昶虹國際(原億麗科技)股份有限公司

資訊安全政策

版　　本：V1.0
發行日期：109.05.08

1 目的

為確保本公司所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本公司之業務需求，訂定本政策。

2 範圍

2.1 本政策適用範圍為本公司之全體人員、委外服務廠商與訪客等。

2.2 資訊安全管理範疇涵蓋 14 項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本公司造成各種可能之風險及危害，各領域分述如下：

2.2.1 資訊安全政策訂定與評估。

2.2.2 資訊安全組織。

2.2.3 人力資源安全管理。

2.2.4 資訊資產管理。

2.2.5 存取控制安全管理。

2.2.6 密碼安全管理。

2.2.7 實體及環境安全管理。

2.2.8 運作安全管理。

2.2.9 通訊安全管理。

2.2.10 系統獲取、開發及維護安全管理。

2.2.11 供應商安全管理。

2.2.12 資訊安全事故管理。

2.2.13 營運持續管理之安全層面。

2.2.14 遵循性管理。

3 目標

為維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全，期藉由本公司全體同仁共同努力以達成下列目標：

3.1 保護本公司業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

3.2 保護本公司業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

3.3 建立本公司業務永續運作計畫，以確保本公司業務服務之持續運作。

3.4 確保本公司各項業務服務之執行須符合相關法令或法規之要求。

4 權責

4.1 本公司應成立資訊安全組織統籌資訊安全事項推動。

4.2 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。

4.3 本公司全體人員、委外服務廠商與訪客等皆應遵守本政策。

4.4 本公司全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

4.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行議處。

4.6 定期審查資訊安全目標之達成。

5 審查

5.1 本政策至少應每年評估一次，以反映相關法令、技術及業務等最新發展現況，確保維持營運和提供服務之能力。

5.2 本公司應考量內、外部議題及利害相關者要求，定訂適當之資訊安全管理制度實施範圍，經由管理階層審核、確認後實行。

5.3 資訊安全管理制度實施範圍應定期或不定期視內、外部環境之變更或執行狀況，如：法令法規之要求、組織異動、資安事件發生、管理制度落實狀況等因素，於管理審查會議進行檢視調整。

內部議題	外部議題	利害相關者	利害相關者要求	備註
組織政策、目標	主管機關要求	主管機關	各項法令、法規	
	政府單位要求	政府單位	各項法令、法規	
組織文化	N/A	內部人員	組織內部規範	
相關資源需求（包括：人力、技術、預算等）	N/A	內部人員	訓練	
		高階主管	績效（KPI）	
	資訊安全事件資訊技術	客戶	合約內容（SLA）	
		供應商	合約內容	
		第三方稽核單位		

6 實施

本政策核定得以書面、電子或其他方式通知同仁、與本公司連線作業之有關機關（構）及提供資訊服務之廠商，修正時亦同。