

富威電力股份有限公司	文件編號	AD02-02	版本	2.0
	制訂部門	資訊部	頁次	1 / 4
文件名稱	資訊安全政策	實施日期	2023 年 11 月 27 日	

1、總則

1.1 目的

本政策規範資訊安全管理制度，為強化資安管理，確保公司資料、資訊、設備、人員與網路的機密性、完整性及可用性，使本公司避免遭受公司內部與外部的蓄意或意外之任何威脅，達到資訊安全。

1.2 適用範圍

凡隸屬本公司組織內之資訊安全相關事項，悉依本規章所規範的體制管理之。

1.3 權責單位

資訊部設置資訊安全專責單位、主管及資訊安全人員，專門負責資訊安全事務，權責單位主管經總經理授權，負責本規章管制，並確保本規章之規範作業。

1.4 名詞定義

「資訊安全」涵蓋範圍如下：

- 1) 資訊安全權責分工。
- 2) 人員安全管理及資訊安全教育訓練。
- 3) 電腦系統安全管理。
- 4) 網路安全管理。
- 5) 系統存取控制管理。
- 6) 系統發展及維護安全管理。
- 7) 資訊資產安全管理。
- 8) 實體及環境安全管理。
- 9) 業務永續運作計畫管理。
- 10) 其他資訊安全管理事項。

2、資訊安全目標

- 2.1 確保本公司所保管資料之機密性、完整性與可用性，防止非法使用資料。
- 2.2 確保本公司所提供資訊服務之完整性與可用性，提供全體員工便利和穩定的資訊服務。
- 2.3 確保本公司所提供軟硬體資源之可用性，合法及正確地使用。

3、資訊安全要求事項

- 3.1 確實遵守「個人資料保護法」、「著作權法」、「電子簽章法」等資訊安全相關法令。
- 3.2 為能有效確保本公司之資訊安全，應針對各資訊安全領域訂定資訊安全規範。
- 3.3 確實遵守本公司相關資訊安全規定，確保適當使用本中心資源。
- 3.4 遵循本公司資安事件通報機制，通報所發現之資訊安全事件或資訊安全弱點。

富威電力股份有限公司		文件編號	AD02-02	版本	2.0
		制訂部門	資訊部	頁次	2 / 4
文件名稱	資訊安全政策		實施日期	2023 年 11 月 27 日	

- 3.5 對於資訊安全事件須有妥善的通報及應變措施，以確保資訊系統及重要業務的持續運作。(參閱：[AD08 資通安全事件通報與應變機制](#))
- 3.6 進行資訊處理時，若含有個人資料，應依據「個人資料保護法」及相關規定審慎處理，不私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。
- 3.8 領取使用者代碼後應立即自行設定密碼，密碼長度至少應有 8 位數字元組成；密碼複雜度設定至少需由英文、數字或特殊符號的其中二個組成；使用者不得將自己的使用者代碼與密碼交付他人使用。
- 3.9 重要系統之使用者密碼有效期限應設為 90 天。
- 3.11 本公司主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。
- 3.12 依角色及職能為基礎，針對不同層級人員，依據實際需要辦理資訊安全教育訓練及宣導，促使全體人員瞭解資訊安全的重要性，各種可能的安全風險，以提高資訊安全意識並熟悉工作中之資訊安全職責，促其遵守資訊安全規定。
- 3.13 應使用具合法版權軟體，避免上網下載來路不明之軟體。
- 3.14 委外廠商應遵循本政策以及相關程序之規定，不得未經授權使用或濫用本公司之各類資訊資產，若涉及限制使用等級以上業務，應簽署保密切結書。
- 3.15 違反本政策與本公司之資訊安全相關規範，依相關法規或懲戒規定辦理。

4、審查與宣導

- 4.1 為確保資訊安全管理制度實務運作之可用性、安全性及有效性。本政策應依業務變動、技術發展或配合政府資訊安全管理要求、法令、技術及最新業務發展現況，每年至少評估或修訂一次。
- 4.2 本政策得以書面、電子郵件 (E-MAIL)、公告於網站、或其他方式公告周知。

5、資訊作業規定

- 5.1 加強員工資訊安全育訓練，防範不法事件、系統入侵破壞及電腦病毒，使業務能永續運作。
- 5.2 發生資訊安全事件務必通報資訊單位，依權責處理。
- 5.3 各部門單位應定期協同資訊室評估、檢測各項軟、硬體設備。
- 5.4 嚴禁安裝非業務上使用及非正版軟體(免費軟體之安裝使用需依專案申請)。
- 5.5 各單位從業人員使用之電腦嚴禁放置未授權軟體及有著作權影片音樂。
- 5.6 維護安裝資訊設備之軟硬體，皆需使用資訊設備「資訊服務申請單」報修，若緊急情況狀況可先處理，惟事後補上「資訊服務申請單」。
- 5.7 「資訊服務申請單」皆需單位主管簽核後才能執行。

