港燈電力投資
HK Electric Investments

資訊保安政策

2022 年 10 月

目錄

1. 引言

1.1 港燈電力投資有限公司及其附屬公司，包括香港電燈有限公司（統稱「集團」）對資訊保安非常重視。集團內的信息資源（「信息資產」或「信息」），無論以任何形式存在，或以任何形式建立、傳達、使用或儲存，均為集團寶貴資產，必須受到保護，以免信息在故意或意外的情況下被未經授權地存取、修改、刪除或披露。

1.2 本政策為資訊保安的綱領政策，概述保護資訊的原則、方法、責任和要求，同時令集團有效和適當地運用資訊從事業務和技術營運。

1.3 本政策是集團資訊保安管治框架的基礎，框架內備有一系列因應特定問題制訂的政策，標準、指引和程序，就以下資訊保安的三個重點作出說明：

- **保密**：保護資訊免受未經授權的存取或披露。存取資訊的權限應就知情需要給予授權人士。
- **完整**：保障資訊免受未經授權的修改或刪除，以確保其準確性、完整性和有效性。
- **可用**：確保資訊僅限於授權人士有需要時進行存取。

2. 範圍

2.1 本政策適用於：

2.1.1 所有經授權進入集團的工作場所、系統或存取資訊的僱員、承辦商及供應商（相關「使用者」）。

2.1.2 集團內所有資訊系統及技術平台（相關「IT 設施」）以及在系統及平台上的資訊、關連的電子媒體，或打印本。

3. 目的

3.1 本政策旨在保護信息資產及 IT 設施免受所有來自內部或外圍、惡意或意外的安全威脅或可能出現的漏洞。本政策的目的為：

3.1.1 就如何合理使用資訊及 IT 設施釐訂原則和要求，並說明如何在整個集團內執行。

3.1.2 以 ISO / IEC 27002 - 「資訊保安管控實務守則」為基礎，建立集團的資訊保安管治框架，以達至以下目標：

3.1.2.1 協助使用者明白集團對合理使用資訊和 IT 設施的期望和要求，以及使用者就保障資訊保密、完整和可用性的角色和責任。

3.1.2.2 遵從因應特定問題制訂的安全政策、標準及指引，實施適宜的控制、程序和技術，確保信息資產的保護符合其風險水平和價值。

3.1.3 提高使用者對資訊保安的意識。

4. 組織角色及責任

4.1 資訊保安和適當保護資訊是所有使用者的責任。每個使用者均應以專業和負責任的態度從事業務，並須為其使用資訊及（如適用）相關 IT 設施的行為負責。此章節概述不同範圍內的角色和責任，以確保資訊及相關 IT 設施的安全。

4.2 資訊科技科總經理

4.2.1 資訊科技科總經理有直接責任確保：

4.2.1.1 管理本政策的發展、執行及維持。

4.2.1.2 負責資訊安全管治，管理因應特定問題制訂的安全政策、標準，指引及程序，以確保信息資產及相關 IT 設施的安全。

4.2.1.3 管理重要資訊保安項目，並監察集團的資訊保安審核。

4.2.1.4 不時檢討現有措施，並在有必要時進行修改或實施新措施，以確定資訊和 IT 設施的安全。

4.2.1.5 建立資訊保安風險評估指引和報告機制，協助集團旗下各業務單位進行保安風險評估，並就各職責範圍滙報資訊安全狀況和重大安全事項。

4.2.1.6 制定使用 IT 設施和資訊的合規程序、流程和實踐方法。

4.2.1.7 在處理安全事故中擔當焦點角色，並就可能影響集團的資訊保安趨勢和威脅，向各業務單位提供建議和協助。

4.2.1.8 為集團制定戰略和實施提高資訊保安意識的教育計劃。

4.2.1.9 至少每年審視一次本政策的有效性，並在適當時對本政策進行必要的更改，以反映當前的業務狀況和規管要求，以及應對日益猖獗且形式多變的資訊保安威脅和漏洞。

