慶豐富實業股份有限公司
資通安全風險管理及 112 年度執行情形

一、資通安全風險管理架構

目前本公司資訊人員隸屬管理部並為資通安全管理之執行單位，進行資通安全預防及危機處理等具體管理方案，並實施對應的安控措施，持續精進內部異常偵測與防護方法，以降低企業資安風險。

本公司因應「公開發行公司建立內部控制制度處理準則」規定，配置資訊安全主管及資訊安全人員各 1 名，負責訂定公司資訊安全政策，規劃資訊安全措施，並執行相關之資訊安全作業。

本公司每年定期向董事會報告「資通安全風險管理情形」，最近一次提報日期為 2024 年 03 月 13 日。

二、資通安全政策

1.法規遵循：本公司執行業務時應遵守政府資通安全與個人資料保護相關法規及標準。

2.資安教育：每年定期實施資通安全教育訓練，宣導資通安全政策及實施規定。

3.規劃資源：建立資訊資產管理機制，統籌分配並有效應用資源，解決安全問題。

4.事先防範：新資訊系統或服務建置或推出前，應納入資通安全因素，以防範危害安全情況之發生。

5.安全監控：建立資通安全監控與防護措施，並定期進行檢視。

6.授權管理：明確規範資訊系統、網路服務、敏感資訊之使用權限，防止未經授權存取之行為。

7.檢討改善：訂定及執行內外部稽核活動，以落實資通安全管理制度，並針對未盡事項執行改善。

8.業務持續：訂定資通安全之營運持續計畫並實際演練，確保突發事故發生時得以應變。

9.資安文化：所有人員皆負有資通安全之責任，且應瞭解及遵守相關之資通安全規定，並於工作職責中落實。依本公司資訊單位辨識的資訊安全風險胃納程度，尚不需針對資安風險進行投保。

三、資通安全具體管理方案：

本公司既有的資訊安全管理程序來落實資通安全風險管理。相關具體執行措施如下：

1.資通安全管理機制：

(1)建置企業級 FortiGate 防火牆針對入侵偵測系統、惡意網址過濾與進階持續性威脅功擊防禦，以防範來自外部網路的惡意攻擊及非法入侵行為。

(2)各廠區間使用 FortiGate IPsec VPN 線路作業，使用資料加密方式傳輸，避免資料傳輸過程遭到非法擷取。

(3)使用中華電信 Hinet 企業資安服務，每日阻擋並監控可疑流量，並告知相關風險報告。

(4)導入微軟集中式目錄管理服務，依據群組安全性元則控管使用者帳號密碼，以提升網路安全。

2.系統存取控制：

(1)公司內各應用系統的使用，需透過資訊服務需求申請程序，經權責主管核准後，由資訊室建立帳號，且經過各系統管理員依所申請之功能開放權限，方得使用。

(2)帳號的密碼設置，需符合規定之複雜性原則，才能註冊使用。

(3)同仁辦理離職手續時，需即時會辦資訊人員，進行各系統帳號及權限的終止作業。

3.落實資安訓練：

(1) 每年度辦理資訊安全教育訓練暨個人資料保護法課程。

(2)新進人員教育訓練中加入資安課程。

(3)提升同仁資安意識，不定期宣導最新資安風險報告。

4.病毒防護與管理：

(1)伺服器與同仁電腦設備皆安裝端點防護軟體，病毒碼採自動更新，確保能阻擋最新型病毒。

(2)電子郵件伺服器配置有 Anti-Spam 與 Anti-Virus 雙重防護過濾機制，保護企業電子郵件不受病毒、垃圾郵件及不明郵件內容干擾。

5.確保系統可用性：

(1)建置硬體虛擬化系統，提高系統可用度與容錯性。

(2)建置備份管理系統，定期將每日備份的資料，一份保留在機房另一份放於異地互相備援。

(3)定期實施災難復原演練，測試還原備份檔案可用性。

6.電腦設備安全管理：

(1)資訊設備盤點管理，汰換及升級高風險設備。

(2)本公司核心主機、各應用伺服器與網路設備皆設置於專用機房，機房隨時上鎖嚴格控管人員進出，且保留記錄存查。

(3)資訊機房內設有不間斷獨立空調兩部及不斷電系統兩部，以維持伺服器設備於適合的溫度下運轉，並確保斷電時維持系統正常運作。

四、112 年度「資通安全風險管理執行情形」，內容如下：

1.除資訊單位自行檢查外，本公司稽核室於 112 年 2 月依計畫執行資訊安全內控查核作業，無重大缺失或存在或有重大風險。

2.112 年依計畫完成年度資安教育訓練暨個人資料保護法宣導。112 年度共舉辦兩場次，共計 230 人參與。

3.全面更新郵件伺服器，加強郵件過濾機制減少惡意郵件攻擊導致資安風險。

4.實施弱點掃瞄作業，盤查公司環境風險較高之資訊設備，並汰換或更新。

5.投入資通安全管理之資源

(1)購入防火牆專用無線分享器，控管無線網路設備上網路由。

(2)完成集團營運系統權限設定檢核作業。

(3)完成集團內部資訊設備盤點檢核作業。

(3)公司對外網站升級為 https 加密網站，提升網站安全性。

6.加入 TWCERT/CC 聯盟，收集最新資安風險與資安漏洞修正方式。

五、資訊系統損害對公司業務之影響與因應措施：

目前公司資訊系統架構中，在硬體部份是建置高穩定性伺服器並逐步建置虛擬化環境，而軟體部份則是定期將資訊系統、電子檔案與系統設定參數做快照備份及差異式資料備份機制以確保縮短服務中斷時間。

在資訊服務不中斷及資料安全上，管理部資訊單位定期將備份資料送往異地保管存放，並定期演練災後復原措施。除此確保不斷電系統正常運行，預防及降低無預警天災以及人為疏失帶來的資訊服務中斷和縮短系統復原的時間。

近來資安威脅分析，來源為外部駭客攻擊佔大宗，其次則為內部員工的疏忽與缺少資安意識下造成的資安事件風險，而這類資安風大都讓使用者誤判點選來路不明釣魚電子郵件或執行不明惡意程式所造成，因此資安防護不僅要從企業端做起，員工也要自我提升資安意識，惟有從工作習慣與公司文化的養成，逐步提升風險意識與資安防護能力，才能真正強化資安防禦能力。

六、112 年度本公司並未無任何重大的網絡攻擊或事件，亦無客戶資訊洩漏及違反資通安全等重大資安事件發生，也未曾涉入任何與此有關的法律案件或監管調查。