寶徠建設股份有限公司

資訊安全政策與風險管理作業

2021.12.29 董事會通過

壹、目的：

為強化公司治理並健全風險管理作業，以符合本公司永續經營與發展，且揭示本公司對資訊安全之重視，特制定「資訊安全政策與管理作業」，保障公司作業電腦化規劃及資料處理之機密性、完整性與可用性。

貳、範圍：

包括本公司資訊作業相關人員實體環境、軟硬體設備、網路資料、文件等，免於遭受來自內部或外 部之不當使用、破壞、遺失、洩密等資訊安全風險。

叁、資訊安全政策與風險管理作業

一、風險管理組織架構與職掌

(一)董事會

本公司董事會為公司風險管理之最高單位，負責核准、審閱及監督公司風險管理政策，以遵循法令，確保風險管理之有效性，推動並落實整體風險管理為目標。

(二)風險管理小組之組織架構

風險管理小組為負責執行風險管理之權責單位，由總經理擔任召集人，成立跨部門小組，定期聽取各單位主管之報告。各單位主管負有風險管理之責任，須負起單位內作業的最初風險辨識、評估及管控的考量與防範之責，並確保風險管理及控制之機制與程序能有效執行。

(三)風險管理小組工作職掌

1. 綜理本公司整體之風險管理，擬訂風險管理政策、架構、組織及機制，並隨時注意國內外法令變動，據以檢討修訂本政策。
2. 每年定期向董事會提出風險管理政策執行情形之報告，並提出必要之改善建議。
3. 依據內外部環境變化與董事會之決議，設定風險控制管理之優先順序。
4. 其他經董事會決議指示應辦理之事項。
5. 檢視各單位風險控制管理報告，追蹤執行與改善進度。
6. 定期追蹤各單位風險管理執行狀況。

二、資訊安全政策

當資安風險或緊急事件發生時，本公司具備應變處置原則及能力，以確保業務迅速恢復正常運作。

(一)管理架構

本公司資訊安全之主責單位為管理部，負責訂定、推動與落實資訊安全政策。由資訊人員依據專業分工，負責公司資訊軟硬體控管、執行電腦化資訊系統作業，並由管理部主管採行必要之統籌、規劃與更新相關事宜。

本公司稽核室為資訊安全風險之查核單位，依據內部控制管理程序及電腦化資訊作業辦法，每年定期執行資訊安全檢查。若有發現缺失或資安事件，立即通知部門主管，要求受查單位提出相關改善計畫與具體作為，且不定期執行資安會議，以降低內部資安風險。

(二)管理機制

本公司資訊安全管理機制，包含以下三個面向：

1. 制度規範：內部訂定「電腦化資訊系統管理制度」，以規範本公司資訊運作環境及人員資訊安全行為，不定期依法規符合性與營運環境變遷進行更新。
2. 軟硬體維護：推展各項應用系統，協助與電腦相關之自動化作業，促進各部門對電腦軟、硬體之充分有效使用，並建置各式資安防護措施，以提升整體資訊環境之安全性。
3. 人員訓練：不定期透過外部或內部教育訓練提升資訊人員的專業職能，亦不定期於內部系統公告與業務相關之資安宣導影片或注意事項。

三、資訊安全管理方案

(一)管理目標：

1. 維持公司伺服器主機運作。
2. 網路連線與電腦設備安全防護。
3. 確保公司資料機密性、控管資料存取之權限。
4. 系統備份及還原作業。
5. 個資管理。

(二)具體措施：

項目	具體措施
伺服器設備管理	1. 公司設有專屬電腦機房，並設有門禁控管人員進出。 2. 機房設有空調，讓伺服器維持在適當的溫度下運作。 3. 伺服器連結 UPS 不斷電系統，以預防突發斷電之狀況發生。
網路設備管理	1. 網路架有 Abocom sg650 負載平衡器，以此防護網路安全。 2. 租用中華電信網路，分別為固定 IP 及浮動 IP，並透過 sg650 負載平衡器設定以固定 IP 做為使用網路，浮動 IP 做為備援網路，確保公司網路連線不中斷。
電腦設備防護管理	1. 伺服器及個人電腦設備皆安裝防毒軟體，且採用自動掃描及自動更新病毒碼之設定。

	2.每年固定安排檢查同仁電腦，確保系統軟體及硬體設備無異常損壞情形發生。
資料存取權限管理	1.NAS 資料主機分成各部門資料夾，並在各部門資料夾設定讀取權限。
系統備份及還原管理	1.公司設置數台 NAS 主機，分別為主要存取資料、自動備份及備援使用。 2.ERP 系統使用 SQL 備份，另使用 Acronis-Backup 備份整台伺服器系統資料。 3.另固定每週備份資料於硬碟且異地安置，以確保資料安全性。
不定期資訊安全風險評估	1.針對資訊資產(硬體.軟體.資料.文件.人員.通訊.環境)進行資訊安全風險評估.

註：資訊資產評估項目對應表

風險 / 種類 / 資產類別	硬體風險	軟體風險	資料.文件風險	通訊風險	人為風險	環境風險
硬體	V				V	V
軟體	V	V			V	
資料	V	V	V		V	
文件			V		V	
人員					V	
通訊	V			V	V	
環境					V	V

資訊資產分為七大類：

人員：內外部全體同仁。

文件：以紙本形式存在之文書資料、報表等相關資訊(包含公文、列印之報表、表單…等紙本文件)。

軟體：作業系統、應用系統程式、套裝軟體等(包含原始程式碼、應用程式執行碼、資料庫等)。

通訊：網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。

硬體：主機設備等相關硬體設施。

資料：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。

環境：相關基礎設施及服務(包含辦公室實體、機房、電力…等)。

肆、實施

本公司之資訊安全政策與管理作業經董事會核准後實施，修正時亦同。