharing Boundaries;
- information of Members' personal profile, group membership; and
- any system log of activities of Representatives on Cybersechub.hk.

Such access permissions given to the Service Desk are limited to the minimum amount necessary to enable effective administration and are subject to audit.

13.1.2 Accuracy and Retention

13.1.2.1 The Service Desk shall take reasonable steps to ensure the Personal Data are accurate and kept up-to-date, and not kept longer than necessary in the Programme. In the event that a Member terminates its membership or a Representative ceases to act on behalf of a Member, the Service Desk shall delete all and any Personal Data from the database upon receiving notification from the Member.

13.1.3 Data Use

13.1.3.1 Personal Data may not be used by the Service Desk, service contractors of the Programme, or any Member other than purposes under these terms and conditions. Any Personal Data of the Member or Representative shall be used for the directly related purposes specified in Clause 13.1.1, unless voluntary and explicit consent with a new purpose is obtained from the Member or Representative.

13.1.4 Data Security

13.1.4.1 Personal Data collected, no matter electronically or physically, shall be stored in a safe repository where unauthorised people cannot access. Personal Data shall be encrypted if they are to be transported out of the physical premise or logical network.

13.1.4.2 The Cybersechub.hk platform shall use industry standard encryption technology to protect Personal Data in motion from being sniffed or contaminated.

13.1.4.3 As for Personal Data on papers, the papers shall be shredded and disposed of securely. All electronic data will be sanitised in a manner consistent with industry standard prior to disposal.

13.1.5 Openness

13.1.5.1 Members and Representatives are informed of the purpose and who will use or access the Personal Data under these terms and conditions. The Service Desk is the contact point for information request about the type of Personal Data the Programme holds and the purpose of use.

13.1.6 Data Access and Correction

13.1.6.1 The Service Desk shall comply with requests from Members to access, update, correct or delete any Personal Data it holds.

14. DISCLAIMERS

14.1 Disclaimer of Endorsement

14.1.1 Any reference to any specific commercial or non-commercial product, process or service by trade name, trademark, manufacturer or otherwise via Cybersechub.hk or any other communication channel of the Programme does not constitute or imply an endorsement or recommendation. The views and opinions of the Programme Management Committee (including its members), the Programme Manager, the Service Desk, Members or Representatives shall not be used for promotion or endorsement purposes.

14.2 Disclaimer of Liability

14.2.1 Members and Representatives shall make their own judgement as regards the use of any Information obtained from the Programme.

14.2.2 Neither the Programme Management Committee (including its members), the Programme Manager, the Service Desk, Members nor Representatives make any warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, or assume any legal liability for the accuracy, completeness or usefulness of any Information, communications, languages, statements, comments, articles, publication or hyperlinks in the Programme.

14.2.3 To the maximum extent permitted by law, the Programme Management Committee (including its members), the Programme Manager, the Service Desk, Members or Representatives accept no liability for any direct, indirect or consequential loss or damage under these terms and conditions, whether arising in tort, contract or otherwise, including without limitation, any loss of profits or anticipated profits, data, business goodwill, income, revenue or anticipated savings and damage to reputation, incurred by any person and howsoever caused arising from or connected with the operation of the Programme in accordance with these terms and conditions, and including loss and damage caused by any error or omission in Information provided through or in connection with the Programme or from any person acting, omitting to act or refraining from acting upon or otherwise using the Information provided through the Programme.

15. PUBLICITY

15.1 These terms and conditions, and the membership of the Programme are considered as TLP:WHITE as set out in Clause 7. Members can freely disclose that they are part of the Programme.

15.2 Each Member agrees that it shall not use the name or logo of the Programme, Cybersechub.hk, or any other Member without explicit consent, or advertise or otherwise publicise the identity of any other Member or Representative of the Programme without prior written consent.

16. NOTICES AND SERVICE AVAILABILITY

16.1 Any notice or other communication to be given under these terms and conditions must be in writing and sent to the Service Desk at admin@Cybersechub.hk.

16.2 Any notice shall be deemed as served at the time the email is transmitted unless a transmission error message is received.

16.3 The Service Desk reserves the right to modify, suspend or terminate the operation of or access to Cybersechub.hk; to modify or change Cybersechub.hk; and to interrupt the operation of Cybersechub.hk as necessary to perform routine or non-routine maintenance, error correction or other changes.

17. ASSIGNMENT

17.1 Members shall not assign, sub-license, transfer or otherwise dispose their rights or obligations under these terms and conditions in whole or in part at any time without the prior written consent of the Programme Management Committee.

18. WAIVER

18.1 No failure or delay by a Member to enforce any of its rights under these terms and conditions shall waive its rights. No single or partial exercise of any rights will preclude any further exercise of such rights. Any waiver must be given in writing and signed by the parties for granting it to be effective.

19. SEVERANCE

19.1 If any clause in these terms and conditions is, or is found to be, unenforceable in whole or in part, the remaining provisions or parts shall continue to be enforceable.

20. ENTIRE AGREEMENT

20.1 These terms and conditions shall constitute the entire agreement among the Members concerning the Objectives and supersede all previous arrangements, commitments, understandings and agreements among the Members concerning the subject matter hereof. Nothing in these terms and conditions shall act to exclude or limit any Member's liability to any other Member with respect to any fraudulent misrepresentations.

21. RIGHTS OF THIRD PARTIES

21.1 Any person who is not a party to these terms and conditions shall not have any rights to enforce any provision of these terms and conditions.

22. RELATIONSHIP OF THE MEMBERS

22.1 Nothing in these terms and conditions shall constitute or be deemed to constitute any form of employment, partnership, joint venture, agency or other business entity among the Members; nor shall any employees, legal partners or agents of one Member be deemed as the servants, legal partners or agents of any other Member.

23. COMPLIANCE

23.1 The Programme Management Committee can investigate or appoint a party to investigate any suspected violation of these terms and conditions. The Programme Management Committee would take reasonable action(s) to mitigate any violation to strike a balance between encouragement of participation and discipline, including but not limited to written warning, restriction of access, suspension or termination of an account.

24. TERMINATION

24.1 These terms and conditions shall continue to apply until a Member terminates its membership by a written notice of no less than ten (10) calendar days to the Service Desk, or the Service Desk needs to enforce compliance according to Clause 23. The Service Desk shall promptly inform all remaining Representatives if any membership is terminated.

24.2 Notwithstanding a termination of membership in accordance with Clause 24.1, the rights and obligations with respect to the disclosure and use of the Information shall remain in effect for a period of six (6) months from the date of termination unless, for a specific piece of Information, a longer period is expressly specified by the Member.

25. VARIATION

25.1 The Programme Management Committee may vary these terms and conditions from time to time by providing a written notice to all Members with a hyperlink to the amended terms and conditions. The new amendments will take effect ten (10) calendar days after Members are notified of the amendments.

26. GOVERNING LAW

26.1 These terms and conditions are governed by the laws of the Hong Kong Special Administrative Region and subject to the exclusive jurisdiction of the Hong Kong courts.