聯傑國際股份有限公司

資通安全管理

一、資通安全風險管理架構與政策：

1、聯傑國際以打造嚴謹有效的資通安全防禦網為資安治理願景，公司指派資訊管理部負責資通安全的專責單位，董事會由 112 年 11 月 9 日通過由資訊管理部門主管-馬中天擔任資訊安全主管。以資安治理一致性為基礎，逐步提升全方位防護能力，以成為資安治理成熟度表現傑出之企業為目標。

2、資訊管理部統籌資訊安全制度及合理的法規，並推動相關作業的落實，持續提升資安意識與專業能力。

3、透過技術的運用，識別資安風險與弱點，並進行有效的強化，建構完善的資安政策與全方位的資安防護能力，進而定期檢討資安政策，並每年一次向董事會報告公司的資安狀況。

二、資通安全落實：

1、建立符合法規與客戶需求之資通安全管理規範。

2、透過全員教育訓練，以達成資安防護，全面落實的共識。

3、保護公司與客戶資訊的機密性、完整性、可用性與法律遵循性。

三、成立資通安全管理組織：

1、資通安全委員會：

5 名成員由相關部門主管所組成，負責執行資通作業安全管理規劃，建置與維護資通安全管理體系，由資安主管擔任召集人並負責督導全公司資通安全作業執行以及資安風險管理機制之有效性，每年一次向董事會呈報整體資通安全管理組織相關資安管理作業及制度之執行成效。

聯傑國際的機密資訊保護，是依據規劃、執行、查核與行動(Plan-Do-Check-Act, PDCA)的管理循環，持續不斷強化機密資訊保護的能力，並提升人員對機密資訊保護的正確觀念及警覺性，降低機密資訊外洩的風險。

2.1. 每季定期進行查核活動，以確保公司的機密資訊 保護措施的落實。

2.2. 透過日常工作與各種場合，宣導機密資訊的觀念 與遵守事宜。

2.3. 落實員工的教育訓練，提高員工資安意識與能力。 除了將機密資訊管制相關內容，列為新進人員的必訓課程外，每年所有員工均必須進行複訓，以期能不斷強化與提升員工資安意識。

四、資通安全管理因應對策：

1、強化資通安全防禦能力及成熟度評鑑：

每半年進行資安系統測試並加以補強，持續進行營運持續應變演練。建立網路安全事件應變計畫，採取對應的通報及復原行動。

2、資通安全風險管理具體執行措施：

本公司透過每一年的風險評鑑作業，從各項可能的威脅與弱點組合中，分析出主要的項目包括：

2.1.詐騙集團利用偽冒的電子郵件，誘騙企業員工匯款或交易。

2.2.商業間諜或競爭對手運用駭客技術，持續滲透內部主機，竊取企業內部資料。

2.3.犯罪集團結合駭客，透過電子郵件、簡訊、社群軟體、通訊軟體，散佈具有惡意連結的內容，使受害電腦資料被加密綁架，要求付出高額贖金。

2.4.駭客透過網路發動大規模數量的連線要求，阻斷公司正常網路的運作。

2.5.內部員工使用非法軟體或將公司機敏資料複製到隨身儲存裝置，因遺失、遭竊或販賣，致使資料外洩。

2.6.天災人禍造成資訊軟硬體或受到損害，導致服務中斷或資料遺失。

2.7.本公司目前雖暫未投保資安險，在無投保資安險的情況下，針對以上的風險項目，運用資安管理準則、導入科技解決方案與強化資安教育訓練，(112 年 1 月~112 年 11 月共執行 2 次資安教育訓練，共 108 人次參加)，多管齊下做好資訊安全的管理機制，包括以下重點措施：

2.7.1.定期執行內外部稽核，精進資安管理體系運作。最近一次資訊安全外部稽核是由資誠聯合會計師事務所於 112 年 11 月 9 日~10 日到公司執行查核作業。

2.7.2.提供資安教育訓練，提升員工對於郵件防護意識。

2.7.3.用戶端安裝防毒防護系統，提供實時異常檢測和警報，取證分析和端點修復功能。同時封鎖 USB 儲存裝置的連接與自行安裝軟體的權限。另提供備份檔案服務器備份重要資料並且承租銀行保管箱實施異地保存。

2.7.4.針對網路層，結合防火牆，針對網路的流量與應用進行管制。

2.7.5.發展內網防護與資料庫存取安全監控管理機制。

2.7.6.透過文件管控系統 DRM（Digital Right Management；數位版權管理）與磁碟加密技術，保護文件機密性。

2.7.7.運用郵件過濾及郵件稽核系統及 Anti-APT，降低電子郵件使用的風險。

2.7.8.導入刷卡系統於閘門管理，達到資訊中心的實體安全需求。

2.7.9.主機集中管理，建立機房環控與告警機制，定期執行資料備份整理並執行備份資料異地保存(承租銀行保管箱)，並每年執行災難備援演練。