

# 聚隆纖維股份有限公司

## 資通安全政策

本公司資通安全政策目標如下：

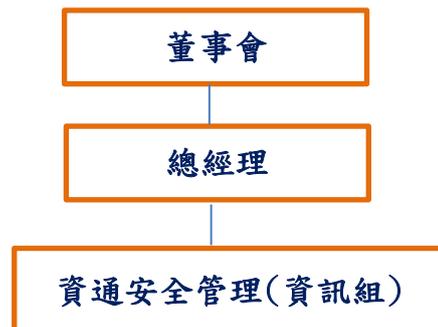
- (1)確保本公司商業活動持續運作，保護本公司所提供的資訊服務穩定使用。
- (2)確保本公司所保管的資訊資產之機密性、完整性與可用性，並保護人員個資之隱私。
- (3)建立資訊業務永續運作計劃，執行符合法令規範之資訊業務活動。

本公司資通風險評估分析之說明：

本公司依資訊應用及 IT 工具使用等網路環境中，依需要：於對外網路上建置有軟體式防火牆以管控使用者使用企業內外網路限制並防堵外部駭客簽入破壞；另建置有 SPAM 主機以阻擋惡意郵件侵犯，並租用中華電信「企業資通功能」以阻隔常見的惡意攻擊及連線。於內部網路資料及共享資訊使用之管理上，建置 AD 環境以統一管理使用者帳號可用設備及網路資源管理，以減少大量資料被攜出及設定分享檔案權限管控；避免有心人事刪除或竄改；資訊應用系統以單一簽入方式進行控管以限制外部連線進入使用，進而降低資料庫被竊取風險。以上方案僅適用於現有網路應用上之方案，惟網路破壞人士、技術層出不窮，再多的防範仍無法保證百分之百有效，僅能於有限範圍內達到有效目標；本公司目前利用 INTERNET(雲應用)之應用方案進行控管雖屬有限，但以現有資通環境架構下尚能有效防堵，並無太大風險發生。但對於有心進行之連續攻擊仍僅能被動進行防範，是以內部仍要求人員應對不明網站及郵件應多加小心，非必要仍不應讀取而以直接刪除處理；是以近年來並無重大資料傷害風險。惟，近來雲端技術及網路應用日新月異，資訊應用來自需求下，內外網路間的溝通將會越來越難界定，本公司除加強人員使用注意宣導外於 IT 技術的應用上將再行盤點評估，以建置符合公司未來應用需求下應有的資通防護環境。而於內控辦法上也將同步進行檢討更新以更符合各有關事項管理及提供人員作業規範。是以，目前評估資訊安全尚無影響本公司之營運重大風險。

本公司之資通架構如下：

負責並定期檢視本公司之資通結構及政策，並於每年度由內部稽核專員進行資通作業檢視，定期檢討資通政策，並定期向董事會報告。



非系統性安全風險評估上，本公司對於資通風險防護控制與具體實施方案如下：

| 資通風險        | 資通風險具體管理、實施方法說明  |
|-------------|--|
| 網路防護機制      | 為了防止公司對外的系統(Web、Email 等)遭受攻擊因而造成系統停擺、損毀，公司採用 Fortinet 公司的 FortiGate E 系列防火牆作為公司的防火牆，此系統可以有效的防堵網路攻擊與偵測入侵行為。                                 |
| 郵件防護機制      | 使用中華數位的垃圾郵件過濾系統，可有效阻擋大多數的垃圾郵件與病毒信件，並降低主機的負擔。使用者也可自行設定過濾的策略可減少郵件被誤判的機率。   |
| 個人電腦防護      | 公司內所有的個人電腦與伺服器都配有防毒軟體，且病毒碼與作業系統皆設定為自動更新，系統更新可以解決系統已知的問題與漏洞，加上防毒軟體的保護可以更有效保護使用者的電腦安全。   |
| 機台資通防護機制    | 因現今攻擊大多數需透過網路進行，故透過 VLAN 機制，將機台使用的網段與公司內部網段做隔離與加裝防火牆作控管，並切斷機台與網際網路的連線；為防止他廠遭到攻擊導致連帶受到波及，故跨廠與跨網段資料傳輸一律透過防火牆做控管與稽核，避免未經授權的流量進入               |
| 機台數據資料庫防護機制 | 為確保資料完整性與不可否認性，故以監控電腦作第一線資料蒐集並存放，再將資料傳輸至收集伺服器中保存，即使網路斷線後資料還是可以在網路恢復時補傳回資料收集伺服器；公司內部的遠端及跨廠系統透過中華電信的 MPLS VPN 傳輸，此傳輸系統為獨立於網際網路上的傳輸技術，以確保資訊安全 |
| 定期更新        | 本公司會定期依照軟體公司所發布的軟體更新包進行更新，在更新之前會做評估，避免因軟體更新後，造成收集資料軟體以及機台作業異常  |
| 資料定期備份      | 本公司會每天進行一次完整備份與四次的差異備份，並保留三天的時間；備份完畢後，會於每天離峰時間將備份資料傳輸到本公司其他廠區做異地備份，並將備份資料保留一個月   |
| 個資保護法       | 資訊蒐集比照個人資料保護法之規定實施。  |
| 資通系統稽核      | 本計畫相關資訊系統必要時委託公正第三方進行資訊進行資訊安全稽核，避免資訊安全上的漏洞與不易察覺之隱憂。  |

### 資通安全管理資源：

本公司設有資訊安全主管一名、一名網路工程師及其他二名資訊組組員以利相互支援，主要負責公司網路架構及設備安全與訂定公司資訊安全政策及規劃資訊安全措施，及執行相關之資訊安全作業。

每月定期召開工作檢討會議兩次(年度合計 24 次)，針對公司組織潛在之資通風險及問題進行討論與提出修正防範措施，並於民國 113/08/20 對全體一、二級主管及行政人員進行資通風險之課程講習，合計 84 人次/時，並將相關資訊放置公司網路供各位同仁研讀，於 113/11/08 將年度教育訓練實施情形呈報董事會。

### 定期稽核作業：

依據公開發行公司建立內部控制制度處理準則，應將資通安全檢查列入每年年度稽核計劃之稽核項目。近年度之稽核執行查核結果如下：

#### 內部稽核計畫

##### 其他管理稽核－資通安全檢查

##### 1. 背景資料

受查單位：資訊組。

查核事項：資通安全。

##### 2. 查核目的

依法令規定查核。

##### 3. 查核範圍

本公司資訊系統。

##### 4. 查核程序

4.1 依行政院資通安全稽核服務團，資通安全外部稽核(自我評審)表，請資訊組自我檢查。

4.2 資訊組自我檢查回覆，稽核組覆核本公司資通安全狀況。

4.3 彙整與建議。

##### 5. 稽核建議

無。

(查核者簽名)

