「資訊安全，人人有責」，為保護資訊資產，包括人員、設備、系統、資訊、資料及網路等之安全，免於因外在之威脅或內部人員不當的操作，遭受洩密、破壞或遺失等風險，需要持續精進風險管理，不斷地強化治理策略、人員訓練，並進行考核審查與配套措施等諸要項。其願景在於打造堅實、安全、與可信賴的企業數位環境，提供企業永續經營的堅固基石。以下闡述諸項具體要件：

治理策略

為落實與提升資訊安全，公司成立資訊安全指導委員會(以下簡稱資安指委會)。資安指委會由公司資安主官擔任主席，各單位一級主管為當然委員，每年定期舉行委員會議。資安指委會的任務在於擬定與審核資安政策，全方位審視與監督資安政策的執行，持續提升資訊安全防護能力，降低資訊安全風險。會議內容視需求向董事會提交報告並整理要項列入企業年報。

資安組織

企業組織因人而成事。公司設立資安主管，下轄產品開發暨資安平台小組、工網資安小組、IT 資安技術小組、資安稽核小組、資安教育訓練小組，執行資安政策及人員教育訓練並落實資安工作，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性。

資安指委會下轄產品開發資安暨網路安全會議、工網資料安全檢核會議、IT 資安資源暨技術會議、稽核及缺失檢討改進會議，提供跨單位資訊安全會報，負責資安政策之審核及資訊安全管理制度之推動事宜

人員訓練

企業成員的資訊安全意識為公司資訊安全的基石。歷年來透過內部訓練的方式，使各單位成員熟悉資安相關課程，鼓勵成員參加必要之資安認證考試，並優先延攬通過認證考試的新進人員，以力求企業資安 DNA 的良性進化。現今更導入線上教育系統，使企業成員能更有效率、更多元化學習所需的資安課程。系統並提供單元學習檢測，透過量化學習成果與系統自動產生的統合報表，大幅提升管理階層對訓練成果的能見度，並利於將學習成績納入 KPI 考核標準。

考核審查

以風險管理為核心的資安防護，藉由網路設備的軟硬體系統所匯集的流量分析、異常偵測、樣態分析、軟體更新等資訊，構建出智能化的即時資安信息；並透過自動化、可視化、與可量化的控管系統，為早期預警、持續監控、通報應變、與協助改善等標準流程，奠定堅實的基礎；並可充分為事前、事中、事後的事件分析，提供必要的數位化資訊。

為求精確量化，所有事件均標示嚴重等級與對應分數，經由自動化系統評判事件積分，即時知會相關人員並自動登入事件管理系統。管理階層更能透過資安管理系統，多角度深入掌握系統現況，作為日後考核審查與評判資安風險之依據。

資安政策

資安威脅無所不在，網路病毒、木馬程式、間諜程式、勒贖軟體、阻斷式攻擊、社交工程等不計其數。近年來由於網路連結與頻寬的急速發展，加上爆量的加密資料傳輸，巨大的資訊流量促使資安系統必須靈敏地與時俱進，並須結合下列的框架與相應措施，才能更完善、更周延地進行資安防護:

a. **前端使用者**：必須遵照資安政策，以及作業系統與企業網域制定的策略條款規範，並配合進行必要的系統更新，以有效阻絕電腦病毒、木馬程式、惡意程式等，提供第一線的安全防護。
b. **企業數據中心**：引進新世代防火牆，有效且即時過濾加密資料，依應用程式類型進行控管，並提供資安管理系統必要的信息，以利自動化分析。
c. **機密資料集中化**：對於公司重要機密資料，應加以集中、避免分散；統合最新資安技術，對於機密資料的存取進行管理監控。對於需要落地的機密資料，應注意落地後的保護與管理，全方位保護公司重要資產。
d. **資料備份管理**：採用先進備份系統，對重要資料依照不同時序與管理計畫，進行全備份、遞增備份、異地與離線備份等方案。所有離線與異地備份資料，均須經過加密處理，並定期抽檢演練，以確保其可還原性。
e. **資安管理數位化系統**：統合企業海量的網路流量信息、各式防毒系統、防駭系統等系統日誌、不定期健檢掃描與滲透測試的系統日誌，經由內部大數據分析處理系

統，予以量化評分，並依不同面向呈現給不同的管理成員，以達信息分類、風險分級、與管理分層的目標，據以防微杜漸並縮小資安威脅對企業營運的衝擊。

資安風險與因應措施

為確實強化資安防護，瑞昱進一步辨識資安風險項目，並個別提出因應措施且定期檢視成效。

辨識資安風險項目	影響評估說明	因應措施	成效管理
個人電腦帳號密碼保全	避免業務機密被有心人士竊取	個人電腦開機密碼定期修改	定期修改密碼，密碼規則有一定的複雜度
資訊安全	資訊系統授權須經由正式的申請流程，並保留紀錄	因應職務上所需資訊，建立申請授權流程	電子表單申請，經由申請人主管及權責單位同意後開放
電腦病毒防護	電腦病毒日新月異，勒索病毒層出不窮，防不勝防	定期更新病毒定義檔，由系統自動派送到個人電腦	強化個人電腦資料的安全
網路管理安全	維護網路防火牆的穩定，阻擋蓄意的攻擊	定期更新韌體與備份	強化網路傳輸的品質
對外上網行為的安全	阻擋與重新導引惡意網域與 IP 位址的存取，限制惡意軟體、網路釣魚、殭屍電腦的命令與控制伺服器等不當傳輸行為	導入企業威脅防護(Enterprise Threat Protector, ETP)防護機制	強化使用對外網路的存取安全