皇翔建設股份有限公司

資通安全管理之資訊揭露

一、資通安全風險管理架構

皇翔建設股份有限公司(以下簡稱本公司)資通安全之權責單位為資訊組，該組設置資訊主管一名負責擔任督導及統籌目前已執行之各項資訊安全政策之查核、檢視，並依據當前資安方向配合策略調整，確保資訊安全管理系統持續運作的適用性、適切性及有效性。另本公司已依法令規定設置資訊安全專責主管，並視實際情況及需要定期及不定期向本公司董事長或總經理報告。

稽核室依據「公開發行公司建立內部控制制度處理準則」之規定，將「電子計算機循環」納入年度稽核計畫，查核資通安全檢查之相關控制是否有效且落實執行。倘若有發現缺失/風險，即請受查單位及協同單位進行檢討，提出具體改善計畫及時程，定期追蹤改善進度，以落實公司資通安全政策。

二、資通安全政策：

本公司為強化資訊安全管理並維護資訊作業相關人員、資料、資訊系統、設備及網路安全運作，特訂定資通安全政策（以下簡稱本政策）。本政策涵蓋本公司及子公司，是以「一、建立符合法規與客戶需求之資訊安全管理規範；二、透過全員認知，達成資訊安全人人有責的共識；三、保護公司與客戶資訊的機密性、完整性與可用性；四、提供安全的工作環境，確保公司業務之永續營運」為指導準則。並以防毒、防駭、防漏三大資安防護主軸為目標，建立防火牆、入侵偵測、防毒系統及諸多內控系統，以提升公司在防禦外部攻擊以及確保內部機密資訊防護的能力。

三、資訊安全管理標的：

本政策所述資訊之安全，係指為保護本公司資訊及資訊系統避免受未經授權的進入、使用、破壞、修改及資料刪除等，維持現有資訊系統的可用性。並持續建構多層次資安防護系統，持續導入資安管控技術，經由多層次資安防護，強化資訊安全及網路安全保護流程，以維護公司資產防護。

強化內部電腦設備資訊安全系統查檢，並檢討及持續改善，當員工違反資安相關規範及程序時，依據規範進行告知及改善，並程序進行全員資安教育訓練已提升資安意識。

四、具體執行措施：

i. 教育訓練：

a. 公司資訊人員必須至少一人完成”ISO 27001：資訊安全管理系統主導稽核員訓練課程”，並取得上課證明。

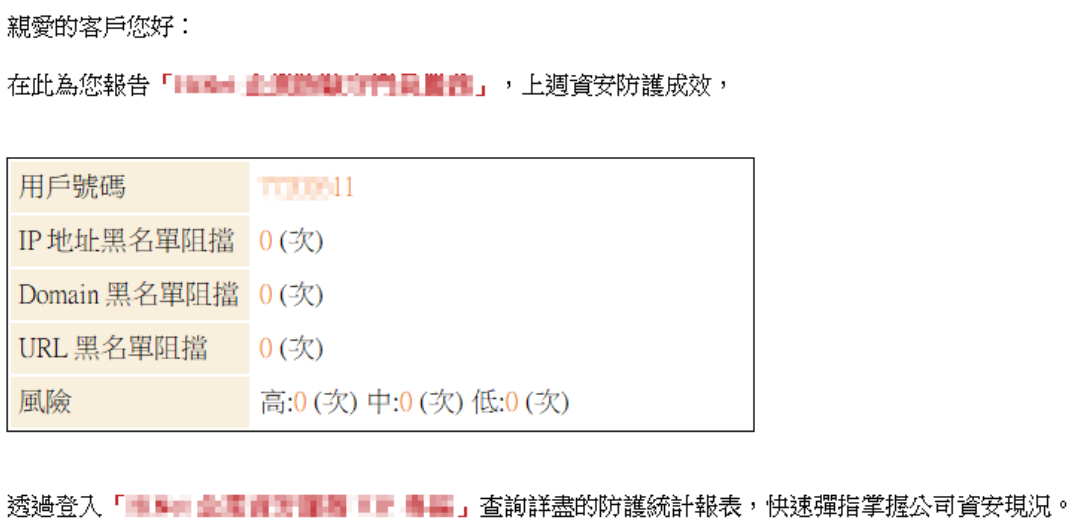
b. 所有新進同仁皆須完成”資訊安全說明教育訓練”課程。

ii. 資訊系統防禦／外部威脅：

防範外部駭客入侵與電腦病毒威脅，除建置防火牆、防毒等資通安全系統外，亦搭配大型網路公司之先進網路防禦系統服務，針對外部攻擊項目進行分析調整防火牆相關條例

a. 網路攻擊監測：

透由大型網路廠商，提供每日資訊安全問題及時通報，並於每週提供檢測報告。



親愛的客戶您好：

在此為您報告「[redacted]」，上週資安防護成效，

用戶號碼	[redacted]11
IP 地址黑名單阻擋	0 (次)
Domain 黑名單阻擋	0 (次)
URL 黑名單阻擋	0 (次)
風險	高:0 (次) 中:0 (次) 低:0 (次)

透過登入「[redacted]」查詢詳盡的防護統計報表，快速彈指掌握公司資安現況。

b. 雙層式防火牆架構：

透由防火牆主機內部之七層架構防護方式，進行網路連線管控及管制，阻礙特殊網站連結開啟、各大知名網頁郵件系統操作，降低網路連線產生之風險行為控管。

c. 郵件過濾／稽核系統：建立郵件稽核系統架構，針對進出郵件進行全過濾，可有效防堵垃圾郵件以及特殊病毒信件的流入，有效降低使用人員電腦設備中毒情況，每年中毒通報件數＜2 件。

d. 防毒系統：建置雙防毒系統軟體，同仁發現異常郵件進入，可透由資安人員協助，透由不同防毒系統進行掃描判斷，降低人員中毒風險。

iii. 門禁系統管制：

機房及資訊室透由門禁系統管制，非授權人員一律無法進入。以達到人員管制目的。

iv. 權限管理／系統存取管制：

新進人員依據所屬部門設定資料權限，並以最小權限原則管理內部系統與資料之存取權限，人員無法使用非經授權之系統功能，亦無法檢視非職務所需之系統資料。若需求其他專案權限，需透由申請機制進行申請後開放。

軟體系統程式建立為強化系統存取控管機制，透過多層式網路架構管理不同用途之系統、限制外部存取權限。

v. 系統可用性：

保內部系統運作之穩定性，和縮短系統異常之服務中斷時間，透由資料儲存陰影複製功能，保存每日資料。並每日進行資料庫備份程序，保存

系統資料庫資料。此外，亦根據資訊系統重要程度建立相應之備份備援機制、 資料異地備援，定期執行資料還原測試，確保備援機制運作正常。

五、資訊安全之目標，係為確保本公司資訊的合法存取，於可能遭受外力入侵時，亦能提供完整、未中斷之資訊系統運作；於事故發生時，作迅速必要之應變處置後，能在最短時間內回復正常運作，以降低該事故可能帶來之損害。透由上述之各項管制措施，藉以達到資訊安全目標。