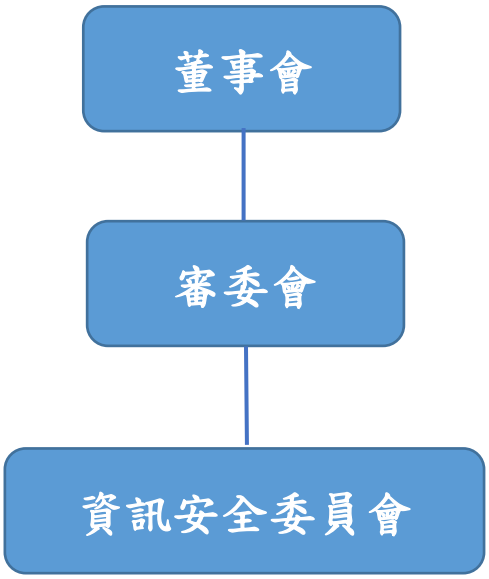
本公司於民國 111 年設立「資訊安全委員會」，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核，由營運管理部最高主管每年向董事會及審計委員會彙報資安管理成效、資安相關議題及方向。

資訊安全委員會由本公司營運長擔任召集人、資訊人員、營運管理單位、法務單位各委派 1 人為委員，內部稽核最高主管為觀察員，每年召開會議，檢視及決議資訊安全與資訊保護方針及政策，落實資訊安全管理措施之有效性。



益安生醫股份有限公司

資訊安全政策

一、政策目的：

本公司為了達到下列之營運與管理目標，訂定本政策。

1.公司之資訊化作業得以持續不間斷運作，維持內部制度管理之有效性，提升資訊服務品質。

2.確保處理與利用之所有資訊的可用性、完整性與機密性。

3.有關蒐集、處理與利用個人資訊之業務流程，符合個人資料保護法的要求。

二、適用範圍：

本公司全體人員、業務往來單位、委外服務廠商、訪客及使用本公司資訊服務之使用者等。

三、政策要求：

1.落實相關法令之遵循，包括智慧財產權保護法、個人資料保護法，以及與外部單位簽訂之協議、契約等。

2.由營運管理單位負責推動相關管理制度之計畫、執行與溝通協調，並積極辦理資訊安全與個人資料保護之教育訓練及宣導，以確保人員熟悉業務執行所負之安全責任。

3.員工因執行業務而持有之資訊資產以公有公用為原則，依其需求進行分類分級與風險評估，以達到有效控管；資訊化作業依業務執行之實際需求，規劃營運持續管理，以確保資訊化作業之可用性。

