Power Assets Holdings Ltd.
電能實業有限公司

資訊安全政策

2021 年 2 月

目錄

1. 政策聲明

本文件旨在界定及協助溝通適用於整個集團（包括電能實業有限公司及其附屬公司（「本集團」）有關資訊保密、其完整性及可用性的共同政策。本文件所述的政策將作為制訂其他資訊安全政策、程序及準則的基礎。

本政策適用於集團所有成員公司，範圍涵蓋集團內所有不同類型資訊的建立、傳達、儲存、傳輸及銷毀，包括但不限於電子版本、印刷本及口頭披露，且不論以個人、電話或其他方式進行。

有關本政策的問題應直接轉交負責集團資訊科技的主管（「資訊科技主管」）。

2. 原則

2.1 問責

集團內各人均有責任保護資訊。

- 資訊安全問責及責任必須在整個集團中清楚界定及確認。
- 集團內的所有人士（包括僱員、顧問、承辦商及臨時員工）均須對存取及使用資訊（如新增、修改、複製及刪除）負責。
- 所有問責方必須以及時和協調的方式，防止資訊及資訊系統的安全遭到違反及應對有關威脅（人手、電腦化、或結合兩者）。

2.2 比例

資訊安全控制，應該與資訊的修改、拒絕使用，或披露的風險成正比例。

- 資訊安全措施，應該與資訊的價值、敏感度，以及可能遭受威脅的程度相對應。
- 資訊安全措施，應足以彌補內外環境中因儲存、傳輸、處理或使用資訊的本有風險。

2.3 知情需要

存取公司資訊應受到限制，僅有明顯商業理由存取資訊者方可存取資訊。

2.4 組織內的角色及責任

須確定組織內的角色及責任，以制訂、溝通、實施及監理政策。

除本政策內特定角色及其責任外，各業務單位的管理層有責任確保本文件內所載政策在其管轄範圍內實施。

2.4.1 資訊科技主管

資訊科技主管須負責：

1. 建立及改善整個集團內的資訊安全文化。
2. 管理集團資訊安全政策的發展、落實及維持。
3. 保證整個集團內的資訊安全狀況，包括妥善落實及遵守集團資訊安全政策的情況。
4. 協調與重大安全事項有關的活動。

資訊科技主管尤須：

- 按需要發表有關遵守本政策的準則。
- 檢討集團資訊安全措施的有效性，包括在有需要時檢討及監察集團內的安全事故。
- 為業務單位制定程序，就資訊安全狀況及重大資訊安全事項進行匯報。
- 負責評估集團資訊安全的管治及風險。
- 促進整個集團內對潛在威脅、漏洞及控制技術的了解。

- 定期舉行培訓和演習，確保業務在發生資訊安全事故後可持續運作。

- 監察集團內外有關資訊安全的趨勢，並讓高級管理層知悉資訊安全相關問題和影響集團的活動。

2.4.2 業務單位主管

業務單位主管[1]須負責：

1. 建立及改善業務單位的資訊安全文化。

2. 確保制訂和落實業務單位的額外政策、程序及準則，以支援本政策及相關政策、程序及準則。

3. 保證業務單位的資訊安全狀況，包括妥善落實和遵守業務單位及集團資訊安全政策、程序及準則的情況。

4. 協調與重大安全事項有關的活動。

業務單位主管尤須：

- 界定業務單位內額外的資訊安全角色及責任。

- 確保落實方法、程序及風險評估，以支持集團的資訊安全政策、程序及準則。

- 提供資訊安全教育，並確保培訓和出席情況。

- 協助業務單位的管理人員制訂應對計劃，有效處理資訊安全事故。

- 制定業務單位的匯報程序，於有需要時就資訊安全狀況向單位和集團匯報。

---

(1) 本政策內，業務單位亦包括提供支援服務予集團的港燈電力投資有限公司旗下服務單位。

- 檢討業務單位資訊安全措施的有效性，包括在有需要時檢討及監察單位內的安全事故並向集團匯報。

- 就進行中及計劃執行的業務，協助業務單位審視其中的資訊安全風險。

- 與業務單位管理人員合作進行資訊安全風險評估。

- 促進業務單位內對潛在威脅、漏洞及控制技術的了解。

- 監察業務單位內外有關資訊安全的趨勢，並讓高級管理層知悉資訊安全相關問題和影響單位的活動。

2.4.3 資訊擁有人

各業務單位的管理層須確保集團每項資訊需有對應的指定擁有人，稱為「資訊擁有人」。 本文件內「資訊擁有人」一詞僅適用於與本政策有關的資訊安全事項，並不代表對資訊有任何形式的法定擁有權。

