壹、 目的：

為強化治理並確保集團穩健經營與永續發展，對可能威脅集團營運的不確定因素進行風險管理，與訂定危機處理作業流程，以資遵循。

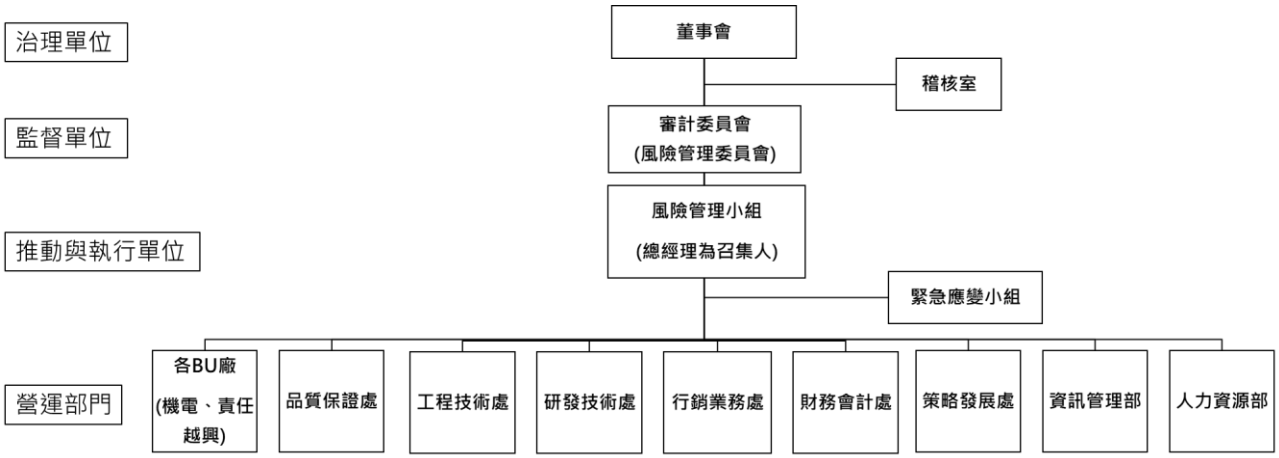
貳、 範圍及依據：

一、 本公司及所屬子公司。

二、 台灣證券交易所-上市上櫃公司風險管理實務守則。

參、 權責：

一、 組織：



二、 職掌：

(一) 董事會：

1. 核定風險管理政策、程序與架構。
2. 確保營運策略方向與風險管理政策一致。
3. 確保已建立適當之風險管理機制與風險管理文化。
4. 監督並確保整體風險管理機制之有效運作。
5. 分配與指派充足且適當之資源，使風險管理有效運作。

(二) 審計委員會：

1. 審查風險管理政策、程序與架構，並定期檢討其適用性與執行效能。
2. 核定風險胃納（風險容忍度），導引資源分配。
3. 確保風險管理機制能充分處理公司所面臨風險，並融合至日常營運作業流程中。
4. 核定風險控管的優先順序與風險等級。
5. 審查風險管理執行情形，提出必要之改善建議，並每年定期向董事會報告。
6. 執行董事會之風險管理決策。

(三) 風險管理小組：

1. 擬訂風險管理政策、程序與架構。
2. 擬訂風險胃納（風險容忍度），並建立質化與量化之量測標準。
3. 分析與辨識公司風險來源與類別，並定期檢討其適用性。
4. 每年彙整並提報公司風險管理執行情形報告。
5. 協助與監督各部門風險管理活動之執行。
6. 協調風險管理運作之跨部門互動與溝通。
7. 執行風險管理委員會之風險管理決策。
8. 規劃風險管理相關訓練，提升整體風險意識與文化。

(四) 營運部門：

1. 負責所屬部門之風險辨識、分析、評量與回應。
2. 每年定期提報風險管理資訊予風險管理小組。
3. 確保所屬部門風險管理及相關控制程序有效執行，以符合風險管理政策。
4. 日常管理與監督，必要時建立相關危機管理機制。

