鑫傳國際多媒體科技股份有限公司暨所屬營運公司
資通安全暨個人資料管理系統資通安全管理政策

安全管理政策

為了促使本公司ISMS能貫徹執行、有效運作、監督管理、持續進行，維護本公司重要資通系統的機密性、完整性與可用性，特頒佈資通安全管理政策。本政策旨在讓同仁於日常工作時有一明確指導原則，所有同仁皆有義務積極參與推動資通安全管理政策，以確保本公司所有職員之資料、資通系統、設備及網路之安全維運，並期許全體同仁均能了解、實施與維持，以達資通持續營運的目標。

1. 落實資通安全，強化服務品質

   由全體同仁貫徹執行ISMS，所有資通作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資通安全制度的工作，強化服務品質，提升服務水準。

2. 加強資安訓練，確保持續營運

   督導全體同仁落實資通安全管理工作，每年持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全之重要性，促其遵守資通安全規定，藉此提高資通安全智能及緊急應變能力，降低資通安全風險，達持續營運之目標。

3. 做好緊急應變，迅速災害復原

   訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資通系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

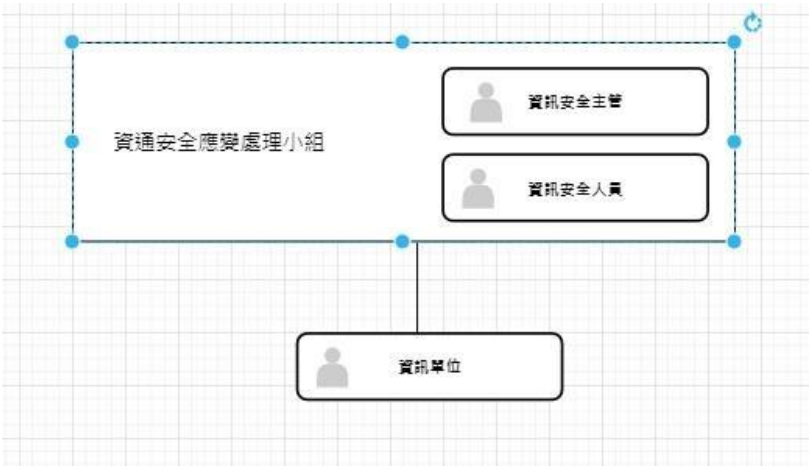
壹、目的

因應鑫傳國際多媒體科技股份有限公司(以下簡稱公司)強化資通安全防護及管理機制，並符合內控電腦化資訊系循環相關控制作業，特擬定本資通安全指引。(相關條文參照上市上櫃公司資通安全管控指引)。