4.3 業務單位主管

4.3.1 業務單位主管有責任確保在其業務範圍完全遵守本政策，以及因應特定問題制訂的相關安全政策、標準、指引及程序。具體來說，業務單位主管須負責：

4.3.1.1 確保轄下所有員工和承辦商完全熟悉本政策，以及因應特定問題制訂的安全政策、標準、指引、程序和相關法律，並意識到違規的後果。

4.3.1.2 為員工和承辦商提供合適培訓，以便使用本集團的 IT 設施和信息資產。

4.3.1.3 在各自職責範圍內擔任信息資產的資訊擁有人。

4.3.1.4 透過定期風險評估和報告，將資訊風險作為其更廣泛的風險管理職責進行管理。

4.3.1.5 在各自的業務範圍內實施適當措施，以降低集團面對的資訊風險。此類措施可能包括業務可持續計劃，職責分工，雙重控制，或在主要敏感區域進行工作輪換。

4.3.1.6 通過既定程序知會資訊科技科（IT）任何可能影響存取權限的改變，包括員工因工作輪換、晉升或辭職導致工作職能或狀態的變化。相同原則亦適用於有權限存取資訊以執行職責的承辦商或其他人員。同樣，業務單位主管亦有責任知會 IT 或相關資訊擁有人任何疑似或實際的違規事故，以及資訊保安方面被視為漏洞的事項。

4.4 內部稽核

4.4.1 內部審核部負責進行信息安全審核，以檢查是否符合政策和指引的規定。

4.5 使用者

4.5.1 本集團的 IT 設施和信息資產僅限於商業用途。使用者可存取、使用或分享資訊，惟僅限於授權範圍及執行指定職務所必須的權限。使用此等資產對使用者構成一定的責任和義務，並受所有適用的集團政策和指引所約束。在這方面，使用者有責任履行以下與資訊保安相關的事項：

4.5.1.1 確保不濫用信息資產和 IT 設施，並遵守所有集團安全政策、標準、指引和程序。

4.5.1.2 通過既定程序向資訊科技科總經理報告所有真實或疑似資訊安全事故，例如盜竊，遺失或未經授權的信息披露；或在集團安全政策、流程或基建中被視為漏洞的任何項目。如情況合適，亦應向其業務單位主管滙報。對於承辦商使用者，應將安全事故報告予指定的集團負責人，報告內容包括但不限於犯罪，威脅，違反安全及其他違規行為。但是，在任何情況下，業務單位主管

都必須承擔問責，並確保採取適當安全措施，以保護其資訊的機密性，完整性和可用性無損。

4.6 資訊擁有人

4.6.1 根據本政策，資訊擁有人是集團內各業務單位的主管或其委任代表，負責決定誰人擁有存取資訊的權限，以及在整個信息生命週期中如何管理和使用信息。

4.6.1 集團內的每項信息資產必須由業務單位主管或其指定代表（「資訊擁有人」）擁有。在資訊保安方面，資訊擁有人須負責：

4.6.1.1 確保根據「集團資訊分類政策」對信息進行分類，並採取適當的安全管控措施防止未經授權的存取，披露或修改。

4.6.1.2 將信息發布予集團內其他業務單位或外部第三方時，須界定所屬類別（即「未分類」、「僅供內部使用」或「機密」）。

4.6.1.3 以最小特權和知情需要為原則控制信息的存取，並僅向使用者授予執行其工作所需的權限。

4.6.1.4 定期檢討與信息資產相關的存取權限，並在適當時進行必要的修改。

5. 法例要求

5.1 集團須實施恰當的保安措施以確保信息資產及其相關系統的保密性、完整性及可用性，同時亦須確保遵守所有適用法例要求。

6. 資訊保安風險管理

6.1 為有效地管理資訊風險，每項風險必須通過正式的風險評估予以識別。本集團採用集團範圍內的評估慣例，以識別新和相關的資訊保安風險，並根據漏洞和對信息和 IT 設施的影響，提出優化建議，實施適當控制及其他降低風險的措施。

7. 適當使用

7.1 資訊和 IT 設施該用於商業用途或其他獲批准的活動。本集團保有權利，在無需任何使用者的同意下檢查和 / 或披露儲存在 IT 設施中，或經 IT 設施傳輸的所有信息。惟此等檢查只能在為了確保遵守內部政策、支援內部合規表現或欺詐調查、遵從收到的傳票或法院命令等法律要求、或協助 IT 設施的管理情況下執行。此類檢查只會在使用者所屬的業務單位主管授權之下進行，在進行檢查時，亦需在有關業務單位的一位代表見證下進行。

8. 資訊分類管理

8.1 信息資產必須按照「集團資訊分類政策」分類為不同類別，以反映其對集團的敏感程度和價值。其生命週期內所獲的安全保護水平直接取決於其分類類別。關於分類詳情，請參考上述 4.6.1.2 項。

