JOURDENESS GROUP LIMITED

資通安全風險管理及執行報告

董事會報告日期：113 年 12 月 17 日

本公司成立之初即設置集團資訊中心負責資訊系統規劃，因應資訊發展趨勢與監管要求，112 年成立集團資安中心，遵循總經理制定之資訊安全政策方向，負責資通訊安全相關工作。本公司於今年度導入 ISO 27001 資訊安全管理系統。透過 ISO 27001 資通安全管理系統導入，強化資通安全事件之應變能力，保護公司與客戶之資產安全。本公司 113 年度資通安全風險管理及執行情形如下：

一、 資通安全政策

1. **實施風險管理**：

   依據公司業務特性，法律法規要求，建立風險評估模型，訂定年度風險接受水準。定期進行風險評估，以識別企業風險變化。當環境有重大變化時，應針對受影響範圍執行再評估。依據風險評估的結果，採取相應措施，降低風險。

2. **確保資訊安全**：

   各資訊系統例行維運時，除了確保系統穩定，需定期修補系統脆弱點，搭配外部情資，評估可能的威脅，找尋適當的工具或方法，降低風險帶來的衝擊。除了資通訊系統，經營管理作業流程中亦加入資訊安全評估要素，並全面強化內部員工資安意識。

3. **業務可持續性：**

   建立資訊安全監督和保證體系，明確定義各工作崗位的資訊安全責任，以人為本，堅持全員、全方位、全過程資訊安全管理。通過測量和監控，持續改進，保證資訊安全管理體系的有效運行，做到制度執行有記錄、記錄記載可追溯，保障企業生產、經營、管理和服務的持續和安全，實現企業發展目標。

二、 具體管理方案及投入資通安全管理之資源

不只有完善的政策與管理辦法，本公司更投入了相應的設備與系統強化資通訊安

全，如防火牆，端點管理等，以下針對重要資安設備或系統說明：

1. 防範外部網路威脅-防火牆
   企業防火牆無疑是外部網路威脅第一道防線。本公司於企業總部，生技園區等據點採用國際領導品牌 Palo Alto Networks，Check Point 次世代防火牆，具有良好的網路安全防護功能。

2. 防止內部威脅-端點防護
   對於內部端點防護，除了一般基本的防毒軟體，於 112 年建置新世代端點安全系統，管理公司內部軟硬體資產，如禁止未授權軟體下載安裝，未授權用戶禁止使用 USB 外接裝置存取企業內部檔案，控制合法授權軟體安裝數量等，有效防止用戶不當行為並提高合規性。

3. 行動裝置管理
   針對門市行動裝置，如 Apple iPad，導入企業行動管理平台 VMware Workspace ONE (AirWatch)，受控裝置僅能安裝與執行企業核發的應用程式，雲端控制中心能統一發佈應用程式與系統更新，及早修補漏洞。

4. 資料備份
   資料安全的最後一道防線就是備份。本公司針對重要交易系統資料庫與檔案持續備份，採用本地備份一體機與雲端儲存架構，符合備份 3-2-1 原則，至少三份備份，兩種不同媒體格式，一份異地備份。

三、113 年度執行情形

1. 委託顧問公司，協助導入 ISO 27001 資訊安全管理系統(ISMS)，制定與發佈資安政策及各項管理辦法。
2. 委託資安廠商，完成重要服務主機弱點掃描與郵件社交工程。
3. 113 年度完成 600 人次資訊安全宣導與教育。另外，資安專責單位人員於上半年取得兩張 iPAS 中級資安工程師認證。
4. 針對門市電腦，配置列印控制策略，增加浮水印顯示用戶名稱，降低個資外洩風險。
5. 依照年度計畫，嘉義生技園區執行備援計劃演練，提高員工對於應變計劃熟悉度。
6. 依外部稽核單位建議，調整網域政策，辦公室電腦閒置 15 分鐘後進入螢幕保護程式，降低資料外洩風險。