貳、資通安全政策及推動組織

2.1 資通安全組織架構圖及權責

在「資通安全組織架構圖」中，各項職位之權責由「資通安全應變處理小組」負責其訂修廢內容之維護。



2.1.1 人員配置

資訊安全主管 1 名

資訊安全人員 1 名

資訊單位 1 名

2.1.2 資通安全管理單位權責

資訊安全主管

1. 協調資通安全責任之分配。

2. 監督資通安全防護措施之施行。

3. 進行資通安全事件之通報、應變及檢討

4. 訂定資訊安全管理相關規範。

資訊單位

1. 資訊安全狀況進行預警、監控，並對資訊安全狀況與事件進行處置。

2. 對資訊安全管理之改善提出建議，以及協助執行資訊安全之自我檢核。

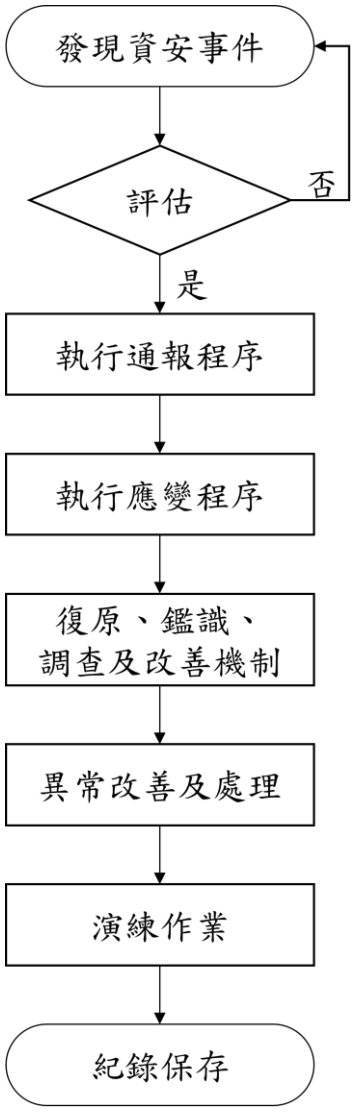
3. 存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

4. 建立資訊安全事件緊急應變暨復原措施。

5. 執行稽核改善建議事項、預防措施之改善。

資訊安全人員相關通報程序與文件記錄

資通安全事件通報及應變管理流程圖

作業流程	權責單位	相關表單
	發現人員 資通安全應變處理小組 單位主管 資訊安全人員 資訊單位 資訊單位 資訊單位 資訊單位 資訊安全人員	資通安全事件報告單 資通安全事件報告單 資通安全事件報告單 資通安全事件報告單 資通安全事件報告單 資通安全事件報告單

2.1.3 資通安全事件通報責任

1. 本公司所有員工與委外廠商人員於資通安全事件發生時，應依據相關通報程序，通知相關負責人員。

2. 本公司員工若發現資通系統可疑的弱點或可能對資通系統造成傷害的威脅時，應向「資通安全應變處理小組」通報。

3. 當資通安全事件發生且涉及法律時，須由「資通安全執行小組」配 合警調單位進行蒐證。

2.2 安全管理政策

為了促使本公司能貫徹執行、有效運作、監督管理、持續進行，維護本公司重要資通系統的機密性、完整性與可用性，特頒佈資通安全檢查指引。本指引旨在讓同仁於日常工作時有一明確指導原則，所有同仁皆有義務積極參與推動資通安全管理政策，以確保本公司所有職員之資料、資通系統、設備及網路之安全維運，並期許全體同仁均能了解、實施與維持，以達資通持續營運的目標。

2.3 落實資通安全，強化服務品質

由全體同仁貫徹執行，所有資通作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資通安全制度的工作，強化服務品質，提升服務水準。

2.4 加強資安訓練，確保持續營運

督導全體同仁落實資通安全管理工作，每年持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全之重要性，促其遵守資通安全規定，藉此提高資通安全智能及緊急應變能

力，降低資通安全風險，達持續營運之目標。

2.5 做好緊急應變，迅速災害復原

訂定重要資訊資產之風險評估及災害復原計畫，並定期執行各項緊急應變流程、以確保系統失效或重大災害發生時，能迅速復原，確保系統持續運作，降低其損失。

2.6 人員教育訓練之管理

所有使用資訊系統之人員，每年接受資訊安全宣導課程，另負責資 訊安全之主管及人員，每年接受資訊安全專業課程訓練。

三 核心業務及其重要性

3.1 定期檢視公司相關核心業務及機敏性資料。

3.2 遵循相關之法令規定

3.3 訂出核 心業務之復原時間目標(RTO)及資料復原時間點目標(RPO)，降低其營運中斷事件機率及影響程度，設置適 當之備份機制。

3.4 針對業務持續演練計畫，定期施作讓相關人員熟悉運作程序，了解相關人員職責相關與資源調配。

四、資通系統盤點及風險評估

4.1 建立核心系統相關資產清冊與盤點。

4.2 針對核心系統鑑別其資安風險，並分析機密性、完整性及可用性之風險衝擊，完成資通安全風險評估。

五、資通系統發展及維護安全

5.1 針對核心資通系統定期辦理弱點掃描，滲透測試。

5.2 將資安要求納入資通系統開發及維護需求規格，並妥善保管相關之文件。