4.實體辦公環境及重要資訊設備機房均進行出入管制，以維持環境之安全。

5.為防範電腦病毒及惡意軟體影響作業，除經合法授權之系統及應用軟體外，禁止使用其他非授權軟體。

6.為確保管理制度之有效性，凡違反管理制度相關程序規範者，依相關規定審議懲處。

四、責任：

1.本公司成立管理組織統籌相關管理制度之推動。

2.管理階層應積極參與及支持管理制度，並透過適當的標準和程序以實施本政策。

3.本公司全體人員、委外服務廠商與訪客等皆應遵守本政策。

4.本公司全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

5.任何危及資訊安全與個人資訊保護之行為，將視情節輕重追究其民事、刑事及行政責任。

五、實施與修正：

本政策經資訊安全委員會審查通過，由總經理核定後實施，修正時亦同。

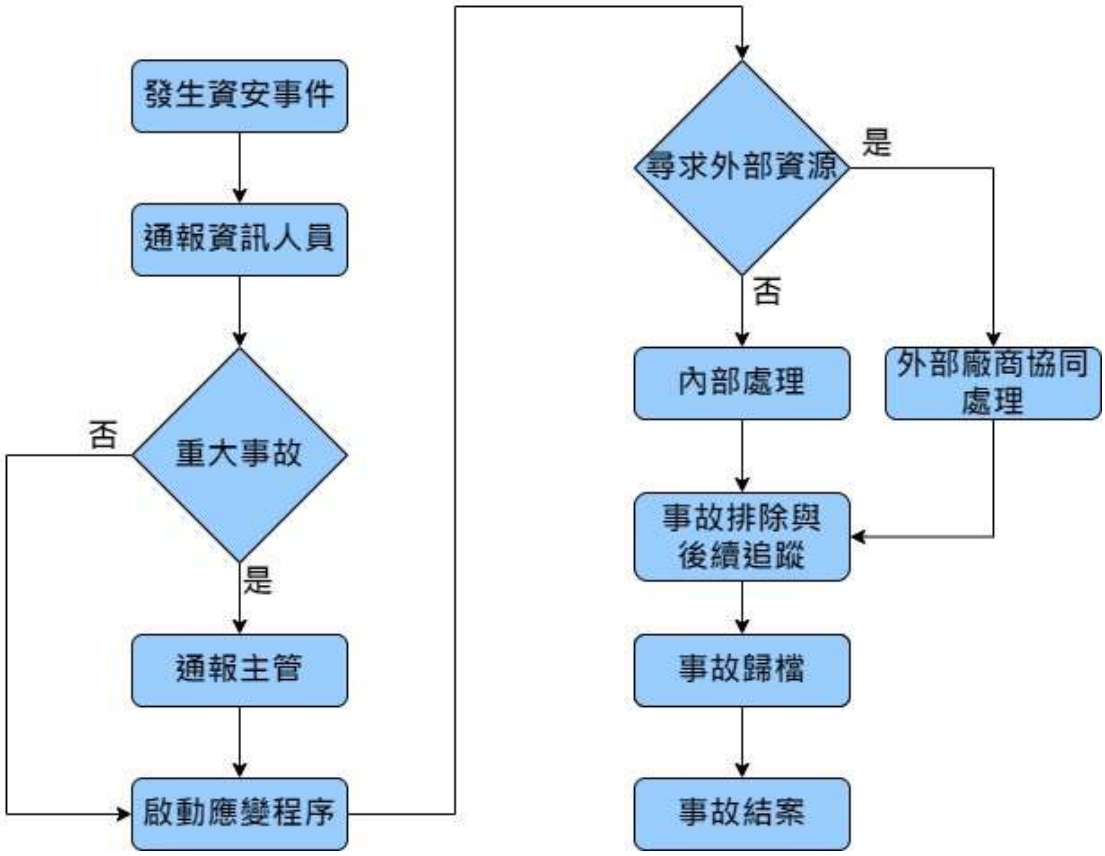
資訊安全的具體管理方案：

本公司考量資安險仍是新興險種，涉及資安等級檢測機構、理賠鑑識機構及不理賠條件等相關配套，因此經資訊安全委員會評估後，暫不購買資安險。本公司目前針對資安風險管理之主要措施與執行情形如下，已能有效防護資訊安全，並於 111 年 1 月 20 日提報董事會：資訊安全風險：強化資安宣導、內/外部存取管控、防火牆/病毒防護、資訊備份措施、本/異地備份機制、定期災害復原演練，並舉辦全體員工資訊安全教育訓練及社交工程演練，增加員工資訊安全防護概念。110 年度資安宣導及案例分享共 72 次，計有 2492 人次參與。
近期更因疫情影響，造成同仁因居家上班工作環境改變，故在評估風險後更導入了 EDR 的防禦措施，提升端點的安全性，來保護端點設備及伺服器的安全性。

項目	具體方案
防火牆維護	•防火牆設定連線規則，預設只開放基本上網、郵件連線。 •如有特殊連線需求需經高階主管核准始能開放。 •每月監控分析防火牆被攻擊數。
使用者上網管控機制	•自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。 •未經核准禁止使用網路硬碟、檔案傳輸等網路服務。
無線網路控管機制	•無線網路僅開放公務筆電和手機、平板等移動裝置使用，其餘裝置需經高階主管核准後始得開放。

