晟德資訊安全風險管理架構

一、資訊安全政策

資訊安全管理制度遵循說明：

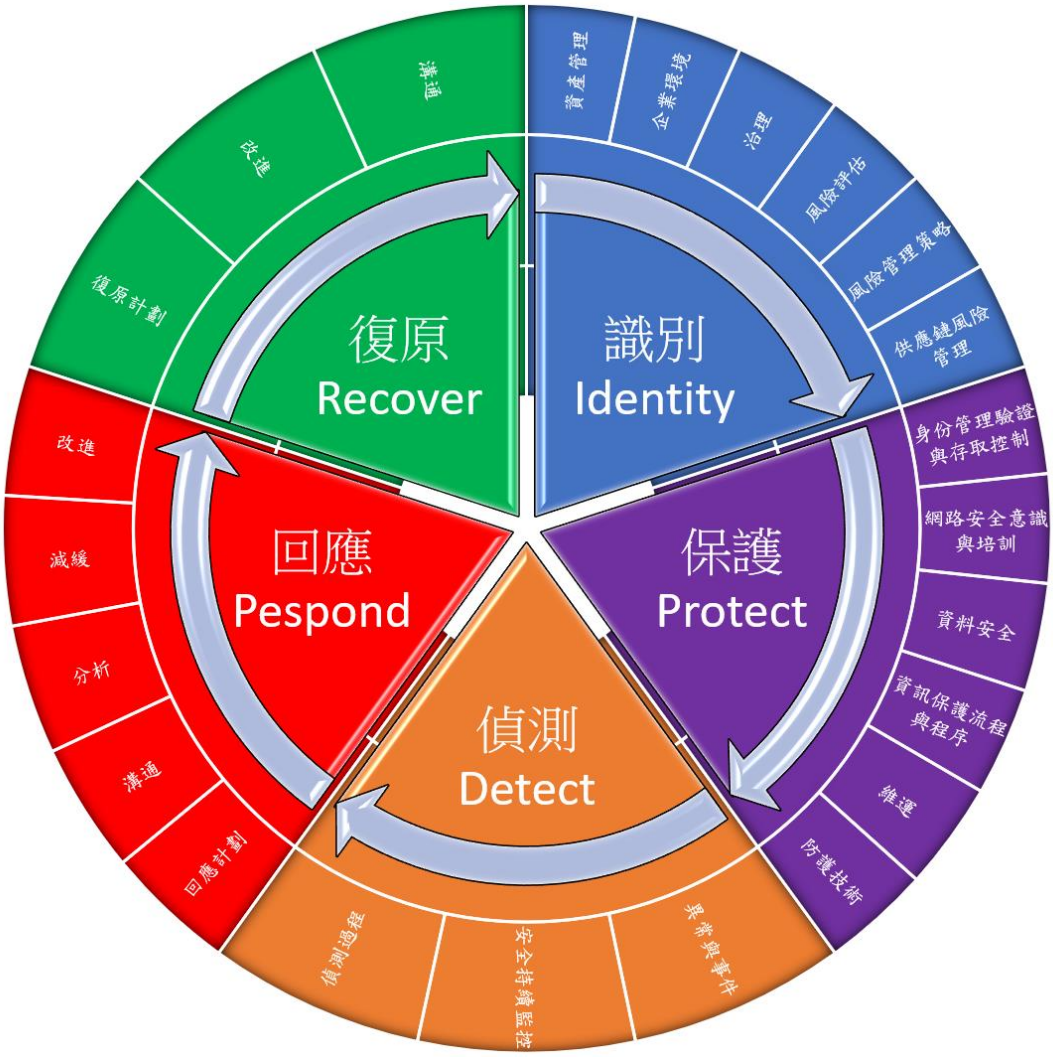
1. 本公司依「公開發行公司建立內部控制度處理準則」第九條「電腦化資訊系統處理」之規定制定相關內部作業規定，以降低新興資訊科技應用以及環境變遷所帶來未知的資安威脅風險。
2. 晟德集團持續對資訊安全完備其治理制度與提升防禦能力，各項資訊作業不僅須符合資安標準流程外，更要符合資訊安全法令法規。
3. 自 2018 年起依循集團【資訊安全發展藍圖】逐步精進，並於 2019 年完成【資安風險內控管理措施】規劃發布，深刻落實資訊安全風險管理。

<資訊安全管理組成結構及資訊安全發展藍圖>

二、資訊安全風險管理架構

為掌握資訊安全風險管理，晟德集團採用 NIST 來對應及預防風險事件發生：

1. 識別：定期自主盤點檢驗，從資產管理、企業環境、治理、風險評估、風險管理策略、供應鏈風險管理著手，主動預防資安事故。
2. 保護:從身份管理驗證與存取控制、網路安全意識與培訓、資料安全、資訊保護流程與程序、維運、防護技術，保護集團，防禦來自內外網攻擊，侵入資訊系統造成破壞，防範公司機敏資訊及營業秘密遭外流外洩，影響晟德永續營運，預防環境內因素（故障/跳電／病毒／設備遺失）造成的生產損失。
3. 偵測、回應、復原：對異常事件偵測過程和安全持續監控記錄，針對異常事件的提出回應計劃，充分溝通並分析原因，減緩異常事件的損害及提出改進和復原計劃，提高系統可靠性



三、具體管理方案

1、本集團資訊系統採雙網路主幹、系統負載平衡及異地備份架構，營運中心設於台北，並於新竹設置災害還原備份中心，兩地間以高速光纖網路連結；營運主機採用 IBM X3650M4 HA 架構，備份主機則為 Synology RS2418 NAS 網路儲存伺服器，建置有異地備份主機機制，每一年辦理災害還原演練。

2、為持續強化本集團資訊安全並善盡保護客戶個人資料之企業責任，除針對各式資訊風險導入管控工具加強管理措施，如：裝置管理、硬體防護、應用系統安全監控、上網及行動安全等，每年定期完成技術面與管理面相關檢核措施，以改善並提升網路、資訊系統安全防護能力及資訊治理水準。此外，為因應網路威脅的數量和複雜程度不斷增加，及新興科技應用所帶來的資訊風險，資訊部落實郵件白名單機制及無線網路實名制連線機制，以強化本集團網路安全環境；另以風險導向的角度，針對資訊安全風險管理、威脅情資管理、資訊安全控管、委外及依賴關係管理、資安事件管理與回應等面向，定期確認營運整體風險，以維持網路安全強度。

3、為強化防範及降低惡意入侵攻擊風險，影響客戶權益，已完成網路流量管理系統建置，可主動系統連線狀態。將分階段進行「安全性資訊和事件管理系統」建置及提昇「弱點掃描系統」，強化資安防護能力。此外，為確保業務運作之穩定、安全，將持續調整系統架構、加強基礎建設、改寫應用系統及擬訂並演練緊急應變計畫。已完成內外防火牆提昇、雙中心核心交換器提昇、雙中心 VPN 架構提昇、VPN 連線系統提昇、備份平台升級建置、異地備份機制。