111 年公司營運風險評估及風險管理政策

本公司依據重大性原則，進行與營運相關之風險評估：

項目	風險說明	111年運作情形
營運風險	營運風險包括客戶信用風險、交期太長或延遲交貨風險、原料供應及價格波動風險、存貨呆滯風險、生產線人力風險等。	1. 透過每月的主管會議，可防範或解決營運產生的問題，包括客戶信用、交期太長或延遲交貨、生產線因疫情影響而需人力調配、原料價格波動而調整採購政策等等。111年度並未有因疫情而影響生產線運作之情形，應收帳款也未有發生無法回收之情事。 2. 每月的鑽頭存貨會議及每季的螺絲及線材存貨會議討論存貨狀況，擬定高庫齡存貨去化策略，並定期追蹤去化實績。
財務風險	包括因利率、匯率等波動產生之市場風險等	1. 本公司截至111年底長短期借款餘額為　　千元，利息費用佔稅前淨利之比率近　%，故利率變動對本公司損益影響尚屬有限；若利率增加1%，在所有其他變數維持不變之情況下，將使本公司稅前淨利減少　　千元。 2. 匯率風險方面透過預售遠期匯率方式鎖住匯率變動風險，維持訂單預期的利潤。另亦可於業務部銷售產品報價時考量因匯率變動連帶產生之售價調整，以保障應有之利潤，並以相

		同進貨幣別之外幣報價，以降低匯率風險。
勞動安全風險	包含未依照相關勞動相關法規規定，造成勞工臨時性或永久性之意外傷害之不確定性事件，亦包含超時工作及不合理剝奪員工福利等。	1. 本公司111年度並未發生職業安全相關傷害事件，亦未有勞工局接獲員工投訴公司之情事。 2. 實施危害鑑別與風險評估，防止職業災害。 3. 定期舉辦衛生安全座談、消防演練及勞工安全衛生座談等加強員工職業安全意識。公司每年第三季進行消防演練、化學品演練，加強員工緊急應變能力。
資訊安全風險	包括資訊系統當機、個資外洩、駭客入侵、ERP資料毀損或遭入侵等，造成公司營運資訊外洩或無法運作，對公司運營產生影響。	1. 111年度本公司未有因資訊安全問題而使公司系統無法運作之情事。 2. 本公司已制定資訊安全管理政策，設立資訊課；並由稽核單位，進行管理制度內部查核、資訊安全預防及危機處理等具體管理方案。相關具體執行措施如下： (1) 網路安全管理：配置多功能防護型防火牆，阻擋駭客非法入侵。 (2) 配置上網行為管理系統，控管網路存取，可屏蔽訪問有害或政策不允許的網址及內容，強化網路安全且防止頻寬被不當佔用。 (3) 帳號的密碼設置，需符合規定之強度，且需文數字參雜，才能通過。 (4) 同仁辦理離職手續時，需會辦資訊課，進行各

		系統帳號刪除作業。 (5) 伺服器與同仁電腦設備皆安裝端點防護軟體，病毒碼採自動更新，確保能阻擋最新型病毒。電子郵件伺服器配置有垃圾信過濾機制，防堵病毒或垃圾郵件進入使用者端PC。 (6) 不定期宣導最新型資安防護訊息，例如：勒索軟體、釣魚郵件、詐騙網址連結。 (7) 本公司電腦主機、各應用伺服器……等皆設置於專用機房，機房門禁採實名制登記進出，且保留記錄存查。資訊機房內有獨立空調及不斷電系統，以維持電腦設備於適合的溫度下運轉，斷電時不會中斷電腦應用系統的運作。 (8) 建置備份管理系統，定期將每日備份的資料，一份保留在機房，另一份放於異地(路竹廠或外接備份裝置)，互相備援。定期實施災難復原演練，選定還原基準點後，由備份檔回存於系統主機。

本公司每年安排至少一次向董事會報告風險管理運作情形，111年度風險管理運作情形報告將於112年第一次董事會報告