資訊安全政策

1.目的

叡揚資訊（以下簡稱本公司）為維護整體資訊安全，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性，並建立安全及可信賴之作業環境，確保資料安全、系統安全、設備安全、網路安全，保障本公司同仁與相關內、外部人員之權益，特訂定本政策。

2.範圍

本政策適用於本公司提供之內、外部資訊服務（包含雲服務），為避免因人為疏失、蓄意或天然災害等因素，導致資料(包含個人可識別資訊(Personally Identifiable Information,以下簡稱 PII））不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。

3.名詞定義

無。

4.目標

4.1 維護本公司提供之內、外部資訊服務（包含雲服務）機密性、完整性與可用性，包括：

4.1.1 保護本公司業務資訊，避免未經授權的存取。

4.1.2 保護本公司業務資訊，避免未經授權的修改，確保其正確完整。

4.1.3 建立資訊業務永續運作計畫，確保本公司業務之持續運作。

4.2 本公司之業務執行須符合相關法規之要求。

4.3 本公司執行資訊安全管理制度，期達以下量測指標：

4.3.1 基礎維運之服務可用率每年達 99.5%。

4.3.2 3、4 級資安事件造成關鍵業務資訊外洩、破壞、竄改等無法作業之事件，零發生。

4.3.3 違反外部法令法規（個人資料保護法、智慧財產相關法規、資通

安全管理法、營業祕密法等）事件，零發生。

4.3.4 各專案因違反合約之相關資安服務水準指標造成罰款事件，零發生。

5.原則

5.1 所有同仁應充分了解本政策之目的及其職責。

5.2 單位主管對於本政策及相關作業規範之遵循，應負監督、執行、稽核之職責。

5.3 資訊資產應定期盤點、分類分級，針對重要資訊資產進行風險評鑑，並據以實施適當的防護措施。

5.4 人員和委外廠商，均須依規定程序及指定措施辦理資訊業務。

5.5 人員及委外廠商應透過適當通報機制，報告資訊安全事件及資訊安全弱點。

5.6 任何危害資訊安全之行為人員，視情節輕重追究其民事、刑事及行政責任與相關懲處。

5.7 雲服務會將 PII 完整儲存於資料儲存系統中，並以嚴密的保護措施防止未經授權人員之接觸。

5.8 依據「IS-D-026 有效性量測表」，定期審查資訊安全管理制度之有效性。

6.審查

6.1 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。

6.2 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。

6.3 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、	主管機關要求	主管機關	各項法令、法規	

目標	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	
	管理制度	ISO 國際組織	ISO 9001 ISO 27001 CNS 27001	
		第三方稽核單位		
		財團法人全國認證基金會		

7.實施

本政策經資訊安全長核定後實施，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。

8.參考資料

無。