中國香港殘疾人奧委會
CHINA HONG KONG
PARALYMPIC COMMITTEE

Guidelines and Procedures on IT and Information Security

資訊科技及信息安全指引和程序

(12 December 2024 version)

Table of Contents 內容

1. Purpose 目的

This Information Technology (IT) Policy aims to establish guidelines for the proper use, management, and security of IT resources within the China Hong Kong Paralympic Committee Limited (HKPC). The policy ensures the security of computer systems and data, and to manage IT resources and communication systems, the HKPC shall establish guidelines and procedures to protect computer files, emails, and any other forms used for storing, transmitting, and processing information. 本資訊科技政策旨在制定指引，以妥善使用、管理和保障中國香港殘疾人奧委會有限公司（本會）的資訊科技資源。本政策確保電腦系統和數據的安全，並且為了管理資訊科技資源和通信系統，本會應制定指引和程序，以保護電腦檔案、電子郵件以及用於存儲、傳輸和處理信息的任何其他形式的資料。

2. Scope 範圍

These guidelines and procedures apply to all board members, committee members, Staff members (including those on short-term contracts and part-time staff), regardless of their terms of employment, as well as members, athletes, and coaches. who access or use HKPC's IT resources, including hardware, software, networks, and data. 本指引和程序適用於本會的所有董事、委員會成員、職員（包括短期合約及兼職職員），無論其僱傭條款如何，以及使用或接觸本會資訊科技資源（包括硬件、軟件、網絡及數據）的會員、運動員和教練。

3. IT Governance 資訊科技管治

3.1 Roles and Responsibilities 角色與責任

- **Administration Department**: 行政部門

  Responsible for implementing and maintaining IT systems, monitoring compliance, and addressing IT-related issues. 負責實施和維護資訊科技系統，監察合規情況，並處理與資訊科技相關的問題。

- **All Users**: 所有使用者

  Responsible for adhering to this policy and reporting any breaches or security concerns. 負責遵守本政策，並報告任何違規行為或安全問題。

3.2 Approval of IT Resources 資訊科技資源的批准

All IT resources, including hardware and software, must be approved by the Administration Department to ensure compatibility, security, and compliance with HKPC standards. 所有資訊科技資源，包括硬件和軟件，必須經由行政部門批准，以確保其與本會標準的兼容性、安全性及合規性。

4. Acceptable Use 使用範圍

4.1 Email Usage 電郵使用規範

This policy covers appropriate use of any email sent from a HKPC email address and applies to all Staff members, vendors, and agents operating on behalf of HKPC in order to prevent tarnishing the public image of HKPC. When email goes out from HKPC, the general public will tend to view that message as an official policy statement from the HKPC. 本政策規範所有由本會電郵地址發送的電郵之適當使用，並適用於所有代表本會運作的員工、供應商及代理，以防止損害本會的公眾形象。本會發出的電郵可能被公眾視為正式的政策聲明。

The HKPC email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Staff members who receive any emails with this content from any HKPC employee should report the matter to their Executive Director immediately. 本會的電郵系統不得用於創建或傳播任何具干擾性或冒犯性的訊息，包括對種族、性別、髮色、殘疾、年齡、性取向、色情、宗教信仰與實踐、政治觀點或國籍的冒犯性評論。如員工收到任何本會員工發送的此類內容電郵，應立即向其行政總監報告。

The HKPC email system shall be used for business purpose, Staff memberss are not encouraged to use the system to send private messages the association reserves the right to monitor messages whenever deem appropriate upon authorization of Executive Director. 本會的電郵系統應用於商務用途，員工不應鼓勵使用該系統發送私人訊息。本會保留在獲得行政總監授權時監控訊息的權利。

The HKPC webmail system allows Staff memberss to access their email outside office at internet browser, Staff memberss shall avoid using public computers to access their email, the login information shall not be saved at any computers and shall not disclose to any other parties. 本會的網頁電郵系統允許員工通過互聯網瀏覽器在辦公室外登入其電郵。員工應避免使用公共電腦登入其電郵做公務通訊，登錄資訊不得保存在任何電腦中，亦不得透露給任何其他人士。

Contents and traffic of emails are monitored as needed to ensure the proper functioning of email system without threats from spam or other types of emails of malicious nature. Access to emails at server level is only restricted to the Administration team members who possess the administrator right, while access to individuals' emails would only be processed under stringent check-and-balance, with proper audit trail logs and regular reporting to the Executive Director on such activities. Whenever considered necessary, the Executive Director can trigger surprise checking to access the system and check on the activity logs. 為確保電郵系統正常運行並避免來自垃圾郵件或其他惡意電郵的威脅，電郵內容和流量將根據需要進行監控。伺服器層級的電郵訪問僅限擁有管理員權限的行政團隊成員進行。對個人電郵的訪問僅在嚴格的監管機制下進行，並須有完整的審計記錄及定期向行政總監報告。在必要時，行政總監可授權進行突擊檢查以訪問系統和檢查活動記錄。