9. 存取控制管理

9.1 存取資訊必須透過存取權限予以保護，確保有關資訊不會被不當披露，修改，刪除或變得不可用。

9.2 資訊擁有人負責誰人可存取其資訊。存取權限將按知情需要及最小權限原則為基礎。

9.3 給予特權予 IT 設施管理人員去管理 IT 設施是不可避免的。為確保 IT 設施的完整性和可用性，任何特權存取的要求必須獲得資訊科技科的部門首長或更高級的主管的授權，並應該只在批准下的期限內使用。所有活動必須記錄在案以供審核和未來參考。

9.4 已制訂流程定期審視用户權限和特權，以確保合法存取。倘某用户已被解除職務而無需存取資訊，其存取權限將立即被撤回。

10. 資訊私隱

10.1 本集團尊重和致力保障個人私隱。集團內所有牽涉個人資料的資訊均根據「集團個人資料私隱政策」管理和保護。

11. IT 資產管理

11.1 本政策內所指的「IT 資產」，為集團所擁有或管理的任何設備或服務，例如伺服器、儲存系统、網絡設備、數據庫及應用程式，而此等設備或服務皆被連接到集團網絡或被應用於集團的業務營運。IT 資產管理是審慎保安及管理的重要手段，亦為所有因應特定問題制訂的資訊安全政策、指引、程序，和標準要求提供背景資料和審視脈絡。

11.2 IT 資產有被攻擊的風險，故在其購買或開發週期內每個階段，均須嚴格遵守「設計安全性」和「預設安全性」的原則。本集團已就第三方提供的 IT 資產發布指引，協助個別業務單位了解其必須符合的基本數據和系統安全要求。此外，IT 資產作為重要資源，在其生命週期內將得到妥善保養和支援。

12. 網絡安全

12.1 網絡基礎設施是內部和外部系統之間的重要連接。為防止惡意侵擾，必須建立

穩妥安全的界限和連接，並且按照集團最新的安全實踐規例進行管理。

12.2 集團的網絡架構必須配合現時和未來的業務要求，且足以應付新湧現的威脅。集團必須採用合適的週邊保安技術以確保使用者瀏覽不可信的網絡（例如：互聯網）時，同時能够確保集團內部網络的安全。

13. 移動設備安全

13.1 集團鼓勵以移動設備作為商業用途，因為它為使用者提供靈活、有彈性的工作安排。為給予使用移動設備的員工最大便捷，而同時將風險降至最低，集團已：

13.1.1 實施移動設備上架程序。獲准登入集團內部網絡存取資訊的移動設備一概由適合的移動設備軟件管理，並設有保安設施進行保護。

13.1.2 制定「移動設備政策」，為移動設備的正確使用、管理，和保安訂立規則和指引，讓使用者在合法的商業用途下存取集團的信息及 IT 資產。

14. 終端用户設備的保護

14.1 終端用户設備（「終端設備」）主要為桌面及筆記本電腦。它們亦是連接到集團 IT 設施和資訊的主要設備。終端保護平台作為保障內部網絡的第一道防線，在集團資訊保安管理上至為重要。

14.2 集團已採用合適的終端安全設施，為終端設備提供全面保護，避免受到精密的惡意軟件和不斷演變的網絡安全威脅侵擾。此外，亦要求用戶全面遵守「集團個人電腦安全政策」中規定的標準。

15. 遠程存取

15.1 遠程存取的定義為通過任何設備（例如筆記本電腦，手提電話或平板電腦）經過未被信任的網絡和不論任何發起連接的位置，連接到集團的內部網絡，從而可以登入 IT 設施及存取信息資產。員工及承辦商的遠程存取資格由負責的業務單位主管決定。

15.2 遠程存取的操作須通過加密和多重認證等手段嚴格控制。獲授權的使用人士必須遵守「集團存取控制政策」，並採取合理的預防措施，確保使用遠程存取時保障集團的資訊和網絡。

