

# 群光電能科技股份有限公司

## 風險管理運作情形

為健全公司治理，落實企業經營之風險管理，並確保本公司風險制度之完整性，本公司業於110年8月5日經董事會通過訂定「風險管理政策與程序」，作為本公司風險管理之最高指導原則。

董事會為風險管理的最高治理單位，由企業永續發展委員會(共5名成員，其中3名委員由獨立董事擔任)督導風險管理政策及風險管控報告，每年定期向董事會報告，並適時向董事會反應風險管理執行情形，並提出必要之改善建議。

### 風險管理範疇

本公司各層級之風險管理包含本公司經營活動涉及營運、財務、環境、危害性事件及氣候變遷等，各項風險之辨識、衡量、監控與報告等流程，應配合經營環境、業務與營運活動之變動適時調整。

### 風險管理職責

#### 董事會：

本公司董事會為公司風險管理之最高單位，以遵循法令，推動並落實公司整體風險管理為目標，明確瞭解本公司營運所面臨之風險，確保風險管理之有效性。

#### 稽核室：

本公司稽核室為獨立之部門，隸屬董事會，職司實施內部稽核，以協助董事會及經理人檢查及覆核內部控制制度之缺失及衡量營運之效果及效率，並適時提供改進建議，以確保內部控制制度得以持續有效實施及作為檢討修正內部控制制度之依據。

#### 總經理：

總經理為本公司風險管理計劃之召集人，統籌指揮各權責單位進行風險管理計劃之各項工作；負責經營決策風險評估及執行因應策略，媒體公關及對外聯絡事宜，及人力資源之配置及應變。

#### 財務中心：

本公司財務中心負責財務風險的評估。

#### 資訊處：

本公司資訊處負責強化資訊安全管理，對於資訊資產之機密性、完整性、可用性與不符合相關法規要求所可能面臨之風險進行控管，以有效及合理地降低企業營運風險。

#### 各業務及管理單位：

各部級主管及單位主管應於日常管理作業中，進行風險評估及管控，強調全員全面風險控管，平時落實層層防範，以利本公司將所涉風險控制於可承擔之範圍。

114 年度主要運作情形如下：

(一)董事會已於 110 年 8 月 5 日通過本公司風險管理政策與程序。

(二)各執行單位針對風險辨識及針對潛在風險提出管控策略與作法。(如下表)