4.2 Internet Usage 互聯網使用

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within HKPC's network. These standards are designed to ensure Staff members use the Internet in a safe and responsible manner and ensure that employee web use can be monitored or researched during an incident. 本政策的目的是定義監控和限制來自本會網絡內任何主機的網絡使用的標準。這些標準旨在確保員工以安全和負責任的方式使用互聯網，並確保在事件發生時員工的網絡使用可以被監控或調查。

This policy applies to all end user-initiated communications between HKPC's network, Internet and WIFI, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy. 本政策適用於所有由最終用戶發起的通信，包括本會的網絡、互聯網和 WIFI 之間的網頁瀏覽、即時消息、文件傳輸、文件共享以及其他標準和專有協議。伺服器間通信，如 SMTP 流量、備份、自動數據傳輸或數據庫通信，均不包括在本政策範圍內。

The Administration Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Administration Department may access all reports and data if necessary to respond to a security incident. 行政部門應監控所有連接到公司網絡的電腦和設備的網絡使用。對於所有流量，監控系統必須記錄源 IP 地址、日期、時間、協議以及目標網站或伺服器。如果可能，系統應記錄發起流量的用戶 ID。行政部門在必要時可瀏覽所有報告和數據，以回應安全事件。

Administration Department shall monitor the Internet websites and protocols that are deemed inappropriate for the corporate environment of HKPC, the following protocols and categories of websites should be avoided: 行政部門應監控被認為不適合本會企業環境的網站和協議，應避免以下協議和網站類別:

- Adult/Sexually Explicit Material, betting / gambling, advertisements & Pop-Ups 成人/色情材料、賭博、廣告和彈出窗口
- Hacking, Illegal Drugs and Intimate Apparel 黑客、非法毒品和內衣
- Peer to Peer File Sharing, Personals and Dating 點對點文件共享、交友和約會
- SPAM, Phishing and Fraud, Spyware, Tasteless and Offensive Content 垃圾郵件、網絡釣魚和詐騙、間諜軟件、低俗和冒犯性內容
- Violence, Intolerance and Hate 暴力、不容忍和仇恨

The Administration Department shall periodically review and recommend changes to web and protocol filtering rules. The Executive Director shall review these recommendations and decide if any changes are to be made. 行政部門應定期審查並建議修改網站和協議過濾規則。執行董事應審查這些建議，並決定是否進行任何更改。

4.3 Computer Files 電腦文件

NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash. **切勿**打開來自未知、可疑或不可信來源的電子郵件附件或宏文件。立即刪除這些附件，然後通過清空垃圾桶進行“雙重刪除”。

- Delete spam, chain, and other junk email without forwarding 刪除垃圾郵件、鏈式郵件及其他垃圾郵件，勿轉發。
- Never download files from unknown or suspicious sources. 切勿從未知或可疑來源下載文件。
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so. 避免直接進行磁碟共享，並開啟讀寫權限，除非確有業務需求。
- Always scan media devices including disc and flash drive from an unknown source for viruses before using it. 在使用來自未知來源的媒體設備（包括光碟和隨身碟）之前，務必進行病毒掃描。
- Back-up critical data and system configurations on a regular basis and store the data in a safe place. 定期備份關鍵數據和系統配置，並將數據存儲在安全的地方。
- Take special attention to files which contains confidential or sensitive data, the use of access/read only password according to the need is highly recommended. 特別注意包含機密或敏感數據的文件。根據需要使用訪問/只讀密碼以保護資料是強烈建議的。

5. Security 安全

5.1 Data Protection 數據保護

HKPC reserves the ownership of files store in devices including website, server and laptops. 本會保留所有存儲在設備中的文件的所有權，包括網站、伺服器和筆記型電腦。

Staff memberss are not encouraged to copy files away from the office, consent should be obtained from respective Executive Director for any case of files copying. 員工不鼓勵將文件複製離開辦公室，任何複製文件的情況應取得相關行政總監的同意。

5.2 **Server 伺服器**

Staff memberss are encouraged to store their working files and data into the server instead of their personal computer in order to maintain the security and integrity of the data. 員工應將工作文件和數據存儲在伺服器中，而非個人電腦，以維護數據的安全性和完整性。

