HKPFA

PHYSICAL FITNESS ASSOCIATION OF HONG KONG, CHINA

中國香港體適能總會

Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to establish guidelines for protecting the confidentiality, integrity, and availability of data and information systems used by Physical Fitness Association of Hong Kong, China (HKPFA). This policy ensures compliance with legal and regulatory requirements while safeguarding member and organizational data.

2. Scope

This policy applies to all employees, contractors, volunteers, and third-party service providers who access, process, or store HKPFA's information assets, including but not limited to:

a. Member personal data
b. Financial records
c. IT systems and networks
d. Physical access to facilities

3. Information Security Principles

a. Confidentiality

i. Sensitive data shall only be accessible to authorized personnel.

ii. Encryption must be used for storing and transmitting personal or financial data.

b. Integrity

i. Data must be accurate, complete, and protected from unauthorized modification.

ii. Regular backups shall be performed to prevent data loss.

c. Availability

i. Critical systems and data must be available to authorized users when needed.

ii. Disaster recovery and business continuity plans shall be maintained.

4. Access Control

a. Role-based access controls (RBAC) shall be implemented.

b. Strong passwords and multi-factor authentication (MFA) are mandatory for system access.

c. Access rights shall be reviewed periodically and revoked when no longer needed.

5. Data Protection

a. Personal data shall be handled in compliance with the Hong Kong Personal

Data (Privacy) Ordinance (PDPO).

b. Data breaches must be reported immediately to the IT Security Officer.

6. **Physical Security**
   a. Secure areas (e.g. server rooms, offices) shall be restricted to authorized personnel.
   b. Visitors must be logged and escorted in sensitive areas.

7. **Incident Response**
   a. A formal incident response plan shall be followed in case of security breaches.
   b. All incidents shall be documented and reviewed to prevent recurrence.

8. **Training & Awareness**
   a. Regular cybersecurity training shall be provided to staff and volunteers.
   b. Employees must acknowledge this policy annually.

9. **Compliance & Enforcement**
   a. Violations of this policy may result in disciplinary action, including termination.
   b. Regular audits shall be conducted to ensure compliance.

10. **Policy Review**
    This policy shall be reviewed annually and updated as needed.

This policy ensures a structured approach to information security for HKPFA while aligning with best practices and legal requirements.

HKPFA
PHYSICAL FITNESS ASSOCIATION OF HONG KONG, CHINA
中國香港體適能總會

信息安全政策

1. 目的

本信息安全政策旨在為中國香港體適能總會（HKPFA）制定保護數據及信息系統的保密性、完整性和可用性的準則，確保符合法律法規要求，同時保障會員及機構數據安全。

2. 適用範圍

本政策適用於所有員工、承包商、志願者及第三方服務供應商，涵蓋對 HKPFA 信息資產的訪問、處理或存儲，包括但不限於：

a. 會員個人資料
b. 財務記錄
c. IT 系統及網絡
d. 設施的實體訪問權限

3. 信息安全原則

a. 保密性
  i. 敏感數據僅限授權人員訪問。
  ii. 存儲及傳輸個人或財務數據時必須使用加密技術。
b. 完整性
  i. 數據必須準確、完整，並防止未經授權的修改。
  ii. 須定期備份以防止數據丟失。
c. 可用性
  i. 關鍵系統及數據必須在需要時可供授權用戶使用。
  ii. 須制定災難恢復及業務連續性計劃。

4. 訪問控制

a. 實施基於角色的訪問控制（RBAC）。
b. 系統訪問必須使用強密碼及多重身份驗證（MFA）。
c. 定期審查訪問權限，並在不再需要時撤銷。

5. 數據保護

a. 個人資料的處理須符合香港《個人資料（私隱）條例》（PDPO）。
b. 數據泄露事件須立即向 IT 安全負責人報告。

6. 實體安全

a. 限制未授權人員進入安全區域（如伺服器房、辦公室）。
b. 訪客進入敏感區域須登記並由專人陪同。

7. 事件應對

a. 發生安全事件時須遵循正式應對計劃。

b. 所有事件須記錄並檢討以防止再次發生。

8. 培訓與意識

a. 定期為員工及志願者提供網絡安全培訓。

b. 員工須每年確認遵守本政策。

9. 合規與執行

a. 違反本政策可能導致紀律處分，包括解僱。

b. 定期進行審計以確保合規。

10. 政策檢討

本政策須每年檢討並按需要更新。

該政策確保 HKPFA 採取結構化的資訊安全方法，同時符合最佳實踐和法律要求。