根基營造股份有限公司
資通安全政策

壹、政策目的

根基營造股份有限公司（以下簡稱本公司）為確保本公司及轄下子公司之資料、資訊系統、設備及網路之安全，防範組織之營運受到資安事件之衝擊，以確保公司的業務與服務持續，並降低運營風險和達成投資回報效益最大化，依循母公司冠德建設所頒佈「冠德建設資通安全政策」之精神特訂定本政策。

貳、適用範圍

本資通安全政策之適用範圍包括人員、應用系統、硬體設備、機房及網路設施、資訊紀錄等五部分：

一、 人員：本公司之正式人員、約聘雇人員，及使用本公司及資訊資源之外部廠商或人員。

二、 應用系統：本公司之各類業務資訊系統。

三、 硬體設備：本公司之各式主機、工作站、伺服器及個人電腦。

四、 機房及網路設施：本公司之網路服務、空調、電力等。

五、 資訊紀錄：本公司共同性系統、系統資料庫、作業資料庫、系統規劃與設計文件、使用與操作手冊、制度文件及各式記錄等。

參、名詞定義

一、 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊

為其他處理、使用或分享之系統。

二、 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、 核心業務：公司維持營運與發展必要之業務。

四、 核心資通系統：支持核心業務持續運作必要之資通系統。

五、 機敏資訊：依公司業務考量，評估需保密或具敏感性之重要資料（如涉及營業秘密或個人資料等）。

六、 機密性（Confidentiality)：保護訊息、資料不被洩露，未經授權的披露、遺失或未經授權的查看。

七、 完整性（Integrity)：透過限制修改機制，來保有資訊、資料的完整性。

八、 可用性（Availability)：透過保護機制來阻擋攻擊，來達到資訊、資料可用性不遭受到損壞。

肆、推動組織

本公司於資訊處設置資訊安全專責主管及資訊安全安專責人員，負責推動、協調監督及審查資通安全管理事項，執行本資通安全政策。

伍、政策內容

一、 本公司依據可能影響資通安全的內外部議題，與關注方對於資通安全之

要求事項，擬定完整的資通安全管理制度。各項資通安全管理規定必須遵守政府相關法規（如：資通安全管理法、個人資料保護法等）之規定。

二、 本公司由資訊處負責訂定資通安全政策及目標，由資訊安全專責主管擬訂並呈報董事長審核，經提報董事會核准後執行。資訊處應建立資通安全制度，定期或不定期檢視公司資通安全政策與監督資通安全運作情形，並每年定期向董事會報告資通安全執行成果。

三、 本公司應適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其符合資訊安全之機密性、完整性及可用性之要求。

四、 本公司資訊資產（包括軟體、硬體、網路通訊設備及資料庫等）應予適當保護，採行合宜之備份措施與回復作業，防止未經授權或因作業疏失對資產所造成之損害。

五、 本公司應強固核心資通系統之韌性，訂定資通安全之營運持續計畫並實際演練，確保本公司業務持續營運。

六、 每年應定期執行弱點或滲透測試，所有資通安全事件或可疑之安全弱點，應即時通報反映，並予以適當調查、處理及防範；並每年定期實施社交工程演練及資通安全通識教育訓練，以加強資通安全政策宣導及全體同仁之資通安全意識。

七、 本公司應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的

存取與竄改。

陸、管理機制

本公司資通安全管理機制，包含以下四個面向：

一、 資訊規章之制定與修訂：由資訊處訂定本公司「資通安全作業程序」，明確訂定人員對於資訊作業的行為，包含核心業務及其重要性、資通安全防護及控制措施、資通系統或資通服務委外辦理之管理措施等，並經資訊安全專責主管審核並經董事長核定後實施。修訂時，亦同。

二、 資訊科技之運用：建置資通安全管理設施，並定期檢視暨提升、汰換軟、硬體資訊設施，以符合當前資安風險控管之需求。

三、 資安宣導與訓練：因應資通安全威脅情勢變化，定期進行資通安全通識教育訓練，並宣導公司資通安全政策及目標，以提高同仁之資通安全意識，本公司全體人員應確實參與訓練。

四、 資安稽核與改善：資訊處將定期進行資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施。本公司稽核部門應將資通安全檢查作業納入稽核計畫，針對上述之資安風險評估資訊提出控制點建議，資訊單位及資訊安全專責主管應依此作調整與改善，以利控管資安風險。此外，資訊安全專責主管應定期進行檢視本政策，利用 PDCA（Plan–Do–Check–Act）循環的概念持續管理及改

善資訊安全，並反映政府資通安全管理政策、法令、技術、內外部議題與本公司業務之最新狀況，以確保本公司資通安全政策運作之可行性及有效性。

柒、資通安全事件通報應變及情資評估因應

一、 於「資通安全作業程序」中訂定資通安全事件通報程序，包含判定事件影響及損害評估、內部通報流程與通報窗口資訊。

二、 加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊，如台灣電腦網路危機處理際協調中心（TWCERT/CC)、行政院經濟部台灣CERT/CSIRT 聯盟等。

三、 發生符合「台灣證券交易所股份有限公司對有價證券上市公司重大訊息

之查證暨公開處理程序」規範之重大資安事件，應依相關規範辦理。

捌、制定沿革

本政策制定於中華民國 112 年 12 月 29 日。