

人權政策具體作法

本公司為善盡企業社會責任，承諾提供員工安全且友善之工作環境並尊重支持國際公認之人權規範與原則，包含「聯合國世界人權宣言」及國際勞工組織的「工作基本原則與權利宣言」，亦恪遵國內之「勞動基準法」、「性別工作平等法」、「職業安全衛生法」等相關勞動法規，杜絕任何侵犯及違反人權的行為而制定本公司人權政策如下：

人權政策	2023 年執行情形
<p>一、 保障勞動人權</p> <ol style="list-style-type: none">1. 本公司承諾遵循適用之相關勞動法令及勞工人權標準，禁止雇用童工及強迫勞動，工時管理及薪資待遇合乎相關規定。2. 公平的對待與尊重每位員工，不以殘暴、侮辱、虐待等不人道方式對待員工重視就業平等，不因任何種族、階級、語言、思想、宗教、黨派、籍貫、出生地、性別、性傾向、年齡、婚姻、容貌、五官、身心障礙、以往工會會員身分或其他法律保護等情況產生就業歧視。3. 成立勞資會議以提供勞資雙方 順暢之溝通管道，維持和諧之勞資關係。4. 制定《性騷擾防治措施、申訴及懲戒辦法》，設置性騷擾申訴處理委員會，定期舉辦教育訓練，提供員工及求職者免於性騷擾之工作環境，禁絕工作場所性騷擾事件之發生。	<ol style="list-style-type: none">1. 本公司召開勞資會議，勞資雙方就勞動條件相關議題（例如調班、特休假相關議題）充分溝通並達成協議。2. 公司嚴禁進用童工與就業歧視並規範於員工任用相關辦法。隨時關注政府法規脈動，並配合制修公司內部相關規定。3. 因應 ISO 45001 執行"職務遭受不法侵害預防計畫"，舉辦職場不法侵害教育訓練，協助同仁確保免於職場不法侵害之工作環境。4. 公司設立「員工意見箱」及電子郵件 whistleblower@ystech.com.tw 作為員工申訴管道以強化勞雇合作關係，並依「申訴舉報處理程序」處理申訴案件。5. 2023 年度元山科技無任何強迫勞動、侵犯員工權益或違反人權的申訴案件。6. 2023 年以電子郵件進行性騷擾防治宣導：「執行職務遭受不法侵害預防宣導」遇到性騷擾勇敢 SAY 『NO』。

<p>二、 維護安全勞動環境</p> <ol style="list-style-type: none"> 1. 提供員工安全且健康之工作環境，遵循相關法規，致力推動職業安全衛生教育訓練，確保工作環境與人身安全保護措施之觀念落實，持續改善工作環境的安全與衛生條件，降低職業災害的風險，確保員工身心健康及權益。 2. 協助員工維持身心健康及工作生活平衡，辦理員工健康檢查，預防潛在健康風險 3. 提供員工多元化活動，透過社團參與以拓展同仁間的互動交流；與外界公司辦理「企業內子女托育服務」，協助員工解決托育問題。 	<ol style="list-style-type: none"> 1. 定期舉辦職業安全衛生教育訓練受訓人次如下： <ol style="list-style-type: none"> (1)2023 上半年度緊急救護訓練：35 人/1.5 小時 (2)2023 下半年度緊急救護訓練：34 人/1.5 小時 (3)元山官田緊急救護教育訓練：5 人/2 小時 (4)一般職業安全衛生教育訓練：388 人/3 小時 (5)每年舉行一次之評核作業，落實職場平等的工作環境。 (6)新人教育訓練進行緊急應變訓練 2. 重視員工健康預防潛在健康風險 <ol style="list-style-type: none"> (1)編列預算確實執行二年一次員工健康檢查 (2)每年一次員工肌肉骨骼及異常負荷之調查 (3)安排醫師定期蒞臨公司，針對健康檢查異常、母性保護、呼吸防護的人員進行訪談 (4)每年一次工作負荷評估與管理、人因性危害預防、母性健康保護、職場暴力預防等健康諮詢 (5)2023 年以電子郵件進行健康宣導：「『工作場所母性健康保護預防宣導』6 分鐘護一生 創造健康的人生」、「『人因性危害預防宣導』低頭族必學~遠離 3C 症候群」、「『異常工作負荷促發疾病預防宣導』別因過勞讓身體洩了氣」、「歲末防寒 迎向新年「心」健康」等主題 (6)多元活動，舉辦年度春酒、企業家庭日、員工旅遊、社團活動 (7)為防止公司意外事故發生，建立各廠區緊急通報處理流程，並於各廠區指定經

	<p>合格緊急救護教育訓練(一年2次)之同仁為急救人員。</p>
<p>三、 個資保護及資訊安全</p> <p>為保障員工、客戶、供應商及其他利害關係人之隱私權，個人資料之蒐集、處理及利用均尊重當事人之權益，以誠實及信用方法為之</p>	<ol style="list-style-type: none"> 1. 對於應聘者與員工因配合本公司蒐集個人資料時，其所提供之個人資料，嚴格遵守個人資料保護法之相關規定，涉及個資檔案皆加密處理以確保個資使用安全。 2. 建立從外部防火牆到內部防毒軟體、加密線路等的防禦機制，提高入侵難度。 3. 管理網路使用者的權限，包含 E-mail、即時通訊、一般網路瀏覽均需申請後，經過核決流程後，方得開放使用權限，同時監控、記錄使用者的網路行為。 4. 加強電子垃圾郵件監控