資訊安全政策
Policy on Information Security

目的 Objective
為確保電腦系統和數據安全，管理資訊科技資源和通信系統，協會需制定政策和程序以保護電腦檔案、電子郵件及用來儲存、傳輸和處理資訊的任何其他形式。
To ensure the security of computer systems and data and better manage the IT resources and communication system, policies and procedures are formulated to safeguard for the use of computer files, emails and any other forms used to store, transmit and process information.

本政策適用於所有執行委員、委員會成員、職員（包括短期合約和非全職職員）無論其僱傭條款如何，即包括短期合約員工，兼職員工、會員、運動員、教練以及裁判員等。
It applies to all Executive Committee members, Committee Members, and staff irrespective of their terms of employment, i.e., including short-term contract or part-time staff, members, athletes, coaches, and umpires.

紀律 Discipline
- 禁止從事任何違法活動：
  The following activities shall not be conducted:
  - 未獲授權下取用電腦資料 Accessing computers without authorization；
  - 有犯罪或不誠實的意圖使用電腦 Accessing computer with criminal or dishonest intent；
  - 刑事毀損如破壞網頁或傳播電腦病毒 Criminal damage such as destroying webpages or spreading computer viruses；
  - 未經授權使用網絡資源 Accessing network resources without authorization；
  - 破解、竊取或者盜用他人賬號和密碼 Cracking, stealing or misappropriating other people's accounts and passwords；和 and
  - 在沒有正當理由的情況下披露他人的帳戶和密碼 Disclosing other people's accounts and passwords without proper reasons。
- 禁止存取或下載色情資料。
  Accessing or downloading pornographic materials is strictly prohibited.
- 禁止製作、存取、下載或轉發辱罵、不道德、歧視性或冒犯他人的資料，或發 表任何可能使協會成員或任何第三方受辱或感到尷尬的低俗言論、建議或評論。
  It is prohibited to produce, access, download or forward offensive, immoral, discriminatory or insulting data, or to make any vulgar remarks, suggestions or

comments that may embarrass or humiliate members of the Association or any third party.

- 協會的資源和工作時間是為協會的運作預留的。不可透過使用聊天室、玩遊戲或類似行為，浪費工作時間和資源及瀏覽非公務用途網站，以避免內部網絡擠塞。

  The Association's resources and time at work are reserved for the operation of the Association. Using computer for any private or commercial purposes, such as accessing chat rooms, playing games or similar activities during working hours is not allowed. Browsing non-business-related websites should be minimized to prevent internal bandwidth congestion.
- 禁止在網絡上或他人電腦中散布電腦病毒及其他干擾或破壞系統機能之程式。

  Spreading computer viruses and other interference or destruction programmes on the Internet or on other people's computers are not allowed.
- 不建議使用 P2P 傳輸軟體來分享和下載檔案。

  Use of P2P transmission software to share and download files is not recommended.
- 除非經過電腦病毒及惡性程式碼檢查及清除所有的感染，否則不得使用來歷不明的外來儲存媒體（如 USB 記憶體）和檔案。

  External storage media (e.g., USB) and files from unknown sources must not be used unless they have been checked and cleared of all virus and malicious code infections.
- 未經適當授權，在使用網際網絡時不得下載或執行任何程式或軟體。

  Do not download or execute any programmes or software when using the Internet unless approved by responsible person.
- 未經適當授權，不得將任何與協會有關的資訊上載到外部網站。

  Do not upload any information related to the Association to external website without proper authorization.

<u>安全與保護 Security and Protection</u>

- 所有桌面電腦和手提電腦都應訂定帳號密碼，更換密碼時設置如下：

  All desktops and laptops should be set up with an account password. Rules of password setting are suggested as follows:
  - 密碼長度應至少 8 個字元及至少包括一個大寫字母、一個小寫字母、數字和一個特殊字符/符號 Length of the password shall be at least 8 characters long. It should include at least one upper case, one lower case letter, number and a special character/symbol；
  - 更改後的密碼不得與以前的密碼相同 The changed password must not be the same as the previous one；
  - 避免使用容易被破解的密碼（如姓名首字母、生日）或常用詞（如 password、qwerty） Avoid using password that are easy to be decrypted (e.g., initials, birthdays), or common words (e.g., password, qwerty)；和 and