(五) 緊急應變小組：

因應重大風險、危機與異常事件成立臨時性小組，由總經理召集人員對應與處置各項重大事件，並知會稽核室。

(六) 稽核室：

對風險管理進行查核，確保符合規定與控管程序。

肆、 名詞定義：

一、 風險管理：為有效管理可能發生事件及最小化其不利影響，所執行之步驟與過程。

二、 危機處理：為避免或降低危機對組織之傷害，對危機情境維持一種持續性、動態性之監控及管理過程。

伍、 作業流程圖：

無。

陸、 作業內容：

一、 風險管理流程包括：風險辨識、風險分析、風險評量、風險回應(處理)，及監督與審查機制(監控風險)。

(一) 風險辨識：找出集團可能面臨之各項風險，由各營運部門依據集團目標及董事會核定之風險管理政策與辦法，就其所屬部門目標與業務執掌進行風險辨識。

1. 透過適當之分析工具及方法(如流程分析、情境分析、問卷調查、PESTLE 分析等)，依據歷史、當前的資訊及未來趨勢，考量內外部風險因子、利害關係人關注重點等，透過由下而上及由上而下的分析討論，結合策略風險與營運風險，全面辨識可能導致集團目標無法達成、造成集團損失或負面影響之潛在風險事件。
2. 營運部門辨識風險時，應系統性完整考量部門之風險因子，評估可能面臨的風險項目，不應由特定部門負責辨識單一風險項目。
3. 集團風險管理範疇，主要包括但不限於下列項目，如有其他風險未列出，各部門應依據營運狀況予以辨識，並納入風險管理流程。

風險項目	定義與描述
災害風險	安全防護暨緊急應變，係指重大危害事件發生機率與損失的風險。
營運風險	係指銷貨集中、採購集中、員工暴動、抗爭、罷工事件、法律遵循、招募及留任人才等風險。
財務風險	指市場風險、信用風險、流動性風險、作業風險...等。
策略風險	包括單一地區過度集中之風險、客戶集中/大客戶影響、代理線集中/大產品線影響、產業集中、併購智慧、財產權保護、企業形象及塑造與維護...等。
資安風險	在資訊系統運作過程中，遭受到外力威脅時，因資訊資產本身存在的弱點所可能引發的各種威脅，例如資料處理錯誤、網路損壞、設備/資料遭竊、軟體錯誤、病毒木馬，或是資訊服務停機...等。
品質風險	因產品設計、生產製造、供應鏈管理及儲存與出貨...等各種流程，未達當地法令或品質規範要求，所造成的品質不確定。

(二) 風險分析：對已辨識風險事件之性質及特徵進行瞭解，並分析其嚴重度(S)、發生度(O)與偵測度(D)，據以計算風險優先指數(RPN)。

1. 各營運部門應針對已辨識出之風險事件，考量現有相關管控措施之完整性、過往經驗、同業案例等，分析風險事件之嚴重度、發生度與偵測度。
2. 依集團風險特性擬定適切的量化或質化量測說明，作為風險分析之依據。
   (1) 風險優先指數之嚴重度(S)依如下評量表予以評估。

嚴重度數值	影響程度	財產損失	業務運作	人員傷亡
3	嚴重	損失達 NT$1,000 萬元(含)以上	停工 5 天(含)以上	死亡

2	中度	損失達 NT$200 萬元(含)~NT$1,000 萬元(不含)	停工 1 天(含)以上，未達 5 天	重傷
1	輕微	損失達 NT$10 萬元(含)~NT$200 萬元(不含)	停工未達 1 天	輕傷

(2) 風險優先指數之發生度(O)依如下評量表予以評估。

發生頻率數值	發生可能性(機率)	詳細敘述
3	非常可能（61-100%）	一年內大部分的情況下會發生
2	可能（31-60%）	一年內有些情況下會發生
1	不太可能（0-30%）	一年內只有在少數情況下會發生

(3) 風險優先指數之偵測度(D)依如下評量表予以評估。

可偵測度數值	可事前檢出或發現之機率	詳細敘述
3	不太可能（0-30%）	幾乎沒有機會於事件發生前檢出
2	可能（31-60%）	有機會於事件發生前檢出
1	很有可能（61-100%）	有高機會於事件發生前檢出