富威電力股份有限公司		文件編號	AD02-02	版本	2.0
		制訂部門	資訊部	頁次	3 / 4
文件名稱	資訊安全政策		實施日期	2023 年 11 月 27 日	

- 5.8 各單位資訊相關設備維護每年底統計報表，審核資訊設備使用狀況，異常狀況者該資訊設備使用者皆需提報日常使用狀況報告。
- 5.9 資訊室應負責不定期督導資訊安全使用管理事項。
- 5.10 資訊系統擁有者或管理者，應負責資訊安全責任。
- 5.11 資料及資訊系統之需求及使用管理保護事項，由資訊單位負責辦理。
- 5.12 資訊機密維護管理事項，由資訊單位辦理。
- 5.13 稽核單位得調閱各系統內有關資料，實地測試或檢查資訊軟硬體設備使用情形，由負責人員提供說明並將缺失簽報予權責主管。
- 5.14 各單位之作業人員應與合約廠商保持密切聯繫，以便在發生資訊安全事件時，能迅速獲得協助解決。
- 5.15 系統及裝備設置及使用，應經資訊單位核准始得使用。
- 5.16 系統及設備停用、報銷應經資訊單位核准。
- 5.17 各部門主管應負督導所屬員工之資訊作業安全，防範不法及不當行為。
- 5.18 不定期對員工進行資訊安全教育訓練，使其瞭解資訊安全重要性，遵守資訊安全規定。
- 5.19 硬體設備不得任意擅自變更使用人及置放地點，若因公務所需者，請填具「資產異動申請單」，並呈權責主管核准。
- 5.20 未經申請許可勿擅自自行安裝移除硬體設備。
- 5.21 各單位從業人員必須採行事前預防及保護措施，偵測及防制電腦病毒以保系統正常運作。
- 5.22 嚴禁任何人與公司內部任一台電腦上自行安裝軟體(不管有無版權一律禁止)，若經查獲，爾後發生之相關法律責任由該安裝人員或是該電腦設備使用者負責之。
- 5.23 所有利用網際網路傳送資料者，應評估可能之安全風險，確定資料傳輸具完整性、機密性等安全需求，並對資料傳輸撥接線路，網路線路與設備等事項，妥適的採取安全控管措施，並承擔所有產生之風險責任。
- 5.24 機密資料及文件未經加密處理妥善，不得以電子郵件傳送。
- 5.25 各單位應於人員上線前，訂定使用單位及使用人員之系統存取權限，並予書面紀錄。
- 5.26 使用者調整職務或離職時，應儘速依調整結果調整或註銷系統存取權限。
- 5.27 若使用者認為個人鑑別身分資料有被竊取之虞，得呈報修改。
- 5.28 資料委託廠商建檔，均應採取必要之安全管制措施，防止資料被竊、竄改、販售或洩漏等情事發生。

富威電力股份有限公司		文件編號	AD02-02	版本	2.0
		制訂部門	資訊部	頁次	4 / 4
文件名稱	資訊安全政策		實施日期	2023 年 11 月 27 日	

5.29 禁止未登記授權之外接式儲存設備連接廠內資訊設備。隨身碟及外接式硬碟相關可攜式儲存設備，皆須管制登記並經核可後，始可放行使用，且未經許可，嚴禁傳輸儲存公司資產檔案及著作至設備內攜帶出廠，違反相關規定者，依公司規章報請懲處。

5.30 任何系統變更作業，皆應獲得權主管之同意。

5.31 員工除非獲得正式的授權，任何人皆不得進行系統存取。

5.32 電腦設備、資料軟體，嚴禁帶離辦公室或藉任何方式外流。

5.33 嚴禁於廠內上班或非工作時間內以任何方式經由網際網路上傳下載，非公司業務範圍內及有違著作權相關之檔案。

5.34 非業務上需求，嚴禁使用通訊軟體，(如 msn、yahoo 即時通等)需使用者皆須經由單位主管核准使用，資訊單位將監控使用者使用記錄。

5.35 系統之使用者密碼應定期更改。

5.36 公司應定期審核帳號與權限之建立、修改、啟用、禁用及刪除狀況。

5.37 與財務有關之重要系統之系統最高權限帳號、僅由權責人員管理。

5.38 與財務有關之重要系統主機之作業系統、資料庫最高權限僅授予權責相關之人員。

6、附則

6.1 制修廢與頒布實施

本規章屬管理規章，呈總經理核准並交權責單位頒布公告實施；修訂或廢止時亦同。

6.2 類別、名稱、編號、版次與發行(組織)、頁次及履歷紀要事項

本文件之類別、名稱、編號、版次與發行(組織)、頁次等，見本文件各頁之首頁與頁尾。

本文件之履歷紀要事項，如：權責單位、管制等及與版次、說明(修訂內容)、責任簽核、(發行)日期、其他備註等，見本文件首頁之「文件履歷紀要頁」。