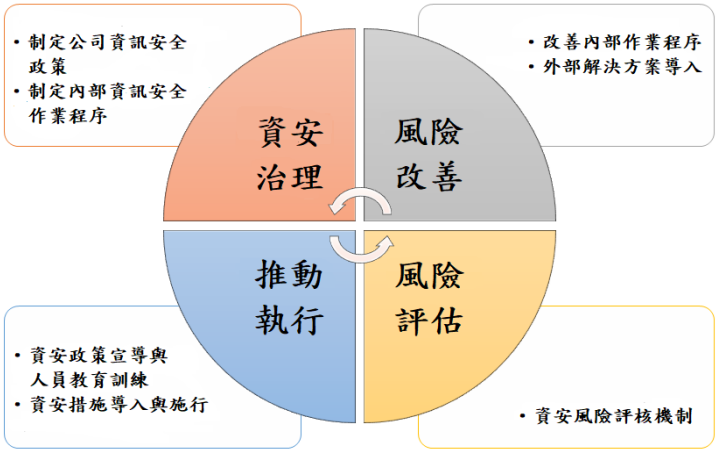
達亞國際股份有限公司

資通安全管理政策及執行情形

1. 資訊安全管理架構：

1. 本公司由管理部召集成立跨部門資訊安全管理小組，資訊與行政管理單位負責主導及規劃，各業務相關單位配合執行，定期召開會議檢討執行情形，並每年定期向董事會報告執行情形。
2. 資訊安全管理小組負責制定資訊安全管理政策，定期檢討修正。

2. 資訊安全風險管理步驟：



3. 管制措施：

類型	相關措施
權限管理	人員帳號之系統權限設定，需填寫申請單經權責主管核准後由資訊人員設定
	人員職務異動時，依其職務內容確認並調整帳號之存取權限
	人員離職時，資訊人員依離職手續單之核准內容，辦理離職人員電腦之資訊保存或清除
存取管控	公司存有機敏資料之電腦設備皆設定帳號密碼管理，無權限之人員帳號無法存取無權限之資料夾
	非經申請允許，個人電腦禁止使用 USB 儲存裝置
	設置使用者個人密碼，禁止個人密碼交付他人使用
	非資訊安全管制人員，非經許可，不得進出主機房
外部威脅	對外網路連接之設備皆設置防毒軟體，防止駭客或電腦病毒
	員工不得私自安裝電腦軟體
	架設防火牆過濾與控管 Telnet、FTP、WWW 等網路服務
系統可用性	定期備份重要軟體及其文件、清冊等媒體記錄，異地存於安全場所保管

達亞國際股份有限公司

資通安全管理政策及執行情形

類型	相關措施
	系統復原計畫至少一年執行一次，並將執行紀錄結果呈交單位主管簽核
	配置足量之不斷電系統，預防停電造成系統損壞及資料遺失

4. 目標：

1. 維持各資訊系統持續運作
2. 防止駭客、各種病毒入侵及破壞
3. 防止人為意圖不當及不法使用
4. 防止機敏資料外洩
5. 維護實體環境安全

5. 資訊安全審查：

為反映相關法令法規、科技變化、客戶期望、業務活動、內部環境與資源等最新現況，公司資訊單位於每年執行下列內部稽核活動：

1. 發送各單位系統權限表並要求各單位查核確認回報。
2. 檢視備份備援等資料存放是否異常。
3. 執行資訊安全風險評估，修正公司資訊安全政策。
4. 執行各資訊系統復原計劃測試。
5. 執行弱點掃瞄安全檢測軟體，進行系統安全檢核與弱點掃瞄工作。

另因應突發性資安事件，辦理專案稽核計畫，以確保公司資訊安全作業之有效性

6. 持續改善：

檢討資訊安全稽核及健檢各不符合事項，並採取有效改善對策，落實預防改善措施，以確保公司各項業務恪遵相關資安規範，維持資安管理制度正常運作。

7. 執行情形：

1. 本公司業已於民國 110 年 10 月 25 日向董事會報告資訊安全風險管理運作情形，當年度並無危害本公司資訊安全事件。
2. 本公司於新進同仁報到後進行資訊安全之教育訓練，本年度共計 51 人次進行 0.5 小時「資訊系統維護管理程序」之教育訓練。

3. 本年度分別於民國 110 年 11 月 16 日、民國 110 年 11 月 17 日、民國 110 年 11 月 18 日及民國 110 年 11 月 19 日辦理六梯次資訊安全教育訓練，經理人及員工共計 129 人次進行 0.5 小時「淺談網路安全演變與防範」之教育訓練。