The share folder deployed at HKPC internal servers shall be owned by respective department and be responsible for data administration. 在本會內部伺服器上部署的共

享文件夾應由相關部門擁有，並負責數據管理。

The access right of the share folder shall be assigned to the respective departmental Staff memberss, consent of the respective department senior must be obtained if Staff memberss in other department request to access right other than their own department. 共享文件夾的訪問權限應分配給相關部門的員工，若其他部門員工要求訪問非自部門的權限，必須獲得該部門高層的同意。

The administration department shall perform periodic backup of the data inside the server. 行政部門應定期備份伺服器內的數據。

6. Software Management 軟件管理

The Policy is to manage its software assets to derive maximum benefit to the organization and its Staff members and, especially, to ensure that the organization and its Staff members acquire, reproduce, distribute, transmit, and use computer software in compliance with international treaty obligations and Hong Kong laws, maintain only legal software on HKPC computers and computer networks. 本政策旨在管理本會的軟件資產，最大限度地為本會及其員工帶來效益，特別是確保本會及其員工在遵守國際條約義務和香港法律的前提下獲取、複製、分發、傳輸及使用電腦軟件，並僅在本會的電腦及電腦網絡中維持合法軟件。

All software is protected under Hong Kong copyright laws from the time of its creation. HKPC has licensed copies of computer software from a variety of publishers to help fulfill its mission. Unless otherwise provided in the software license, duplication of copyrighted software, except for backup and archival purposes, is a violation of this Policy. 所有軟件自創建之日起均受香港版權法保護。本會已獲得多家出版商授權的電腦軟件副本，以幫助實現其使命。除非軟件許可證另有規定，否則除備份和存檔外，複製版權軟件違反本政策。

Staff members may not knowingly use software for which HKPC lacks the appropriate license. If parties become aware of the use or distribution of unauthorized software in this organization, notify the Executive Director. 員工不得故意使用本會未獲得適當許可的軟件。如果員工發現本會內部使用或分發未經授權的軟件，應通知行政總監。

Staff members may not loan or give to anyone any software licensed to this organization. 員工不得將本會授權的任何軟件借給或贈送給任何人。

The licenses for some of this organization's software permit Staff members of the organization to make a copy of the software for home use. The Executive Director may approve such use by Staff members that can demonstrate a need to conduct the organization's business from their homes. Under no circumstances, however, may an employee use the organization's software for purposes other than the business of this organization. 本會某些軟件的許可證允許員工將軟件副本用於家庭使用。執行董事可批准有需要在家中處理本會業務的員工使用該軟件。然而，在任何情況下，員工不得將本會軟件用於本會業務以外的目的。

No employee may use or distribute personally-owned software on the organization's computers or networks. Such software threatens the integrity and security of the organization's computers and networks. 任何員工不得在本會的電腦或網絡上使用或分發個人擁有的軟件。此類軟件會威脅到本會電腦和網絡的完整性及安全性。

A variety of software is available on the Internet. Some of this software, called "freeware" or "shareware," is available free of charge for limited use and may be downloaded to your computer with the prior written approval of your Executive Director. Other software available on the Internet and from other electronic sources, however, requires the user to obtain a license for its use, sometimes for a fee. No employee shall download such software to his or her computer without the prior written approval of the respective department senior. 網絡上有各種各樣的軟件。有些軟件稱為「免費軟件」或「共享軟件」，可以免費使用並可在獲得行政總監書面批准後下載到您的電腦上。然而，來自互聯網和其他電子來源的其他軟件，則需要用戶獲得使用許可證，有時還需付費。任何員工不得在未獲得相關部門行政總監書面批准的情況下，下載此類軟件到自己的電腦。

If there is any an uncertainty or enquiry about the nature of the software, please contact the Administration department for further assistance. 如果對軟件的性質有任何疑問或查詢，請聯繫行政部門以獲得進一步協助。

7. Hardware Management 硬件管理

Hardware refers to IT equipment including computers, monitors, printers and laptops. 硬件是指包括電腦、顯示器、打印機和筆記型電腦在內的 IT 設備。

Staff members should be using the equipment with good care, contact the Administration department if there is any defect or malfunction is found. 員工應妥善使

用設備，如發現任何故障或異常，應聯繫行政部門。

Several types of equipment is available for loan from Administration department, Staff members are reminded to clear any data on devices inside on loan equipment especially USB flash drives and laptop before returning, Administration department shall clear all the data inside the devices without prior notification. 行政部門提供多種設備借用，員工需在歸還借用設備前，清除設備內的所有數據，特別是 USB 隨身碟和筆記型電腦。行政部門將不事先通知而清除設備內的所有數據。