- 避免在鍵盤上使用一系列連續的字母或使用重複的字母或數字 Avoid using a series of consecutive letters on keyboard or using repeated letters or numbers。

- 切勿將您的裝置連接至不可靠或來歷不明的無線網絡。
  Do not connect your office device to unreliable or unknown wireless network.
- 所有職員要妥善保管所有行動裝置設備（筆記型電腦或手機等），尤其是在外出的時候，要隨身攜帶。但是如果設備無人看管時，要確保不易被竊。
  All staff should take proper care of their office devices, such as desktops, laptops and mobiles, etc., especially when travelling. In case where the device is unattended, device owner shall use proper security tool (e.g., a laptop security lock) to keep it safe.
- 協會將通過安裝防病毒和防火牆系統，確保資訊系統免受威脅。如果懷疑電腦受到病毒感染，用戶必須立即停止使用該電腦並向 IT 同事報告。
  The Association shall ensure information system is protected from threats by installing Anti-virus and Firewall Systems. If a computer virus infection is suspected, the user must stop using the computer immediately and report the issue to the IT staff.
- 協會將定期進行安全風險評估和內部合規審計，包括對資訊系統更新、漏洞修復、修補程式安裝、權限管理和安全配置的檢討，以識別潛在的安全漏洞並尋求解決方案。
  The Association shall conduct regular security risk assessments and internal compliance audit, including reviews on information system updated, vulnerabilities repairs, patch installations, authority management and security configurations, to identify potential security breaches and seek resolutions.
- 電腦附近請勿放置茶水、飲料、細小文具用品等物品，以免造成電腦設備損壞。
  Do not place items such as drinks and small stationery near the computer so as to minimize the risk of damaging the device.
- 用戶應使用訪問密碼等安全工具，以保護電腦終端機和桌上電腦的安全。
  User should keep the office device safe by using security tools such as an access password.
- 應在離開工作場所之前採取關閉電腦的做法，電腦關機應依正常程序操作。
  The practice of switching off the computer before leaving the workplace should be adopted.
- 請勿任意拆卸或加裝任何電腦設備。
  Do not disassemble or modify any office device.
- 一旦發現設備或資訊遺失或被竊，應立即通報。
  A report should promptly be made if the device or data is lost, stolen and crashed.
- 注意釣魚郵件。請勿存取任何可疑連結或提取可疑附件，應適時清除並向相關 IT 同事報告，不要蓄意或惡意地回寄或轉寄這些郵件。

Be aware of phishing emails. Do not access any suspicious links or extract suspicious attachments. Do not forward or reply to suspicious emails but timely delete them and report to the IT staff.

- 通訊賬戶只能供授權人員使用，不允許任何形式的賬戶共享。
  The communication account shall only be available to the authorized person and any form of account sharing is not allowed.

備份和存檔 Backup and Archive

- 用戶應定期對與工作相關的資料和資訊進行備份。
  Users shall perform regular back-up on work-related data and information.
- 機密或敏感檔案資料建議進行實體隔離，或與外部網絡隔離。
  Confidential or sensitive data should be physically isolated, in particular, from external networks.
- 協會在備份敏感和機密資訊/資料時，應啓用加密選項（如有）。
  The Association shall enable encryption options (if any) when backing up sensitive and confidential information/data.

版權 Copyrights

只有遵從相應的軟體授權協議的軟體才能安裝到辦公設備上。

Only licensed software can be installed to office's device in compliance with license agreement.

緊急情況 Emergency

遇上任何資訊保安事故時，應立即向 IT 同事尋求即時協助。

Any information security incident shall be reported immediately to the IT staff for prompt assistance.

培訓 Training

協會將確保所有職員都了解本政策所載列的要求，並適時安排簡報會或培訓，以提高職員資訊安全的意識。

The Association should ensure that all staff are apprised of the requirements outlined in these policies and arrange briefings/training to enhance their awareness on information security.

檢討及修訂 Review and Revision

本政策及有關措施的內容，將適時進行檢討及修訂。

The Association will review and, where necessary, revise this Policy and the related measures from time to time to ensure their effectiveness and compliance with prevailing legislation, regulatory requirements and best practices.

訂立日期 Effective Date：22/9/2026
修訂日期 Last Updated：-