一般而言，除非另有指定，否則，

1. 一項資訊的建立人須被假定為資訊擁有人。

2. 對於從外界接收的資訊，指定收件人將自動成為「資訊擁有人」。

「資訊擁有人」負責：

- 確定與資訊相關的授權及處理程序。

- 採取措施確保資訊的儲存、處理、發佈及正常使用有合適控制。

- 確保資訊按知情需要提供予所相關人員。

2.5 資訊管理

2.5.1 分類及標籤

為管理及控制資訊的存取，業務單位的行政人員應考慮將資訊正式分類及標籤，但應適當考慮業務上的需要、成本（內部及外部）和實際可行等因素。正式分類的指引載於附錄一。

2.5.2 資訊保護的一致性

不論資訊置身任何地方、以何種形式儲存及目的為何，須一致受到保護。

2.5.3 披露資訊

經與業務單位主管商議，而其操作亦符合集團資訊科技主管發出的標準，業務單位的管理人員需就披露和收取任何敏感資訊建立和實施特定規則及指引，例如：發出或簽署不披露協議，及處理從外界人士收取的敏感資訊。

2.5.4 控制權變動

資訊安全過程中的改動，包括系統及程序上的變動，必須獲得適當批准、予以記錄，並通知有關人士。應就保密資訊實施正式的控制權變動程序。

2.6 存取控制

存取資訊和處理相關風險之間應作出適當控制以取得平衡。

- 無論要求存取資訊人的士職級為何，存取資訊必須以「知情需要」作為基礎，按分類遵從特定商業規定指引進行。

- 存取資訊須取得授權。須就每個資訊系統（不論電腦化與否）實施授權過程。授權過程須由「資訊擁有人」以及相關的業務單位主管批准。

2.7 評估

公司應定期評估與資訊及資訊系統有關的風險。

- 業務單位的行政人員應確保定期及在情況需要時進行風險評估，從而審視資訊控制的有效性。於風險評估中識別的弱項應視乎威協及影響，訂立時限妥為處理。

- 就每個業務單位實施的資訊安全措施，公司應定期進行獨立檢討。當單位作出重大修改，令其風險環境可能出現變動時，以上檢討亦同樣適用。

2.8 意識

所有因需要知情而可存取資訊的人士，應可查閱有關資訊安全及資訊系統的原則、標準、公約或機制，並應獲告知有關資訊安全可能出現的威脅。

- 在存取資訊或獲提供支援資源前，所有人士的誠信、知情需要及技術能力的相關資歷應先進行核實。

- 集團所有人員必須明白集團有關資訊安全的政策及程序，並必須同意根據該等政策及程序履行工作。

- 集團的業務夥伴、供應商、客戶及其他商業聯繫人士，必須清楚明白其對資訊安全的責任。此等責任需在與集團的合約中用特定文字清楚界定。

- 集團資訊科技主管應設立渠道及組織，與集團業務單位分享及溝通資訊安全的相關知識和經驗。

2.9 教育

本政策須傳達予集團內所有人員，確保他們明白本政策及政策下的責任。

- 公司必須向所有僱員提供有關資訊安全的培訓。培訓包括政策、標準、底線、程序、指引 、責任、相關執行措施以及未能遵守有關規定的後果。公司應定期進行培訓及複習訓練。

- 集團所有僱員應獲提供參考資料支援其妥善保護，或以其他方式管理資訊。

2.10 事故管理

公司應盡快及有效地回應所有資訊安全事故，盡量減低對業務的影響及日後遇到同類事故的機會。

- 資訊安全事故（即影響或可能影響資訊安全的任何事件）必須向適當人士匯報，包括集團法律顧問及公司秘書、「資訊擁有人」、有關業務單位主管，以及在業務部門或集團其他單位可能受影響的人士。匯報內容亦應包括解決事故的過程和步驟。

- 各業務單位應設立有效的資訊安全事故應變計劃。該計劃應說明（其中包括）：(i) 單位內應對事故人員的組成及角色；(ii) 與內部及外界人士溝通流程（後者包括客戶、執法機 構、監管機構及傳媒)；及 (iii) 識別事故成因以及適時恢復受影響數據所用的技術、工具和資源。

2.11 持續營運及應變計劃

資訊系統的設計和運作，應以機構能確保不間斷的營運為依歸。

各業務單位須設有計劃確保維持資訊的保密性、完整性及可用性，以便在業務中斷或災難情況發生時支持業務持續運作。該計劃必須予以記錄及告知相關人士，並定期進行相關演習。

2.12 法律、監管及合約要求

所有與資訊安全有關的法律、監管及合約要求（包括適用的個人資料保護及私隱法律）必須加以考慮及處理。

- 當處理資訊安全時，集團最低限度必須符合所有適用法律及監管要求。各業務單位有責任確保遵守各自的監管及其他法律要求。

2.13 資訊私隱

各業務單位須審慎執行資訊安全措施，以符合業務單位和集團適用的法律、以及保護資訊私隱和資料的政策。

2.14 政策文檔及管理

資訊安全政策及其相關的支持標準、底線、程序和指引應被妥善制訂和執行，以應對資訊安全各方面的要求。有關指引必須指明個人或機構實體獲授權的責任、酌情權及可承擔的風險水平。