3. 風險胃納(容忍度)提報並經核定，決定可承受之風險限額區分為：極度風險、高度風險、中度風險與低度風險，作為後續風險評量與風險回應之依據。

(三) 風險評量：透過風險分析結果與風險胃納加以比對，決定需優先處理之風險事件，並作為後續擬訂回應措施選擇之參考依據。

1. 各營運部門彙整出各項風險項目，依據風險嚴重度、發生度與偵測度評量表，評估風險事件之各項數值，建立風險優先指數。其計算公式：風險優先指數(RPN) = 嚴重度(S) x 發生度(O) x 偵測度(D)。
2. 依核定之風險等級，比對風險優先指數規劃與執行風險回應方案。

風險等級	風險優先指數	風險回應方案
極度風險	18-27	營運部門應立即評估與提報可行性與方案，經總經理核可後投入資源降低風險，由該部門持續監控與回報，確保風險有效掌控與降低。
高度風險	8-12	營運部門應研擬計畫與提供資源降低風險，由

		部門一級主管督導所屬部門持續監控與回報。
中度風險	4-6	部門一級主管應督導所屬部門，並明定責任歸屬做必要監督。
低度風險	1-3	落實營運部門日常管理與監督。

3. 各營運部門彙整相關風險分析與評量結果，記錄到「風險評估與處理彙整表」(表單編號：4P-SD-16-01)，作為後續風險回應措施之參考。

(四) 風險回應(處理)：降低並最小化風險對集團之負面影響，針對風險回應訂定相關處理計畫，確保相關人員充分理解與執行，並持續監控相關處理計劃之執行情形。風險處理流程說明如下：

1. 列出可行的風險對策，其基本原則如下：
   (1) 接受：風險在可容忍範圍內，落實日常管理與預防。
   (2) 規避：風險在可容忍範圍外，處理成本高於利益時，採取不涉入或退出風險。
   (3) 降低：依據風險評量結果，研議及採取適當內部控制或其他機制，降低風險發生之可能性及影響程度，或提高事件檢出能力，將風險控制在可容忍範圍內。
   (4) 移轉：藉由其他團體承擔或分擔部分風險，降低風險影響，例如購買保險或業務委外。
2. 評估並選擇風險對策：評估風險對策之可行性、成本及利益，排列風險對策之優先順序，並選擇適當的風險對策。
3. 準備處理計畫：針對所選擇之風險對策，訂定權責分工、處理流程、資源及預算分配、預期績效及階段目標之處理計畫。
4. 執行處理計畫：依據所訂定之處理計畫據以執行。
5. 紀錄部門殘餘風險表：經各部門新增風險對策與執行處理計畫後，現有風險優先指數將可降低，再據以重新評定其指數並彙整至「風險評估與處理彙整表」。
6. 應考量集團目標、內、外部利害關係人觀點、風險胃納及可用資源，來擇定風險對策，使風險回應方案在實現目標與成本效益之間取得平衡。
7. 為降低風險所造成的損失，營運部門得依業務狀況評估、規畫與執行演練計畫，或依當地法令要求進行演練。
8. 「風險評估與處理彙整表」應作為附件檢附至 OA 系統「聯絡通知單」(文件編號 4P-SD-04-01)，呈送主管及風險管理小組簽核。

(五) 監督與審查機制(監控風險)：風險管理小組應確實審查風險管理流程及相關風險對策是否持續有效運作，並將相關審查結果納入報告事項中，並不斷檢討與改進。

1. 營運部門應持續監控風險，並檢討風險是否仍然存在或已改變，以及新風險是否出現，當風險顯著改變時，應修改「風險評估與處理彙整表」，確保有效控制管理風險。
2. 風險管理小組應於上下半年各召開一次會議，彙整與報告風險管理執行結果。
3. 當營運部門監控或發現風險優先指數達極度風險時，應立即依風險回應(處理)流程執行作業，並實施管理與監督。

二、 風險管理過程中辨識或未辨識出之風險，因故失控而導致風險情境發生時，迫使集團立即進入危機處理。危機處理流程包括：危機應變、危機溝通、危機復原、經驗學習。

(一) 危機應變：

1. 分析研判危機發展狀況，儘速發掘問題核心與釐清危機可能涉及之層面，並於蒐集資訊、診斷危機、確認控制對策及處理行動後，立即處理危機重點，避免危機擴大，迅速解除危機。
2. 依據危機影響程度，由該部門權責主管施行適度之緊急應變措施後，應盡速回報各級主管事件狀況。
3. 危機應變處理原則：

