隆大營建事業股份有限公司
LONG DA CONSTRUCTION & DEVELOPMENT CORPORATION

113 年度資訊安全風險管理報告

一、組織架構

(一)為強化本公司之資訊安全管理、確保資料、系統及網路安全。
(二)資訊安全管理委員會由資訊安全主管負責、資訊人員執行管理，並每年一次向董事會提送資訊安全報告。

二、管理機制

執行資訊機房、電腦資訊檔案、網路、郵件及資訊系統控制存取等管理。

三、資訊安全政策

資訊安全之目標：
建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及網路安全，保障公司利益及各單位資訊系統之永續運作。

資訊安全之範圍：
(一) 人員管理及資訊安全教育訓練。
(二) 作業系統安全管理。
(三) 網路安全管理。
(四) 資料存取管制及備份。
(五) 系統維護管理。
(六) 資訊資產安全管理。
(七) 實體及環境安全管理。
(八) 資訊安全稽核。

資訊安全的原則及標準：
(一) 定期辦理資訊安全教育訓練及宣導，包括資訊安全政策、資訊安全法令規定、資訊安全作業程序、以及如何正確使用資訊科技設施等，促使員工瞭解資訊安全的重要性，各種可能的資安風險，以提高員工資訊安全意識，並遵守資訊安全規定。
(二) 為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒採取偵測及防範措施，對入侵及惡意攻擊建立主動式入侵偵測系統，以確保電腦資料安全。
(三) 為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或資訊系統等中斷，建立資訊系統永續運作規劃之政策。

員工應遵守之相關規定：
(一) 資訊帳號申請及異動，須填寫「資訊帳號及權限申請（異動）表」，送交資訊組辦理。
(二) 電腦資料及設備，不得任意破壞、外借或不正當修改，以維護資訊安全。
(三) 禁止使用非法或無授權之軟體。
(四) 電腦作業結束或長時間不使用時，應登出或關機，以免資料機密外洩，或為他人所破壞。
(五) 電腦設備之擺放位置，除以方便為原則外，應遠離茶水或潮溼地點，以保障設備安全。

（六）電腦使用者離職或職務異動時，由資訊組衡量資料相關性作適當處置。
（七）電腦設備無法正常作業時，使用者應立即通知資訊組檢查或維修。

四、管理方案

網路安全：
（一）網路服務採用「中華電信-HiNet 資安艦隊」方案，該服務主要為對企業網路防護，包含「先進網路防禦系統(ANDs)」、「企業防駭守門員」、DDoS 防護、垃圾與病毒郵件過濾等服務，針對異常流量、駭客入侵及非安全連線等行為主動防禦。
（二）防火牆建立設定連線安全規則。

防毒軟體：
（一）全電腦設備安裝防毒軟體，病毒碼採自動更新，降低病毒感染風險。
（二）防毒軟體即時掃描，發現病毒將立即採取刪除等防護手段，以確保電腦作業安全。

作業系統：
作業系統不同版本更新模式有所區別，原則優先採取自動更新，以維持系統安全性。

機房安全管理：
（一）採用雙機房備援模式運行，分別設立於 18 樓之 3 資訊室及 19 樓之 3 資訊室，如主要伺服器發生故障情形，備援伺服器將立即啟用，工作將不受影響。
（二）機房門禁管制，僅限資訊人員保管有門禁鑰匙；維護廠商或其他外部人員因工作須進入，應填寫「外部人員機房出入管制表」備查。

檔案存取管制：
（一）依個人作業及權職，劃分檔案及系統控制存取權限；資訊帳號申請及異動，須填寫「資訊帳號及權限申請（異動）表」，經主管核可後，由資訊組辦理。
（二）人員職務異動時，依規定依新任職務調整現有檔案及系統控制存取權限。
（三）電腦設備閒置或報廢時，舊有檔案清除或設定還原，避免公司資料外流。

資料定期備份作業：
（一）每日執行虛擬主機鏡像備份，於主要伺服器建立備援虛擬主機。
（二）每日執行伺服器鏡像備份，於備援伺服器建立完整虛擬主機群。
（三）每週執行資料完整備份，以七組硬碟交替備份，檔案可保存達七週之久。
（四）每八週執行一次資料完整異地備份，以四組硬碟交替備份，檔案可保存達三十二週之久；備份作業完成後送至「國泰世華商業銀行南高雄分行」保管箱存放，以達異地備份目的。

郵件安全管控：
（一）有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。
（二）個人電腦接收郵件後，防毒軟體將掃描是否包含不安全的附件檔案。

資訊稽核：
（一）內部控制作業層級評估。
（二）「電子計算機處理循環」稽核作業。
（三）安永聯合會計師事務所 內控資訊審查作業。
（四）安永聯合會計師事務所 資訊系統環境相關查核程序。

資安宣導：

（一）每年進行員工教育訓練，加強員工資訊安全意識。

（二）不定期發布資訊安全相關文章，及案例分享，認識時下常見資安犯罪行為。

五、緊急通報程序

當有資訊安全事件時，發生單位應立即通報資訊組，判斷事件類型，並找出問題點，即時依事件處理。

六、資安維護項目評估及檢查

項目	風險	頻率	結果
機房環境巡檢	中	每週	無異常
機房空調設備保養	低	每年	本年度預定於 2024/11/23 進行
作業系統更新檢查	中	每月	無異常
防毒軟體病毒碼更新	中	每月	無異常
防火牆更新	高	四年一次	2024/09/24 完成
虛擬主機鏡像備份	高	每日	無異常
伺服器鏡像備份	高	每日	無異常
資料完整備份	低	每週	本週備份作業失敗，將持續完成作業。
資料完整異地備份	低	八週一次	無異常
系統災害復原測試	低	每年	2024/10/22 完成
ERP 高權限帳號檢視	中	每年	本年度預定於 2024/12/16 資訊查核時進行
ERP 使用者帳號檢視	低	每年	2024/10/22 完成
員工教育訓練	高	每年	2024/05/02 完成
資安宣導	高	不定期	無異常
非法軟體檢查	高	不定期	無異常
電子信箱剩餘空間檢查	高	不定期	無異常
內部控制作業層級評估	高	每年	2024/02/26 完成
電子計算機處理循環稽核	高	每年	2024/04/19 完成
內控資訊審查作業	高	每年	本年度預定於 2024/12/16 資訊查核時進行
資訊系統環境相關查核程序	高	每年	本年度預定於 2024/12/16 資訊查核時進行

七、年度資安維護費用

設備購置：

電腦更新 716,297 元

儲存裝置 20,688 元

硬體維護：

伺服器修繕 18,333 元

防火牆維護 36,015 元

軟體維護：

ERP 155,833 元
備份系統 96,600 元
ZOOM 會議軟體 10,912 元

八、結論

(一)本年度至今無發生重大資安事件，未對公司營運造成影響。
(二)目前資訊設備可靠性及資安管理政策均能發揮其成效，亦能符合會計師事務所之審查標準，將持續落實資訊安全管理。