本政策是一份不斷更新的之文件，需定期審閱和更新。此過程可包括（其中包括）監管關注事項和法例的變化，以至核心業務和技術的改變。

2.15 政策例外情況

本政策有時須就業務或實際需要設有例外情況，惟須按資訊科技主管建議和批准，由相關業務單位主管授權。

- 對於例外的情況，包括其理據、期限及詳情，必須在合理時間內記錄。

- 對於例外的情況，倘業務或風險有所改變、或負責的行政人員出現變動，或在資訊科技主管指定的一段時間後（以較早者為準），公司須重新評估及批准該等例外情況。

2.16 違反政策

違反本政策被視為嚴重違反行為，將受到適當處理，重點在於防止日後再次發生。

不遵守資訊安全政策、有關標準或程序可促成紀律處分，包括終止聘用。

- 完 -

附錄一：數據分類及標籤指引

1. 數據分類

所有資訊應其按敏感度分類。建議分類為：

- 公開
- 內部使用
- 保密

此等分類的目在於根據「知情需要」的政策保護資訊免受任何未經授權的披露、使用、修改或刪除。換言之，即存取公司資訊應受到限制，只有明顯商業理由存取資訊的人士方可獲授權存取資訊。

並無特定分類的資訊應被仔細審視以確定其類別，如無法分類，則會被設定為「內部使用」，並應作出相應處理。

在本附錄內：

- 資訊的存取控制表為獲授權存取資訊人士或組別的名單。
- 分派名單為實際獲分發資訊人士或組別的名單。

1.1 公開

「公開」類別適用於已獲相關業務單位管理層，明確批准向集團以外公眾人士公開披露的資訊。

只有獲指定人士方可將資訊分類為「公開」。

只有獲指定人士方可披露「公開」資訊。披露有關資訊須依循預設的程序、規則及指引。

1.2 內部使用

「內部使用」類別適用於資訊，即如不慎地或無取得授權下獲披露，可能對業務單位、部門或集團造成負面影響，並就處理有關影響時可能招致成本。

不得在無獲得「資訊擁有人」事先批准的情況下向集團以外的任何人士披露供內部使用的資訊。如供內部使用的資訊附有任何存取控制名單，則在無獲得「資訊擁有人」的事先批准下，不應向控制名單以外的任何人士披露；惟對於內部使用且並無存取控制名單的資訊，則可在集團內披露。

「資訊擁有人」可以就供內部使用的資訊施加額外披露或處理限制。額外限制不得削弱本文件所述的基本披露規則。

1.3 保密

「保密」分類適用於資訊，即如不慎地或在無授權情況下披露，可能對業務單位、部門或集團造成重大負面影響，或就處理此等影響可能招致重大成本。

保密資訊應經常設有分派名單或存取控制名單，以及在無資訊擁有人的事先批准下，不應向該分派名單或存取控制名單以外的任何人士披露。在無存取控制名單的情況下，分派名單會被視為存取控制名單。在無分派名單及存取控制名單的情況下，没有資訊擁有人的事先批准，不應向任何人士披露保密資訊。

資訊擁有人亦可以進行額外披露或處理保密資訊的限制。額外限制不得削弱本文件所述的基本披露規則。

此外，處理保密資訊（包括展示、儲存、傳送及棄置），必須就故意及不慎作出未經授權披露作出進一步保護。

由於集團業務多元化及基於當地需要，業務單位應進一步因應其業務需要、遵守法例及行業要求制定合適的資訊類別。然而，最終的類別應能夠被納入以上三個預設的分類，及不得違反或抵觸本政策所載的原則。

2. 資訊標籤

業務單位的管理層負責評估、設計及實施其各自業務部門資訊標籤的適用程序。然而，有關活動應符合需要及按以下準則進行：

1. 當地法例所規定，或

2. 在沒有其他替代方法的情況下，個別標籤是持份者得知資訊敏感度的唯一方法，及

I. 其在技術上可行，及
II. 其在經濟上可行，意即此等做法的整體利益超出包括持續維護等成本。

如某個業務部門決定進行資訊標籤，應適用下列規則：

- 保密資訊應首先被標籤。
- 資訊擁有人負責按照分類對資訊進行標籤。
- 只有資訊擁有人或其指定人士獲授權更改資訊的標籤。
- 分類標籤應是顯而易見。
- 存取控制名單以及任何額外限制應在分類標籤清楚說明，或令其明顯易見。分類標籤的例子如：「內部使用 - 僅供 X 公司使用」或「保密 - 僅供 XX 部門使用」或「內部使用 - 僅供電能實業集團內部使用」。
- 存取控制名單或額外限制不能取代分類，即不論資訊的任何額外限制，資訊分類（如保密）應標示在標籤上。

- 完 -