嚴重度(S)	應變處理原則
嚴重	1. 八小時內由該部門進行控制、決策可行性評估與初步處置規則。 2. 總經理召集必要之部門主管，成立緊急應變小組並指定權責主管負責危機應變與處理。
中度	1. 二十四小時內由該部門進行控制、決策可行性評估與初步處置規則。 2. 如危機屬於跨部門，則由總經理指定權責主管負責危機應變與處理。
輕微	由各營運部門主管進行決策可行性評估與處置。

(二) 危機溝通：

1. 透過平時建立之內、外部即時通報窗口及機制，取得利害關係人之瞭解與協助。
2. 內部通報：

(1) 依事件影響程度通報各級主管，必要時總經理得依狀況召集相關部門主

管，確立指揮系統，並即時協調整合相關部門與資源。

(2) 通報方式以能迅速報告主管之工具為主，簡述事件發生狀況與緊急處理方式，必要時，不限口頭或文字等方式，盡速取得上級主管緊急對策核可。

(3) 事件處理過程中應定期向上級主管回報進度，並留存相關通報與處理紀錄。

3. 外部聯繫：

(1) 統一由發言人對外公開說明，集團同仁不得任意對外發言，違者召開人事評議委員會懲處。

(2) 發生事件如涉及重大消息之範圍者，依「內部重大資訊處理作業程序」(文件編號：2P-FI-13)執行。

4. 通報規定與說明：部門各級主管收到通知時，應依情節通報上級主管。

嚴重度(S)	緊急通報時限與說明
嚴重	部門一級主管應於一小時內通報董事長與總經理，如牽涉對外聯繫與公共關係等事件，須通報公司發言人；如危機影響屬跨部門，需一併通報相關部門。
中度	部門一級主管應於八小時內通報總經理，得依情節通報董事長；如危機影響屬跨部門，需一併通報相關部門。
輕微	部門主管應通報部門最高主管，得依情節知會總經理與相關部門主管。

(三) 危機復原：

危機暫告段落後，應查核損失並回報部門主管，依情節制定與施行復原措施，最終必須確認部門之運作恢復正常。

(四) 經驗學習：

1. 危機處理完竣後，應依經驗及事實，檢討危機處理之前因後果及評估其有效性，據以訂(修)相關辦法與作業。

2. 檢討部門(包括緊急應變小組)運作與決策有無缺失或改善空間，必要時進行人事調整及獎懲。

3. 事件嚴重度如達中度與嚴重，危機處理結果由該權責部門填寫「危機事件處置表」(表單編號：4P-SD-16-02)，詳述事件發生原因、過程、處置與最終結果，並將此表單作為附件檢附至 OA 系統「聯絡通知單」，呈送權責、相關主管及風險管理小組後，仍應納入風險管理機制持續予以監控，以防止此危機及類似風險

再發生。

4. 該權責部門應作成知識管理教材，俾供傳承、學習及改進，以建立未來處理能量，且應依不同影響程度作成內部知識管理，說明如下：

嚴重度(S)	內部知識管理說明
嚴重與中度	發生部門應完整紀錄危機處理過程，並做成知識管理教材，上傳到興學堂供集團同仁警惕與學習。
輕微	各部門應建立危機處理資料庫，供內部經驗傳承。

三、 投資人關係課應每年定期於官網揭露下列風險管理相關資訊，提供外部利害關係人參考，並持續更新。具體應揭露項目包含：

(一) 風險管理政策與程序。

(二) 風險治理與管理組織架構。

(三) 風險管理運作與執行情形（包含向董事會報告之頻率與日期）。

四、 風險管理小組應隨時注意國內與國際企業風險管理機制之發展，據以檢討改進集團所建置之風險管理架構，以提升集團治理成效。

五、 本辦法經董事會通過後實施，修正時亦同。

柒、 參考文件

一、 內部重大資訊處理作業程序（文件編號：2P-FI-13）

捌、 產出表單：

一、 風險評估與處理彙整表（表單編號：4P-SD-16-01）

二、 危機事件處置表（表單編號：4P-SD-16-02）