(三)由稽核室進行單位督導，以確保全體員工的風險管理意識及執行力度。

風險類別	潛在風險	管控策略與作法
氣候風險	天氣型態變動劇烈： 天災、缺水、斷電進而影響生產	<ol style="list-style-type: none"> <li>1. 各廠區與當地政府溝通協調，將廠區列為供電、供水優先區</li> <li>2. 投入防災措施與定期保養維護。</li> <li>3. 原物料供應商的所在區域風險有效性評估。</li> <li>4. 各廠區導入相關能源管理系統，評估再生能源裝置可能性。</li> <li>5. 各廠區設置防水與排水系統與緊急應變措施。</li> </ol>
環境風險	全球氣溫升高 (溫室氣體排放量增加)	<ol style="list-style-type: none"> <li>1. 進行溫室氣體盤查並通過第三方驗證，合併財務報表所有營運據點皆已完成 ISO-14064 查證。</li> <li>2. 進行設定科學基礎減量目標 (SBT, Science Based Targets)，已於 2022 年 8 月完成減量目標審核，台北總部及各廠區持續進行各項節能減碳措施。</li> <li>3. 增加高能效產品研發投入，減少產品碳排放量。</li> <li>4. 增加產品環保材料之比例，減少不可回收廢棄物產生。</li> </ol>
職安衛風險	員工職場安全	<ol style="list-style-type: none"> <li>1. 台北總公司、東莞廠、蘇州廠、重慶廠及泰國廠皆已完成 ISO 45001 職業安全衛生管理系統驗證。</li> <li>2. 台北總部及廠區環安衛小組進行定期現場巡視，降低危害風險。</li> <li>3. 實施作業環境監測，確認工作場所環境不會對同仁健康造成影響。</li> </ol>
	火災爆炸風險	<ol style="list-style-type: none"> <li>1. 針對電烙鐵及高溫加熱設備的安全使用 (如熱風槍、熱熔膠槍等) 已制定相關規範並定期宣導，要求同仁重視火災爆炸風險。</li> <li>2. 除原有電烙鐵管控措施外，並實施電烙鐵實名制，確保每台電烙鐵都有進行保管及維護。</li> <li>3. 現行高溫加熱設備無法自動降溫者，需加裝自動斷電之倒數計時器，以及防呆護蓋，減少誤觸可能。</li> </ol>
	員工健康管理	<ol style="list-style-type: none"> <li>1. 資深員工健檢：自 2024 年起將主管人員到院高階健檢套組擴及年資滿 5 年以上的資深員工，每三年一次高階健檢套組，讓員工能夠享有全方位的健康照護。</li> <li>2. 針對高風險員工進行健康關懷及追蹤，隨時留意同仁健康。</li> <li>3. 定期實施環境消毒，提供同仁健康環境。</li> <li>4. 流感疫苗施打。</li> <li>5. 健康職場認證。</li> </ol>
資訊風險	<ol style="list-style-type: none"> <li>1. 資訊系統異常</li> <li>2. 遭外部惡意攻擊入侵破壞系統</li> </ol>	<ol style="list-style-type: none"> <li>1. 每年完成國際資安認證 ISO 27001 定期稽核並維持認證。</li> <li>2. 本公司全體同仁、委外廠商及其協力廠商，均須簽署保密聲明書與相關協議。</li> <li>3. 定期推動資訊安全宣導與教育訓練，每季發布資安公告，提升全體同仁的資安意識與防護能力。</li> <li>4. 所有操作須遵循資訊安全政策及相關法規，並正確使用個人帳號、密碼與系統權限，須定期更新，以降低帳號遭盜用之風險。</li> <li>5. 公司定期建立與更新資訊資產清單，依據風險評估結果採取適當之風險管理措施，並制定配套控管方式。</li> <li>6. 重要資訊系統全面導入多層次防禦機制，自網路邊界(例：內外防火牆、入侵偵測系統、入侵防禦系統)至終端設備(例：防毒軟體、資產盤點系統)皆設置資安防護，並建立備援及即時監控機制。</li> <li>7. 每年定期執行系統與應用程式弱點掃描，針對高風險以上的弱點立即進行修補與調整。同時，已導入 MDR (Managed Detection and</li> </ol>

風險類別	潛在風險	管控策略與作法
		<p>Response)託管式偵測與回應服務，透過即時監控和專業分析，有效降低異常事件的發生率，提升威脅偵測與快速回應能力。</p> <p>8. 為降低電子郵件相關威脅風險，本公司已導入 BEC(商務郵件詐騙防護)與 APT(進階持續性威脅防護)模組進行智慧化過濾，防堵詐騙與惡意攻擊。</p> <p>9. 嚴禁安裝未經授權軟體，以避免惡意程式或未明風險進入公司網路。所有硬體更換及軟體安裝作業，由資訊處專責人員統一執行，以降低資安風險並提升資產管理效率。</p> <p>10. 為避免因私人行為造成資安風險，本公司規定嚴禁同仁攜帶或使用私人電腦於公司環境。此舉旨在降低外部裝置攜入惡意軟體或不當存取之風險，確保辦公環境與系統安全，保障公司營運及客戶資訊資產完整性。</p>
財務風險	匯率波動風險	對於進銷貨美元應收、應付帳款部位採相互抵銷之自然避險，對於抵銷後之美元淨部位及未來可能產生之流量，持續注意國際經濟情勢，掌握國際匯率走勢，以適時承作遠期外匯交易之方式進行避險。

本公司「企業永續發展委員會」已於 114 年 11 月 11 日董事會中報告與公司營運相關之環境、社會、公司治理重大議題及其風險管理之相關運作及執行情形。