德鴻科技股份有限公司_資通安全管理政策

資料來源：113 年度年報

(一) 資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源如下:

1. 風險管理架構

本公司由資訊部設置專責資安主管與資安人員針對資訊安全之防駭、防毒、防災進行規劃，制定公司資安政策與因應措施，執行相關資安作業，定期彙整提供稽核進行查核，如需改善，由資訊部提出改善計畫並進行改善與追蹤。

2. 資通安全政策

本公司之資安政策為『持續保護、強化應變、自動偵測、快速復原』，根據此政策制定相關資安管理辦法，並根據實際狀況隨時修正管理辦法與目標以達成完善之資通安全目標。

3. 本年度之資通安全目標為

(a) 資通系統操作人員，需接受全體參加之資通安全教育訓練，本年度預計於第一季完成。

(b) 資訊安全主管及負責人員，需接受資通安全專業教育訓練，每人每年執行 8 小時 ，本年度預計於第三季前完成。

(c) 對外服務之核心資通系統，需執行弱點掃描，每月自動執行乙次，並於執行後三個月內將高風險弱點 100%完成控制。

(d) 本公司郵件服務之使用人員，需接受郵件社交工程演練，每年執行乙次，並對開啟連結、輸入資料人員實施教育訓練，本年度預計於第三季前完成。

(e) 本公司若發生資安事件，應於規定的時間完成通報、應變及復原作業，並每年完成一次災備演練，本年度預計於第三季完成。

4. 資通安全原則

(1) 資料存取控管

員工所使用系統帳號及其所設定密碼應符合系統複雜度原則，並定期更新密碼，並依職能設定各系統權限以作為有效控管機制、製作檢核表以記錄各系統設備問題處理...等，並妥善進行特權帳號之管理，以維護核心系統之安全。

(2) 設備安全

(a) 設備機房得設置溫度控制、異常警告等相關安全監控措施並應考量地震、火災等不可抗力事故發生時之緊急應變措施。

(b) 公司配屬電腦設備皆應安裝防毒軟體，並維持最新病毒碼，並限制外部裝置之使用。

(c) 禁止使用未經授權軟體，員工內部電腦軟體統一由資訊部監控，並依工作型態配置預設軟體。

(d) 重要設備建置 UPS 以確保不會因為瞬間斷電造成設備損失。

(e) 建置 SIEM、ITAM 等資安與資產資訊監控系統，隨時監控系統紀錄與狀態，預防資安事件之發生。

(f) 定期進行設備之弱點掃描工作，確保相關設備之安全性。

(3) 宣導及檢核

(a) 隨時宣導資訊安全資訊，並每年進行一次全員資通安全政策宣導事宜。

(b) 每年進行至少一次社交工程演練以養成同仁資安意識。

(c) 每年至少進行一次業務持續運作演練，確保核心設備之持續運作能力。

(d) 定期內外稽、並由稽核人員報告董事會。

5. 具體管理方案

(a) 於公司內部控制制度之電腦資訊循環中訂有資通安全檢查之控制作業，作為同仁遵行依據，同時不定期檢討內控制度之有效性，進一步強化及落實。

(b) 加入TWCERT等組織，隨時取得最新弱點資訊並評估是否會有設備受到安全漏洞之影響。

(c) 持續建置資訊安全管理系統(ISMS)，強化資安防禦機制。

(d) 稽核人員每年對公司資訊安全管理進行稽查，以了解資安運作狀況，評估對各項風險控制及異常事項之改善是否確實，以降低及避免相關資安風險。

(e) 持續要求相關人員進行資通安全相關訓練，持續強化自身防禦能力。

6. 投入資通安全管理之資源

(a) 網路硬體設備：防火牆、AD 網域控制站、NAS 備份系統與相關服務之硬體設備等。

(b) 建置相關資安監控機制，隨時監控電腦設備的狀況以預先預防並即時處理可能的資安問題。

(c) 投入人力：每日各系統狀態檢查、定期備份及備份媒體異地存放之執行、每年系統災難復原執行演練、資訊人員不定時進行資安課程進修，新進人員皆須簽定資通安全保密協定。

(二) 最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實:

本公司平時即重視資通安全，最近兩年度及截至公開發行說明書刊印日止無重大資通安全事件。