風險管理

風險管理政策

建漢依循永續經營目標及重大性原則，遵守相關法令及辦法，維持積極主動之全面風險管理機制，且持續檢視內外部營運環境及議題變化、分析營運衝擊並辨識相應風險及機會，加強營運有效性及韌性，以實現企業永續經營承諾，保障利害關係人最佳權益。

營運持續管理

建漢以營運持續為目標，對內外部各項事件所隱藏風險且影響公司營運者，持續關注並投入資源進行風險控管與因應措施，而營運持續管理計畫為管理之重要一環。防範公司面對事故時，在可承受之風險範圍內，預防可能的損失並持續進行關鍵營運活動。並已逐步完成火災、地震、資訊安全侵害、傳染病事件與原物料短缺等事件之演練與風險管理策略制定，未來也將持續完備各種不同情境的營運持續管理計畫應變能力。

組織架構

一、董事會：為本公司風險管理之最高決策單位，核定風險管理政策與相關規範，監督風險管理整體落實情形，確保風險有效管控。

二、審計委員會：為協助董事會執行其風險管理職責，下設風險管理執行小組，並置召集人一人。風險管理執行小組進行公司營運風險與新興風險的綜合評估，且至少一年一次向審計委員會及董事會提出風險管理運作情形。

三、風險管理執行小組：由各單位最高主管擔任風險管理成員，確保營運單位確實落實風險管理制度，並指派單位人員擔任風險管理執行人員，及會同各營運單位相關人員，負責落實執行風險管理程序。

風險管理程序

本公司風險管理流程包括風險辨識、風險分析、風險評量、風險因應及風險監督與審查。

風險管理執行小組應至少一年一次向審計委員會及董事會提出風險管理運作情形。

2024 年重大風險

風險類別	風險衝擊	因應策略
營運風險	經濟衰退	審慎調漲價格，提升自動化能力，提高產品價格競爭力。
	資安攻擊	•安裝含有防勒索的防毒軟體並且不定期更新。 •防火牆升級及不定期進行作業系統修補。 •進行資安教育訓練加強同仁資安認知。 •不定期資安宣導及進行社交工程演練，隨時提醒資安警覺和提高危機意識。 •資訊安全的監控，軟體安裝限制及管控。
	人力難覓	•加強人才庫搜尋與補強、召募方式多元、提升招募條件。 •提高薪資及工作環境福利，以吸引人才加入。
	市場競爭激烈	多元化市場及產品銷售渠道。
	永續供應鏈管理	建立綠色採購政策及供應商篩選與檢核制度，與 RSM 供應鏈管理機制。針對 CSRDDD 對於人權與環境的要求事先進行因應。
	智慧財產	•定期進行智慧財產風險評估，識別潛在風險，定期更新專利和商標，並採取法律行動保護權益。 •導入 NAC 管理系統，進行電腦網路合規存取控制。 •評估文件管理機制，防止重要資訊外流。
	物料管理	•建立安全庫存量並定期檢討。 •即時監控並反應市場緊缺狀況，即時與上下游供應商及客戶協議，轉嫁風險。
	會計合規	遵循各項法規及定期教育訓練。
	客戶 ESG 相關要求	依循國際永續脈絡(GRI、SASB、TCFD、CDP)逐步將 ESG 全面導入企業運營，並積極設定減碳目標，除環境議題外，更納入人權(RBA)與多元(DEI)評估等指標。
	天然災害	•準備災害防治計劃。 •提高供應鏈韌性。
策略風險	客戶過於集中	開發多樣化產品，區隔不同產品市場，以利分散客群。
	產品資訊安全	•立即修補已發現的漏洞，並進行全面測試以確保修補有效。 •建立強大的補丁管理流程，確保補丁能夠及時、一致地部署。
	地緣政治	•即時了解國際情勢並適時與集團策略規劃結合。 •投資風險再定位：避免投資單一地區，既有投資方向架構重新盤整。 •逐步建構在地行銷業務人才，以更貼近市場，以提供客戶更即時性的服務。
	市場低碳產品需求	•導入產品生命週期(LCA)概念，與導入 ISO14067 產品碳足跡計算流程，開發低碳產品，以符合市場消費需求。
財務風險	碳稅徵收	•持續關注政府單位對於碳費徵收的實施辦法與細節，以及歐盟 CBAM (歐盟碳邊境調整機制)，以及美國 CCA(清潔競爭法案)的申報與課稅之執行方式與立法進程。 •落實組織碳盤查，以 CDP 問卷確實揭露碳排放，承諾 SBTi 倡議，提出科學減碳計畫，明確規劃淨零路徑。

資訊安全風險管理

資通安全風險管理架構

本公司為因應外部日新月異的網路與病毒攻擊，資訊部負責主導及規劃，各業務相關單位配合執行，以確認資訊安全管理運作之有效性。

資訊安全政策

為維護網路資訊系統的正常運作、確保網路資訊傳輸交易安全，保障電腦處理資料的機密性與完整性，以確保資料、系統、設備及網路安全並依據「資訊帳號管理辦法」、「資訊設備及安全管理辦法」及「個人資料保護管理辦法」規範作業。

具體管理方案

1.資訊帳號管理：確保資訊帳號之完整性、機密性及可用性。

2.資訊服務管理：資訊系統、網域及電子郵件帳號申請與管理規定。

3.資訊設備安全控制：資訊部門人員每日檢視機房設備運作，查看系統日誌紀錄，確保伺服器與網路設備運作正常。

4.電腦機房安全控制：機房門禁系統管制，進出入授權登記，系統不斷電系統管理。

5.合法軟體版權管制：合法軟體授權安裝與管制。

6.電腦病毒防治：佈署防毒軟體，避免電腦遭病毒攻擊與感染。

7.備份作業：執行日備份、週備份，落實備份作業與紀錄。

8.災害復原：擬定災難回復重建計劃並演練與檢討執行結果。

投入資通安全管理之資源

1.本公司已投入資安團隊共計 2 人。

2.定期參與集團資安會議，通報分享最新資安風險與資安漏洞修正方式。

3.防毒端點防護攔截端點威脅事件。

4.SPAM 全方位郵件過濾攔截垃圾郵件與威脅郵件。

5.資訊安全教育訓練實施與社交工程信件演練，提升員工資安威脅意識。