Procurement 採購

The cost incurred for the procurement of IT-related equipment shall be borne by the respective departments; it is strongly recommended that departments should include the consideration of related cost in their own budget. IT 相關設備的採購費用應由相應部門承擔；強烈建議部門在自身預算中考慮相關費用。

Staff shall send the requests for software and hardware to their respective department senior, where department Senior shall certify the request together with the budget details and send to the Administration department for procurement process. 員工應將軟件和硬件需求發送給其部門高層，部門高層應認證需求並附上預算詳情，然後將其發送至行政部門進行採購流程。

For non-budgeted items, Staff member shall send the request to their respective department senior where department senior shall send the request together with the reason for the procurement to the Administration department, the Administration department shall justify the request and seek approval from the Executive Director (with reference to the procurement policy) to make the procurement. 對於非預算項目，員工應將需求發送給其部門高層，部門高層應將需求及採購理由一同發送至行政部門。行政部門將對需求進行合理性審核，並根據採購政策向行政總監尋求批准進行採購。

7.2 Maintenance 維護

The Administration department shall be responsible for all the installation and maintenance of related equipment and software. 行政部門負責所有相關設備和軟件的安裝和維護。

The Administration department shall store in a secure, central location all original software licenses, disks, CD-ROMs, and documentation upon receipt of all new software, including copies of completed registration cards. 行政部門應在安全的集中位置儲存所有新軟件的原始授權證書、光碟、CD-ROM 和文檔，包括填妥的註冊卡副本。

No employee shall install or distribute software for which this organization lacks the appropriate license. 任何員工不得安裝或分發本組織未持有適當授權的軟件。

No employee shall install any software upgrade on a computer that does not already have resident on it the original version of the software. 任何員工不得在未安裝原版軟件的電腦上安裝任何軟件升級。

The Administration department shall destroy all copies of software that is obsolete or for which the organization lacks the appropriate license. Alternatively, the Administration department may obtain the license(s) necessary to maintain unauthorized software on organization computers. 行政部門應銷毀所有過時或本組織未持有適當授權的軟件副本。或者，行政部門可獲取必要的授權，以便在組織電腦上維護未經授權的軟件。

The Administration department is responsible for establishing and maintain a recordkeeping system for software licenses, hardware, original CD-ROMs and diskettes, user information, and review information. Maintain this information in a secure, central location. 行政部門負責建立和維護軟件授權、硬件、原始 CD-ROM 和磁碟、用戶信息及審查資料的記錄系統，並將此信息儲存於安全的集中位置。

8. Clean Desk Policy 清理桌面政策

The purpose for this policy is to establish a culture of security and trust for all Staff members at HKPC. An effective clean desk / clean screen effort involving the participation and support of all HKPC Staff members can greatly protect paper and electronic documents that contain sensitive information about our clients, customers and vendors. All Staff members should familiarize themselves with the guidelines of this policy. 本政策的目的是為了在本會所有員工中建立一種安全和信任的文化。一個有效的清理桌面/清理屏幕措施，涉及所有員工的參與和支持，可以保護包含我們客戶、顧客和供應商敏感信息的紙本和電子文件。所有員工應熟悉本政策的指引。

The following are suggested actions that can be taken to enhance the execution of this policy: 以下是可採取的建議措施，以加強本政策的執行：

- Allocate time in your calendar to clear away your paperwork. 在日程表中分配時間

來清理文件。

- Always clear your workspace before leaving for longer periods of time. 離開工作場所較長時間前，務必清理工作區域。
- If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shredded bin. 果不確定是否應保留敏感文件的副本，最好將其放入碎紙桶中。
- Consider scanning paper items and filing them electronically on your workstation. 考慮將紙本文件掃描並在工作站中電子存檔。
- Lock your portable computing devices when you are away from them Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer 離開便攜式計算設備時，務必鎖定它們。將 CD-ROM、DVD 或 USB 驅動器等大容量存儲設備視為敏感資料，並將其保存在上鎖的抽屜中。
- When printing, clear sensitive and confidential information from printers immediately. 打印時，立即清除打印機中的敏感和機密信息。
- Lock your desk and filing cabinets at the end of the day. 下班時，鎖好您的桌子和文件櫃。
- Angle your computer screen as far as possible so that unauthorized persons cannot read it. 盡可能將電腦屏幕調整角度，使未經授權的人無法查看。
- Activate the Windows Security Lock when there is no activity for a short pre-determined period of time. 在無活動一段預定的短時間後啟動 Windows 安全鎖。
- Ensure that reactivation is password dependent. 確保重新啟動需要密碼驗證。
- Users should log off their PCs when they leave the office at the day end. 員工在下班時應登出電腦。

