附錄 15：資訊保安政策

我們的目的

本政策規定了香港中華煤氣有限公司（「本公司」）及其附屬公司（統稱「中華煤氣集團」）的責任和政策，確保中華煤氣集團資訊和技術資產的機密性、完整性和可用性。我們鼓勵所有項目公司、聯營公司、 供應商和業務夥伴在適用的情況下參考本政策的原則。

我們的承諾

資訊是公司極具價值和重要的資產，須防範可能對其機密性、完整性和/或可用性受威脅的風險。有效的資訊安全管理能夠在資訊共用的同時將其所面臨的風險減到最低。 我們將不斷改進資訊安全系統，以助監控和應對資訊安全威脅。

根據 ISO/IEC 27002 國際資訊安全管理標準，中華煤氣集團承諾：

- 保障中華煤氣集團資產能得到適當的等級保護並問責；
- 確保僱員、承包商和協力廠商用戶瞭解他們的責任和資訊安全要求，及符合他們所擔當角色的相關要求，以幫助降低被盜竊、欺詐或濫用設施的風險；
- 降低在正常工作時間內外資訊遭到未經授權訪問、丟失和損壞的風險；
- 透過意識培訓，確保正確利用任何電腦、網絡、移動設備、電話、電子郵件、即時通信服務、社交網站、語音郵件和傳真來開展內部和對外業務；
- 保護中華煤氣集團的知識產權，包括商標、版權和商業秘密，免遭濫用和未經授權的披露；
- 監管中華煤氣集團外部的供應商、顧問、承包商和其他服務提供者的選擇和管理，並保護中華煤氣集團的資訊及其處理設施；
- 制定一份記錄在案並通過測試的災難復原計劃管理文檔，描述當在關鍵系統因災難中斷影響運營的情況下，如何確保仍可繼續營運業務；
- 保護客戶資訊；
- 確保採用適當的用戶授權訪問資訊系統及妥善維護帳戶；
- 制定使用移動設備訪問中華煤氣集團資源的可接受範圍；
- 實施控制措施限制授權人員訪問資訊處理設施，同時提供正常業務活動中斷期間的監控；
- 監控外網遠程訪問系統；
- 確保按照業務和安全的基本要求控制對網路、服務和資訊系統的訪問，同時權限需得到適當授權、分配和維護，嚴禁未經授權的訪問；
- 建立創建強式密碼、密碼保護以及更改頻率的標準；
- 最低安全風險實踐貫穿於系統需求收集、開發和維護整個過程中，以確保所有

資訊系統得到足夠安全保護，並防止應用程式使用中出現錯誤、丟失、未經授權的修改或誤用；

- 以合理及可預見的方式管理對生產伺服器、設施、應用程式、網路和基礎設施服務的更新修改，以便僱員和用戶能夠做出有計劃的應對，從而降低未經授權此類更新修改與錯誤造成系統服務中斷的可能性；
- 為已經得到公眾認可並證明有效的加密演算法提供使用指引，提供管理加密金鑰方向，並確保遵守有關使用加密技術的適用規則；
- 確保資訊備份足以覆蓋大部分可預期情況，以儘量把丟失資料和影響操作減到最小；
- 制定使用的網路設備、伺服器和應用程式的補丁管理和技術更新的基線要求，將潛在漏洞的風險降至最低；
- 制定檢測、預防和恢復流程，防止在中華煤氣集團擁有或管理的用戶終端設備（如已派發的工作站、筆記型電腦和移動設備）以及 IT 基礎設施網路和系統上執行惡意軟件；
- 通過採用雲服務商提供的安全保護服務與措施，保障雲端應用系統安全且高效；
- 確保對煤氣公司面向互聯網的網路資源和面向客戶的網路應用程式得到適當的保護；
- 確保對煤氣公司的機密資料按照分類級別進行適當的洩漏預防保護;
- 制定應用程式 API 介面的管理, 包括介面驗證及數據加密保護措施等;
- 確保人工智能用得其所符合中華煤氣集團利益及數據安全;
- 確保物聯網設備開發及應用，融入風險考慮因素及保護措施，減少網絡攻擊風險；及
- 確保特權帳號的存取控制僅限於具有合理業務需求的帳戶，包括對特權帳戶的申請、審批、記錄、檢視及設置密碼的要求。

針對我們的資訊安全要求和考慮已制定了一套內部政策。

更新日期：2024 年 8 月 30 日