

ESG 治理與策略

永續經營

● 建基 ESG 治理

唯有讓公司能夠在獲利的同時善盡環境與社會責任，才能實現企業的永續發展，進而發揮我們的社會影響力。建基專注在經濟績效表現的同時，並依循集團策略目標，持續落實公司治理推動、發展永續環境與社會影響力之永續目標。

● 推動永續發展之治理架構

建基已於113年11月6日董事會，根據本公司實際需要，決議通過訂定本公司「永續資訊管理作業程序」及「永續報告書編製及確信作業程序」，議定永續發展作業相關工作之權責單位、控制措施、作業監督與改進規定。由各類別永續資訊之提供單位組成永續發展工作小組（包括但不限於總務、人力資源、法務、供應商管理、採購、專案管理/研發、客戶服務、企業溝通、財務、資訊安全、產品物流與產品安全相關部門），並由總經理擔任召集人，至少一年一次定期向董事會報告永續發展推動情形。

為健全與強化本公司風險管理機能及實踐永續發展目標，並強化永續治理，亦已於114年11月5日增訂「風險管理暨永續發展委員會組織規程」，設置隸屬董事會之「風險管理暨永續發展委員會」，同時經董事會同意委任全體獨立董事及公司總經理擔任委員。

執行單位：由本公司各事業單位/功能組織最高主管組成風險管理組織，檢視本公司之各種策略、營運、財務等決策及執行，觀察所遇之各式災害及氣候變遷等相關事件所造成之影響，評估其潛在的風險並規畫及採取有效之管理或防免措施，定期向風險管理暨永續發展委員會暨董事會提出報告。

執行情形：針對跨部門的重要永續議題，進行溝通協調、並針對重要議題規劃、執行、及追蹤行動專案的進度與成效，定期向董事會報告永續相關議題的趨勢、影響與執行績效

誠信經營暨業務行為準則

誠信經營是公司治理內部控制機制重要的一環。會在事前辨識各項法令規章，再與內部相關單位溝通、衡量公司相關規則之制定與落實，以求符合法規與實務之順暢進行。誠信經營中之法令遵循、反貪腐與反競爭概念與社會責任與公司商譽有重大關聯，為建基永續經營重點之一。

● 誠信經營守則及道德行為準則

「誠信經營守則」及「道德行為準則」為建基所有經營階層、同仁及所有業務往來夥

伴，都能共同遵循的最高商業道德標準；內容服膺政府機關及國際條約宣言對於誠信經營及尊重人權之精神，同時在法務、人資及稽核等單位多方匯聚共識下，共同制定事件通報處理程序，使同仁對處理違反事例有所依循、防止再犯。

● 落實誠信經營

為健全誠信經營之管理，本公司由人力資源單位負責誠信經營政策與相關措施之制定及監督執行。透過不定期舉辦誠信經營相關辦教育訓練與宣導，確保所有相關人員皆了解、接受並恪守本公司道德行為準則。相關人員發現任何違反道德行為準則之行為時，均有責任向主管或董事會報告。如有必要，可直接向人力資源最高主管、稽核單位最高主管、董事長或經由員工申訴管道提出報告。同時已建立有效的會計制度、內部控制制度，並由內部稽核單位定期查核。

113年建基法規遵循相關教育訓練落實成果如下：

課程名稱	訓練對象	113 年完訓人數%
反賄賂、反貪腐及員工行為準則	全體同仁(並同時公告在 INTRANET，方便同事讀取最新資訊)	100%
職場不法侵害預防	全體同仁	100%
個人資料保護(另於「資訊安全意識」線上課程中，也再次宣導個人資料及資訊系統之間的關係)	全體同仁(並同時公告在 INTRANET，方便同事讀取最新資訊)	100%
尊重智慧財產(宣導台灣區規定)	全體同仁(並同時公告在 INTRANET，方便同事讀取最新資訊)	100%
禁止內線交易(宣導台灣區規定)	全體同仁	100%

● 舉報與保護

任何違反誠信經營守則或法律之事件一經通報，將旋即由權責單位調查並驗證事件真偽；倘事證確鑿，且確有違例情節，建基即刻採取適當處置、要求違例員工停止該等行為，並將視其必要採行法律上作為，以維護建基之權利與名譽。俟事件確定，建基資訊將會集權責單位、人資、法務及稽核等相關部門，審視相關程序並共商可行之矯治措施，以臻公司內控制度之全備。