9. Training and Awareness 培訓與意識

HKPC will provide regular training sessions to ensure all users understand IT security best practices and their responsibilities under this policy. 本會將定期提供培訓課程，以確保所有用戶了解最佳的 IT 安全實踐及其在本政策下的責任。

10. Policy Review 政策檢討

This policy will be reviewed annually by the IT Department to ensure it remains effective and relevant to HKPC’s operational needs. 本政策將由 IT 部門每年檢討一次，以確保

其對本會的運營需求保持有效性和相關性。

11. Discipline 紀律

- Prohibition of illegal activities: 禁止非法活動:
  - ➢ Unauthorized access to computer data; 未經授權訪問計算機數據;
  - ➢ Use of computers with criminal or dishonest intent; 以犯罪或不誠實的意圖使用計算機;
  - ➢ Criminal damage, such as tampering with web pages or spreading computer viruses; 刑事損壞，例如篡改網頁或散播計算機病毒;
  - ➢ Unauthorized use of network resources; 未經授權使用網絡資源;
  - ➢ Hacking, stealing, or misusing others' accounts and passwords; and 黑客攻擊、竊取或濫用他人賬戶及密碼;

    Disclosing another person's account or password without proper justification. 未經適當理由透露他人的賬戶或密碼。
- Accessing or downloading pornographic material is prohibited. 禁止訪問或下載色情資料。
- Creating, accessing, downloading, or forwarding abusive, unethical, discriminatory, or offensive material, or making vulgar statements, suggestions, or comments that could embarrass or insult members of HKPC or any third party, is strictly prohibited. 嚴禁創建、訪問、下載、轉發侮辱性、不道德、歧視性或冒犯性資料，或發表可能使本會成員或任何第三方感到尷尬或侮辱的低俗言論、建議或評論。
- HKPC resources and work time are reserved for official operations. Activities such as using chat rooms, playing games, or engaging in similar conduct that wastes time and resources, as well as visiting websites for non-business purposes, are prohibited to avoid congestion of internal networks. 本會資源和工作時間僅用於官方操作。禁止進行如使用聊天室、玩遊戲或從事浪費時間和資源的類似活動，並禁止訪問非業務用途的網站，以避免內部網絡擁塞。
- Spreading computer viruses or other programs that interfere with or damage system functionality, whether on the network or others' computers, is prohibited. 禁止散播計算機病毒或其他干擾或損壞系統功能的程序，無論是在本會網絡還是其他人的計算機上。
- The use of peer-to-peer (P2P) software for sharing and downloading files is

discouraged. 不鼓勵使用點對點（P2P）軟件來共享和下載文件。

- External storage media (e.g., USB drives) and files of unknown origin must not be used unless they have been scanned for and cleared of computer viruses and malicious programs. 除非已經掃描並清除計算機病毒和惡意程序，否則不得使用外部存儲介質（例如 USB 驅動器）和來自未知來源的文件。
- No software or programs should be downloaded or executed from the Internet without prior approval from the responsible authority. 不得從互聯網下載或執行任何軟件或程序，除非事先獲得負責部門的批准。
- Uploading any information related to HKPC to external websites without proper authorization is prohibited. 禁止未經授權將任何與本會相關的資料上傳至外部網站。

12. Copyright 版權

Only software that complies with the relevant software licensing agreements is permitted to be installed on office equipment. 僅允許符合相關軟件許可協議的軟件安裝在辦公設備上。

13. Contact Information 聯絡信息

The organization is committed to communicating this Policy with its Staff members. The organization will: 本機構致力於與員工傳達此政策。機構將會：

- Distribute the Policy as part of the induction materials to all Staff members. 將此政策作為所有員工入職材料的一部分發放。
- Require new and existing Staff members whose responsibilities include the installation, maintenance, or oversight of information technology systems to acknowledge and sign the Software Policy Statement. 要求負責安裝、維護或監督信息技術系統的新員工和現有員工確認並簽署軟件政策聲明。
- Circulate reminders of the Policy on a regular basis (at least annually) or remind Staff members of the Policy in other ways (at least annually), for example, through notices or email. 定期（至少每年一次）發送政策提醒，或通過其他方式（例如通知或電子郵件）提醒員工此政策。
- Inform Staff members where they can get additional information on the Policy and software theft prevention. 告知員工可在哪裡獲取有關政策和軟件盜竊預防的更

多信息。

If you have any questions concerning this Policy or your obligations under it, you may direst them to Administration department. 如對此政策或您在其中的責任有任何疑問，請向行政部門查詢。