項目	具體方案
	•不定期變更 Wifi 密碼 •依使用者裝置與需求，設定不同連線 SSID 控管連線主機的權限。 •訪客僅能使用獨立的無線網路直接連到外網。
網路活動檢視	•檢視網路設備、資安設備及伺服器之存取紀錄。 •識別異常紀錄與確認警示機制。
資訊機房安全管控	•設置獨立空調及滅火器，管制特定人員才能進出。 •機房有 UPS 不斷電系統，不正常停電時可自動將伺服器關機，保護伺服器系統不因停電而故障。
伺服器安全性設定	•須符合複雜性密碼原則。 •限制其登入次數鎖定原則。 •啟用帳號登入稽核原則。 •檔案存取權限依權限申請單進行設定。
防毒軟體	•使用多種防毒軟體，分散新病毒中毒機會。 •定時更新防毒軟體病毒碼，降低中毒風險。 •定期排程掃描，確定系統現況。
郵件安全管控	•有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 •個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。 •可統計使用者外部郵件收發件數與明細，監控異常收發狀況，避免機密資料外洩。
備份機制	•重要資訊系統資料庫皆設定每日完整備份。 •重要檔案每日進行備份一次。 •所有重要檔案皆有在異地辦公室存。 •每年不定期進行災難復原演練
機房點檢機制	•資訊中心檢查紀錄表紀錄機房溫濕度是否異常、資料備份等紀錄。
資安意識培養	•不定期進行資安宣導教育訓練。 •不定期資安新聞分享。 •每季進行一次社交工程演練。

資安事件通報程序：



資訊技術安全之風險及管理措施：

益安生醫已建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。這些網路攻擊以非法方式入侵益安生醫的內部網路系統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴重網路攻擊的情況下，益安生醫的系統可能會失去公司重要的資料。益安透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性，但不能保證公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業祕密及其他機密資訊，例如客戶或其他利害關係人的專有資訊以及益安生醫員工的個資。
惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導入本公司的網路系統，以干擾公司的營運、對本公司進行敲詐或勒索，取得電腦系統控制權，或窺探機密資訊。這些攻擊可能導致公司因延誤或中斷訂單而需賠償客戶的損失；或需擔負龐大的費用實施補救和改進措施，以加強公司的網路安全系統；也可能使本公司因涉入公司對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。

本公司未來也可能面臨因未及時更新而遭受攻擊。為了預防及降低此類攻擊所造成的傷害，本公司落實相關改進措施並持續更新，例如強化網路防火牆與網路控管以防止電腦病毒跨機台及跨網段擴散以及導入 Patch Management 對系統及應用程式進行更新的管控；依電腦類型建置端點防毒措施；導入先進的解決方案以偵測與處理惡意軟體；加強釣魚郵件偵測；

並定期執行員工警覺性測試。雖然本公司持續加強資訊安全防護措施，但仍無法保證公司免於惡意軟體及駭客攻擊。

此外，本公司需要分享高度敏感及機密的資訊給部分其雇用提供本公司及其全球關係企業服務的第三方廠商，以使其能提供相關服務。儘管本公司在和第三方服務廠商簽訂之服務合約中，要求其遵守保密及 / 或網路安全規定，但不能保證每個第三方服務廠商都將嚴守這些義務。由上述服務廠商及 / 或其承攬商所維護的內部網路系統及外部雲端運算網路（例如伺服器），亦會有遭受網路攻擊的風險。若本公司或其服務廠商無法及時解決這些網路攻擊所造成的技術性問題，或確保本公司（及屬於本公司客戶或其他第三方）的數據完整性及可用性，或控制住公司或其服務廠商的電腦系統，皆可能嚴重損及本公司對客戶和其他利害關係人的承諾，而公司營運成果、財務狀況、前景及聲譽亦可能因此遭受重大不利影響。

資通安全重大事件：

最近年度及截至 110 年 1 月 12 日止，暫無遭受重大資通安全事件，尚無因其造成之影響其損失可提供。