舉報申訴管道：

- 建基檢舉申訴管道：電子郵件信箱 stakeholder@aopen.com

建基公司之董事、經理人、員工（統稱建基人員）、客戶、供應商、投資人及社區等，皆可使用

風險管理

本公司堅持永續經營之理念及對社會、客戶、員工、供應鏈合作夥伴及投資人承諾之長期永續責任，以積極且具成本效益的方式，整合並管理本公司所有對營運及獲利可能造成影響之各種策略、營運、財務、災害及氣候變遷等相關潛在的風險。

● 風險管理組織暨職掌

● 董事會/審計委員會：

1. 為本公司風險管理之最高權責單位。
2. 依整體營運策略及經營環境，推動並落實公司整體風險管理政策，以確保風險管理之有效性。

● 風險管理委員會：

1. 由本公司各事業單位/功能組織最高主管組成，並由內部稽核主管擔任觀察員向審計委員會暨董事會報告。
2. 彙總風險環境、風險管理重點、評估結果及相關因應措施。
3. 指導及核准風險控管之優先順序。
4. 督導風險管理之持續改善。
5. 觀察員定期檢視風險管理政策之執行狀況。

● 風險管理工作小組：

1. 由本公司各事業單位/功能組織處級主管代表組成。
2. 辨識風險、評估潛在風險情境及營運衝擊。
3. 依風險情境規畫並執行風險預防及緩釋行動。
4. 持續精進風險管理作為及確保其有效性。
5. 整合企業風險管理報告並呈報風險管理委員會。
6. 建立危機管理相關作業程序並進行演練。

● 風險管理程序

風險辨識及風險評估 / 風險控管及風險緩釋 / 風險監控及企業風險管理報告

● 風險管理運作情形

檢視本公司之各種策略、營運、財務等決策及執行，觀察所遇之各式災害及氣候變遷等相關事件所造成之影響，評估其潛在的風險並規畫及採取有效之管理或防免措施，並於113年11月6日分別向審計委員會及董事會提出報告。

資訊安全與隱私保護

● 資訊安全政策

本確保資訊資產的機密性、完整性與可用性，並符合《資通安全管理法》，本公司制定資訊安全政策，適用對象包含全體員工（含外包商、顧問、實習生等第三方人員）。

● 資通安全風險管理架構

為有效因應資安風險，本公司建置風險管理機制，涵蓋風險辨識、評估、處理與監督，並明確劃分組織層級與職責如下

組織層級	職責說明
高階管理層	定期審閱資安政策與重大風險事件，決策資安資源與策略方向
資訊安全管理單位 (資訊處)	規劃資安制度與技術防護措施，執行資安風險管理及應變計畫
各部門資安聯絡人	配合執行部門內部的資安規範、通報事件、推動資安意識
全體員工	遵守資安政策，參與教育訓練，落實安全操作流程

● 具體執行成果

113 年企業資訊安全措施推動執行情形

- 導入防火牆入侵防禦系統、入侵偵測系統，提升網路使用的安全性。
- 導入 NAC 系統，提升設備控管的能力，確保設備的合規性。
- 導入帳號 MFA 多重要素驗證，提升帳號登入的安全性。
- 導入 EDR 端點防護系統，強化終端設備端點資安防護。
- 導入 UEM 系統，自動化 PATCH 派送及安裝，強化端點安全度。
- 定期執行社交工程演練及員工教育訓練，宣導同仁最新詐騙釣魚郵件/型態，避免同事誤觸。
- 定期盤點系統使用帳號，確保無未經授權的存取。
- 定期進行資通安全宣導，提高同仁資安相關意識。以減少資通安全事件的發生。
- 定期執行軟體相關盤點工作，確保軟體的合法性及版本相關控管工作。
- 定期執行網站源始碼掃描，改善程式的漏動以提升系統的安全。
- 定期執行弱點掃描，完成相關改善工作。定期執行紅隊演練或滲透測試，完成相關改善工作提高及改善各系統的密碼複雜度及安全性設定，降低被駭客攻擊的風險。

- 隱私保護

本公司重視客戶個人資料與商業資訊的保護，已訂定《資訊安全政策》與《個人資料保護管理政策》，落實法規遵循並確保資訊資產的機密性與完整性。並依循集團之資安政策方向，透過日常管理機制強化資料保護與風險控管能力。

- 隱私保護主要管理機制如下

明定個資蒐集、處理、保存與刪除之作業流程，並於各服務節點提示使用者同意告知事項。

核心系統建置使用者權限分層、存取記錄管理與異常登入警示機制。

資訊設備全面導入端點防護 (如防毒、管控軟體) 與 MFA 多重驗證。

透過教育訓練與社交工程測試提升全員資安意識。

與外部委外廠商簽署個資保密條款，納入資安合規審查範疇。

設有資訊安全事件通報程序，定期進行模擬演練與改進。