16. 應用程式的保安

16.1 在應用程式開發的生命週期內所有階段，安全是最重要的考慮因素，尤其是當開發是用以管理關鍵的信息和資源。

16.2 集團對應用程式的設計和開發，堅決採用「設計安全性」和 「預設安全性」的

方法，由起創到開發週期的不同階段，均著重將安全功能嵌入應用程式，以防止程式推出後面對保安漏洞的威脅。

17. 安全日誌紀錄和監控

17.1 能夠及時偵測資訊安全事故，有賴持續監察和對保安日誌的全面分析。有關登入紀錄的產生由安裝在集團內部網絡的無數個保安設備負責，例如防火牆、入侵檢測系統，以及安裝在集團的 DMZ （非軍事區）及內部網絡的電郵過濾設備。

17.2 集團已聘請外部的保安運營中心進行二十四小時主動監控和作出安全日誌分析，並就集團內部及週邊範圍的保安紀錄進行實時相關比對，以便及早發現疑似安全事故，採取對策。

18. 安全事故管理

18.1 本集團已執行適當措施偵測安全事故的發生，並訂立事故處理程序，確保採取迅速、有效和有序的回應，控制和減低相關破壞的措施。

18.2 事故發生後將進行檢討，以確定是否有安全隱患需透過實施新的或修訂的安全控制措施予以解決。

19. 漏洞管理

19.1 所有 IT 設施都難免存有漏洞，並時刻受到惡意攻擊的威脅，破壞資訊的保密性、完整性和可用性。

19.2 修補漏洞可以透過安裝供應商的安全修補程式解決。「集團保安修補程式管理政策」的制定，旨在確保為已知漏洞進行準確和適時的更新，保護 IT 和信息資產的安全。

19.3 倘若真的出現目前的技術不能抵禦的攻擊（例如，零時差漏洞），或因業務需要就該漏洞進行糾正，則可以使用補償控制來解決已識別的漏洞。

20. 變動管理

20.1 《集團變動管理指引 – IT 部門》界定了標準化流程，確保 IT 設施的變動獲得適當管理，並且在系統化、安全和受控的前提下得以記錄、評估、授權、確定優次，並予以執行和發放。變動管理流程的主要目標為（a）通過定期檢討和學習培養有關人員持續改進的態度；（b）根據業務需要檢討變動事項及其優次；（c）評估變動帶來的風險影響並實施必要的緩解措施；（d）建立變動後的問責和責任制度，貫徹始終；（e）防止對 IT 設施在未經授權下出現變更，以及（f）盡量減少因非計劃或緊急變動造成的破壞。

21. 災難復修計劃

21.1 本集團已制定災難復修計劃（DRP），並實施信息備份操作和開發 IT 服務恢復功能，確保一旦發生災難時可按業務運營需求和優次，恢復個別關鍵 IT 設施和信息資產。

22. 第三者風險管理

22.1 聘用承辦商時，應就其參與的工作性質採用適當的資訊保安控制措施，特別是與第三者賣方和供應商共享的集團專用和敏感資訊，對集團引發的安全風險須透過營運手段及合約條文予以管控。

22.2 為減輕與供應鏈相關的資訊安全風險，本集團已制定指引協助個別業務單位，針對合約的不同性質和風險建立相關的資訊保安控制措施。該指引亦幫助業務單位進行評估，以進一步了解承辦商的安全狀況。

23. 資訊安全意識教育

23.1 除非使用者已閱讀並理解本政策，以及因應特定問題制訂的安全政策，標準，指引和程序，否則不得被授權存取資訊或使用集團的 IT 設施。各業務單位主管應制定適當措施，確保完全符合要求。

23.2 業務單位主管應確保其員工了解與其活動相關的安全風險，並有足夠的培訓和技能，在授權下安全地使用本集團的 IT 設施和資產。

23.3 IT 將提供複修課程和其他材料，定期提醒使者有關資訊保安的義務和責任。

23.4 除常規的培訓和提高安全意識的活動外，IT 將定期進行類似消防演習的資訊保安演習，確定使用者時刻提高警覺，防患未然。

24. 違反政策

24.1 所有使用者有責任確保其行為不會引致實際或可能發生的違反安全事故。違反本政策被本集團視為嚴重紀律事宜，可促成紀律處分包括终止聘用。

24.2 第三者違規行為將按本集團與第三者合約所訂立的條款處理。

25. 溝通及查詢

25.1 任何關於本政策或因應特定問題制訂的安全政策、標準，指引或程序等查詢或改進建議，應轉交資訊科技科總經理跟進。

26. 政策檢討

26.1 本政策必須每年或在適當情況下更頻繁地進行檢討，以確保所有政策規定切合所需。

- 完 -