志聯工業(股)公司 資通安全政策

一、目的

強化資訊風險管理，建立安全之電腦化作業環境，確保公司資訊系統正常營運。

二、組織與權責

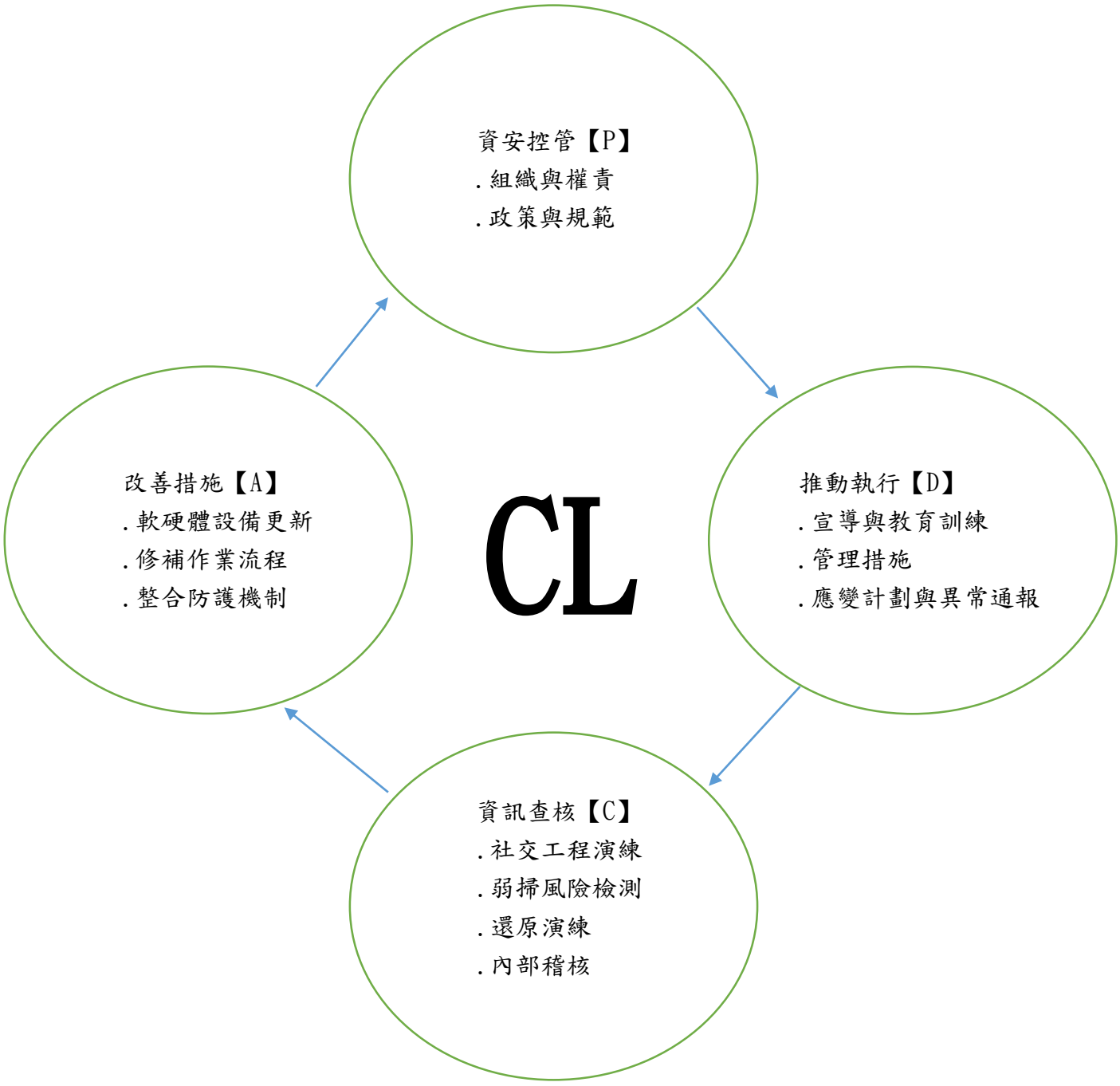
・單位：資訊室

・資訊室負責統籌規劃公司資通安全政策之計畫、研議、建置與評估等事項。

・資訊系統之安全需求提出、妥善保管、應用等事項，由資訊室與相關部門負責辦理。

・資通安全稽核事項由稽核室執行監督與督導。

三、資安架構（PDCA）



四、資通安全目標

・確保公司資安作業之正確性、可用性與機敏性。
・增強員工資安意識與法令觀念。
・避免資安事件發生。
・資安事件發生時能迅速應變，且在最短時間內回復正常運作，降低損失。
・執行符合相關法令、法規之要求。

五、資通安全管理措施

・系統使用管理：使用者有各自帳密登入系統，並依職責設置存取權限。
・密碼管理：使用者帳號、個人電腦、伺服器皆設定密碼，並定期更新密碼。
・智慧財產權：尊重智慧財產權，公司安裝軟體皆有合法授權。
・架設防火牆：各項網路服務之使用，應依據網路規則執行。
・防毒軟體：自動更新病毒碼，降低病毒感染機會。
・作業系統更新：自動掃描與不定期更新作業系統，修補高風險與安全性漏洞。
・郵件安全管控：郵件過濾、防毒軟體掃描、垃圾郵件管理。
・資料備份：重要資料備份與異地備援機制，確認備份資料之正確性及有效性。
・災害復原計畫：不定期舉辦核心業務系統演練，以利資安事件發生時能快速恢復正常運作。
・教育訓練：資安宣導公告與上課，強化同仁資安認知與法令觀念。
・電腦機房規劃：建立資訊設備在以安全、穩定的環境下運作。

六、緊急應變計畫與通報機制

・事件通報：確認發生資通安全事件，應須先通報相關單位主管與資訊室。
・抑制損害範圍擴散：資訊系統與機器設備應先進行初步處理，查證受損害之真實性，確認損害範圍與阻止損害擴散，評估立即斷網與關閉設備等措施，並同時聯繫委外廠商到場處理。
・進行事件調查與證據留存蒐集程序：凡因遭外力入侵導致資通安全事件，應即請委外廠商協助進行現場事件調查，並於調查過程留存紀錄。
・系統設備恢復服務程序：系統若無法於可容忍中斷時間內正常提供服務，應準備啟動備援方案以維護公司系統正常營運。
・資安事件發生，通報單位主管與資訊室，詳實紀錄事件發生過程與數據，並於後續進行檢討與改善計畫。

七、資通安全之資源投入

・制定公司資通安全政策。
・網路斷線運作機制與設備測試。
・資訊設備之軟體、硬體、韌體更新與升級。
・社交工程演練。
・弱點掃描與安全性更新。
・資安宣導公告。
・員工資安教育訓練。
・資訊系統(核心作業)回復演練，確認流程機制與資料正確性。
・電腦機房環境(溫濕度、電力等)改善。