資通安全管理

資通安全管理

112/12

(一)資通安全組織架構

本公司於民國 110 年設立「資訊安全小組」，隸屬企業永續發展小組管轄下，由資訊處及各子公司高階主管組成，統籌資訊安全及保護等相關政策之制定、執行、風險管理與遵循度查核，並定期向董事會及審計委員會彙報資安管理成效、資安相關議題及運作情形，而審計委員會就其執行成果提出建議，並提報董事會。

(二)資通安全政策與運作

1.資訊安全政策

資訊安全組織為有效落實資安管理，每季依據規畫、執行、查核與行動（PDCA）等階段的管理循環機制，檢視資訊安全政策適用性與保護措施。

「規畫階段」著重資安風險管理，建立完整的資訊安全管理辦法，從系統面、技術面、程序面降低企業資安威脅，建立符合需求、最高規格的機密資訊保護服務。

「執行階段」則建構多層資安防護，持續導入資安防禦創新技術，將資安控管機制整合內化於軟硬體維運、資安管理等平日作業流程，系統化監控資訊安全，維護公司重要資產的機密性、完整性及可用性。

「查核階段」積極監控資安管理成效，每年經由公司內部稽核單位及外部會計師進行查核，並將查核結果呈報董事會。

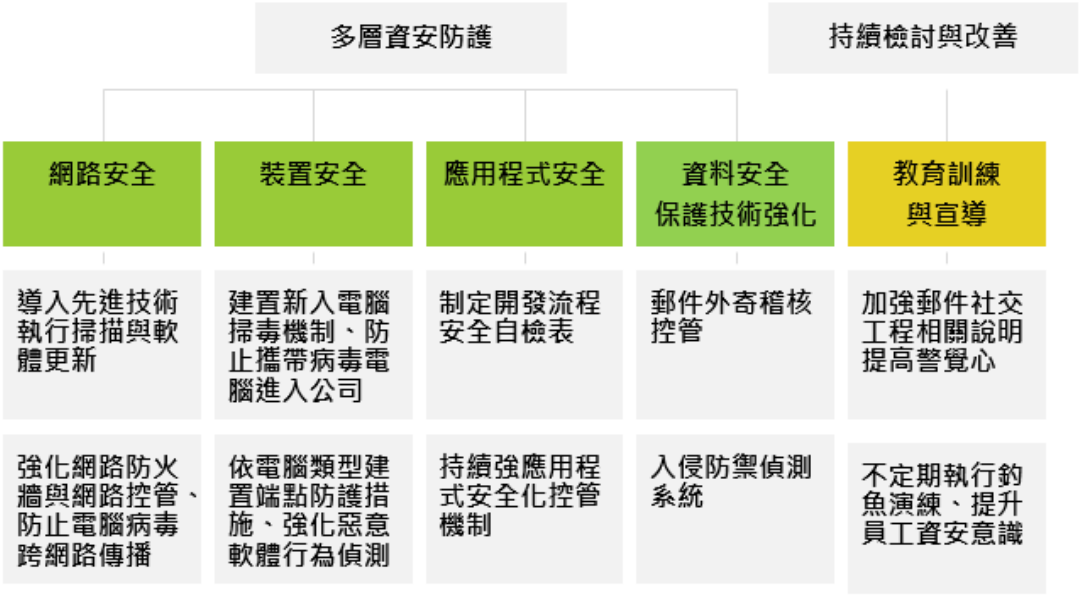
「行動階段」則以檢討與持續改善為本，落實監督、稽核確保資安規範持續有效；定期檢討及執行包含資訊安全措施、教育訓練及資安宣導等改善作為，確保公司重要機密資訊不外洩。

2.資訊安全運作

本公司 111 年已依據金管會發布之「公開發行公司建立內部控制制度處理準則」第 9 條之 1 規定，指派資安主管及 1 名資安人員。依據「上市櫃公司資通安全管控指引」定期檢討制定資安政策，並加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊，以強化公司資安措施。

資安風險管理架構

3.具體管理方案



(三)資通安全風險與因應措施

1.資訊技術安全之風險及管理措施

公司已建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司營運及報表等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。這些網路攻擊以非法方式入侵公司的內部網路系統，進行破壞公司的日常營運活動，而公司在遭受嚴重網路攻擊的情況下，系統可能會失去公司重要的資料，相關服務也可能因此停擺，進而造成公司重大損害，甚至嚴重影響公司商譽。

公司透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性，但不能保證在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取營業祕密及其他機密資訊，例如客戶或其他利害關係人的專有資訊以及公司員工的個資。也可能使公司因涉入對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。有鑑於此，本公司透過三個面向因應之：

(1)「教育面」: 在會議、教育訓練等各種場合不斷的進行資安宣導，提高同仁資安意識，於 112 年進行網路及資安防禦研討會 36 人次、資訊安全及個人資料保護法宣導 734 人次、社交工程演練訓練 137 人次、新人訓練營-資訊安全 87 人次，並每年針對資安人員進行專業教育訓練。

(2)「制度面」: 成立跨部門資安小組，保護資源分享的安全，訂定資安相關規範。

(3)「技術面」: 依照需保護的資料敏感程度，評估導入適當之解決方案。