# 幸福水泥股份有限公司
# 114 年度資訊安全管理政策及程序執行情形報告

報告日期及主要內容：資訊安全專責主管林煥殷於 114 年 12 月 19 日分別於審計委員會及董事會報告，述明如下：

1. 依「公開發行公司建立內部控制制度處理準則」，本公司應於民國 112 年底配置「資訊安全專責主管」及至少 1 名「資訊安全專責人員」。本公司已依前項規定辦理並完成公開資訊之申報。

2. 本公司已加入資安組織「台灣電腦網路危機處理暨協調中心(TWCERT/CC)」，適時取得資安資訊、資安跨域聯防與情資分享。

3. 本公司於 114 年度投入資通安全之項目如防火牆、加密系統等之金額計 9,680 仟元；另 115 年預計將投入 AD 系統版本升級、Nutanix 主機升級等，亦與資訊安全相關，並已列入 115 年之年度預算中。

4. 本公司資訊安全之說明、針對各項資安風險之評估及因應措施如下：

    隨著數位化時代的快速發展，企業在享受科技帶來的便利和效益的同時，也面臨著日益嚴峻的資訊安全挑戰。資訊安全不僅是技術部門的責任，它已經成為每一位員工、每一個業務單位的共同責任。數據洩漏、網路攻擊、勒索病毒等安全事件的頻繁發生，對企業的聲譽、營運以及客戶信任造成了極大的威脅。為了保障公司資訊資產的安全、維護客戶隱私和信任，我們必須採取積極的防範措施，確保資訊系統的完整性、機密性和可用性。

    在這樣的背景下，公司制定了明確的資訊安全政策和管理措施，旨在提高所有員工對資訊安全的認識，強化內部控制，降低潛在的風險，並確保各項業務運作不受資訊安全事件的干擾。這些措施將從防火牆設置、加密技術、身份驗證到員工的資訊安全教育等方面，形成一個全方位的安全防護體系。

    資訊安全不僅僅是防範外部攻擊，更涉及內部的風險管理和規範流程。每一位員工都應該在日常工作中保持警覺，遵循公司的資訊安全政策和最佳實踐，並且及時上報任何可疑的行為或安全事件。只有通過全員參與、持續學習和實踐，才能夠有效應對不斷變化的安全威脅，保護公司的數位資產，並確保企業在競爭激烈的市場中保持穩定與信任。

    在此，我們希望每位員工都能夠充分理解資訊安全的重要性，並積極投入到公司的資訊安全管理中，共同營造一個安全、穩定的資訊環境，為公司的長遠發展保駕護航。

以下為針對各項資訊安全風險所做的評估與因應措施

| 風險管理範疇 | 風險項目 | 風險評估 | 因應措施 |
|---|---|---|---|
| 資訊安全風險 | 1.權限管理 | • 用戶獲得過多權限，可能導致濫用或未經授權的存取。<br>• 權限授予、調整、撤銷等流程不完善，可能會導致權限過度或不一致。<br>• 離職員工或變動職位的員工仍然擁有存取權限。 | • 遵循最小權限原則，僅授予員工完成工作所需的最少權限，定期審查和調整權限。<br>• 審查和測試現有的權限管理流程，確保流程清晰並符合標準操作規程。<br>• 建立流程，確保員工離職或調職時及時撤銷其權限。權限調整時採先刪除權限再依其職位需求授予權限。 |
| | 2.存取管控 | • 用戶選擇弱密碼或未能妥善管理密碼，可能會被破解或被盜用。<br>• 員工可能因為社交工程攻擊而無意中洩露權限或敏感信息。<br>• 外部合作方或服務提供商的權限管理不當，可能導致數據洩露或不當存取。<br>• 缺乏有效的監控和審計，無法檢測不當權限使用。 | • 強制執行強密碼策略，要求定期更新密碼。<br>• 加強員工的安全意識訓練，並實施多因素身份驗證來減少風險。<br>• 與外部合作方建立明確的安全協議，並簽署保密協議，定期審核其權限和存取紀錄。<br>• 實施權限監控和審計工具，定期檢查和追蹤權限變更及使用情況。 |
| | 3.外部威脅 | • 外部攻擊者可能進行攻擊或駭客入侵。<br>• 攻擊者通過欺騙員工獲取敏感資訊。<br>• 病毒、間諜軟體、勒索病毒等可能感染系統。<br>• 外部攻擊者竊取機密資料。 | • 部署防火牆、入侵檢測系統（IDS），定期測試安全防護。<br>• 加強員工安全意識培訓，定期進行釣魚測試。<br>• XDR 跨端點、網路與雲端整合威脅偵測與自動化回應的平台，讓企業快速、精準阻止攻擊。<br>• 購買加密軟體保護敏感資料，實施嚴格的訪問控制。 |

| | | | |
|---|---|---|---|
| | 4.系統可用性 | • 硬體或軟體故障導致服務中斷。<br>• 資源不足以應對負載高峰。<br>• 自然災害或意外事故中斷服務。 | • 系統/網路可用狀態監控及通報機制，服務中斷之應變措施。<br>• 進行容量規劃，啟用自動擴展。<br>• 制定災害復原計畫、資料備份備援措施，設立異地備援。 |