

連宇股份有限公司	資訊安全政策	資料編號	3-003	版本	A
		生效日期	108年8月8日		
		制定部門	資訊部		
		頁次	第1頁；共4頁		

一、目的

連宇股份有限公司(以下簡稱本公司)對於營運產生所有形式的各類資訊，除致力於保障其機密性、完整性及可用性，更確保其免於被惡意或意外之入侵、破壞及洩露。資訊資產關係著本公司日常營運之持續，因此對於資訊資產，必須基於其重要性予以不同優先等級之保護，能夠有效運用資源，達到最大資訊安全效果，以配合本公司資訊安全工作的推行。

二、適用範圍

1、本公司全體員工、協力廠商及相關人員。

2、所有資訊資產，包括：硬體、資料、軟體、文件及人員。

(1) 資料：資料庫及資料檔案。

(2) 軟體：應用軟體、系統軟體、發展工具及公用程序等。

(3) 硬體：電腦及通訊設備及其它技術設施。

(4) 人員：本公司全體員工等。

(5) 文件：系統流程檔、使用者手冊、訓練教材、營運持續計畫、維護合約。

三、定義

1、資訊資產:係指維護本公司資訊業務正常運作之資料、軟體、硬體、人員及文件。

連宇股份有限公司	資訊安全政策	資料編號	3-003	版本	A
		生效日期	108年8月8日		
		制定部門	資訊部		
		頁次	第2頁；共4頁		

- 2、機密性:應建立適當安全機制，以確保資訊資產能被合法授權使用者取得。
- 3、完整性: 應建立適當安全機制，以確保資訊之輸入、讀取、儲存、處理及呈現等之正確性與完整性。
- 4、可用性: 所有資訊資產及資訊服務均能隨時可用。
- 5、可靠性: 應建立適當安全機制，以確保資訊資產及資訊服務之可靠性。
- 6、風險評估: 評估資訊安全性漏洞，對資訊處理設備帶來的威脅和影響，及其發生的可能性。
- 7、風險管理: 以可以接受的成本，確認、控制、排除可能影響資訊系統的安全風險或將其帶來的危害最小化的過程。
- 8、業務持續運作之資訊環境: 係指為維持本公司各項業務正常運作所需之電腦作業環境。

四、目標

- 1、防範資訊安全風險發生，減輕資訊安全事件發生之影響
- 2、保護本公司資訊內容，避免未經授權的存取修改，確保其正確完整性。
- 3、辦理資訊安全教育訓練，推廣員工資訊安全意識與強化相關責任之認知。
- 4、執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
- 5、提高資訊系統及設備之可用性，確保資訊系統正常運作。

連宇股份有限公司	資訊安全政策	資料編號	3-003	版本	A
		生效日期	108年8月8日		
		制定部門	資訊部		
		頁次	第3頁；共4頁		

五、責任

1、資訊部主管

負責統籌協調各相關部門，訂定並定期檢討及更新各項作業程序或資訊安全作業規範，以確實落實資訊安全政策。

2、各部門主管

負責所屬資訊資產監護之責任，確保其受到適當之保護。同時應督導日常作業中各項資訊安全規範、程序或機制之落實。

3、本公司相關人員

本公司員工、協力廠商、外包相關人員，應遵守本公司各項安全作業規範、程序及安全機制。所有相關人員應避免未經授權讀取或使用資訊資產之行為，並向資訊部主管通報任何資安洩密或違反規定情事。

4、任何危害資訊安全之行為，將視情節輕重依照「職工獎懲管理辦法」進行懲處，若有觸及法律責任將依照法律程序進行訴訟。

六、資訊安全政策維護

1、本公司訂定之資訊安全政策及相關作業規範、程序以及安全機制，應至少每年評估一次修改之必要，確保資訊安全實務作業之有效性及合理性。

2、為確保資訊安全政策之落實，由資訊部及其它相關部門一起配合，每年定期實施資訊安全稽核作業。

連宇股份有限公司	資訊安全政策	資料編號	3-003	版本	A
		生效日期	108年8月8日		
		制定部門	資訊部		
		頁次	第4頁；共4頁		

七、實施與修訂

本政策由資訊部制定，經呈董事長核准後實施，修訂時亦同。

本政策沿革：擬訂於民國108年7月23日，生效於民國108年8月8日。