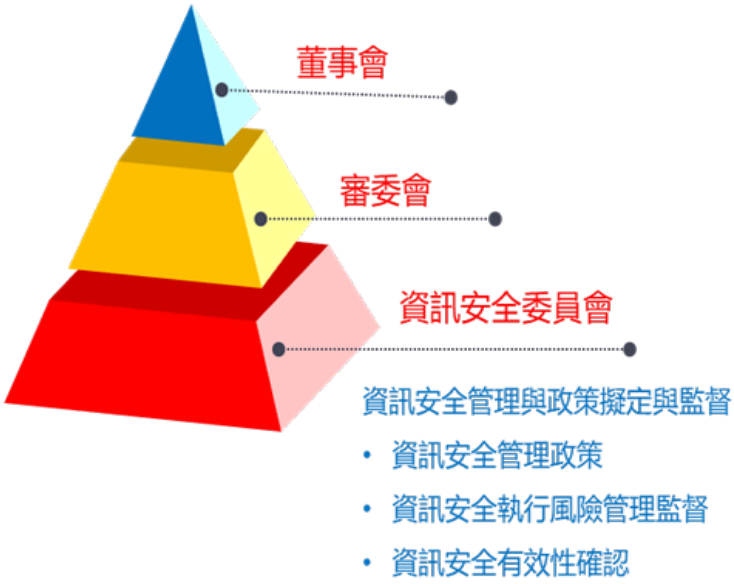
本公司業已於 115 年 1 月 23 日向董事報告資訊安全風險管理情形，相關內容節錄如下：

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執行副總經理擔任召集人、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：

為強化本公司資訊安全管理，建立可信賴之資訊處理環境，並確保各項業務資訊之安全性，特訂定本政策。本政策旨在達成下列目標：

1. 持續運作管理：確保本公司資訊化作業穩定運行，並建立災害復原機制，以維持業務連續性及行政管理之有效性。
2. 三位一體保護：確保資訊資產之機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），防止未經授權之存取、竄改或損毀。
3. 合規性維護：確保個人資料及業務資訊之蒐集、處理與利用，均符合「個人資料保護法」及相關法令規範，並尊重利害關係人權益。

二、適用範圍：

本政策適用於本公司全體同仁、派遣人員、與本公司有業務往來之供應商、委外服務廠商、訪客，以及所有使用本公司資訊資源（含硬體、軟體與數據）之對象。

三、政策要求：

為落實資訊安全管理目標，本公司全體人員應遵循下列要求：

1. 法規遵循與合約義務 落實各項資安相關法令之遵循，包含但不限於《個人資料保護法》、《著作權法》及智慧財產權相關法規。同時，應嚴格履行與外部單位（如客戶、供應商）所簽訂之保密協議（NDA）與服務契約義務。
2. 管理架構與職責培訓 由營運管理單位專責推動資安管理制度之規畫、執行與溝通協調。全體人員應定期參與資訊安全與個人資料保護之教育訓練與宣導，確保清楚理解並履行其業務執行所負之安全責任。
3. 資產管理與營運持續
   - 資產屬性：員工因公務持有之資訊資產應遵循「公有公用」原則，嚴禁挪作私用。
   - 分級控管：所有資訊資產應進行分類分級與風險評估，並依等級落實適當控管措施。
   - 持續運作：關鍵資訊化作業應依業務需求規劃「營運持續管理計畫（BCP）」，並定期演練，以確保系統之高可用性。
4. 實體與環境安全控管 針對實體辦公環境、機房及重要資訊設備存放區，應設置嚴謹之出入監控與門禁管制措施，非經授權不得進入，以防範未經授權之存取或物理破壞。
5. 惡意軟體防治與軟體授權 嚴禁於公司設備安裝或使用未經授權之非法軟體。僅限使用經公司核可之合法授權系統及應用軟體，以防範電腦病毒、勒索軟體或惡意程式之入侵。
6. 稽核與違規處置 應定期辦理資安稽核以確保制度之有效性。凡違反本政策或相關作業程序者，將依公司人事規章或相關法律程序進行審議與懲處；情節嚴重者，公司保留法律追訴權。

四、責任：

1. 管理決策責任 管理階層應積極參與資訊安全決策，提供必要之資源，並透過審查會議確保本政策之有效性。各部門主管應督導單位內部落實標準作業程序，確保資安文化融入業務流程。
2. 組織推動責任 本公司成立「資訊安全推動委員會」(或稱管理小組)，統籌管理制度之規劃、建立、實施、稽核及持續改善事項。
3. 全員遵循責任 本公司全體人員(含正式員工、約聘、派遣人員)、委外服務廠商、合作夥伴及訪客，均應瞭解並嚴格遵守本政策及相關配套規範。
4. 異常通報義務 全體人員與委外服務廠商均負有主動通報之義務。凡發現資訊安全異常事件、系統脆弱點或疑似受駭情事，應立即透過本公司指定之通報機制進行回報，不得隱匿。
5. 違規懲處與法律責任 任何違反本政策或危及資訊安全、個人資料保護之行為，除依本公司人事規定辦理審議懲處外，若涉及法律責任，本公司將依法追究其民事、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。

資訊安全風險管理與持續改善架構

資訊安全管理與執行重點

本公司採取「預防、偵測、應變」之主動防禦策略，並透過 PDCA（規劃-執行-檢查-行動）循環持續精進資安韌性。

(一) 核心防護策略

1. 端點與產線防護：部署先進病毒偵測與端點防護系統（EDR），嚴格控管辦公設備及生產線機台之存取安全性，杜絕惡意軟體感染風險。
2. 網路安全邊界：強化下一代防火牆（NGFW）與網路分段控制，阻斷橫向滲透，並建置自動化惡意行為截獲機制。
3. 資料與雲端安全：導入資料加密技術與中心化安全管理，強化資料中心（Data Center）之實體與虛擬防護層級。
4. 威脅預警與演練：利用資安維運平台（SecOps）提升事件偵測與自動化處置效率，並透過模擬攻擊演練（Red Teaming）精進應變能力。

(二) 年度執行與演練重點

公司每年定期執行下列資安強化工作，以確保防禦機制之有效性：

營運韌性:

1. 業務持續作業演練,確保關鍵業務於災難發生時能迅速復原。
2. 備份機制與備援計畫,落實「3-2-1」備份原則，並定期執行復原驗證。

技術防禦:

3. 安全性檢測與弱點修補,定期進行源碼掃描與滲透測試，並限期完成修補。
4. 威脅偵測管理機制,全天候監控異常流量，主動獵捕潛在威脅。
5. 資通安全防護控制,優化權限控管、防毒措施與軟體發行流程。

環境與稽核:

6. 實體安全控管,機房及辦公區門禁紀錄審查與監控系統檢核。
7. 資通安全稽核,透過內部及外部稽核，驗證管理制度之遵循情況。

意識培訓:

8. 電子郵件社交工程演練,測試員工警覺性，防範釣魚郵件攻擊。
9. 資通安全教育訓練,針對不同職位人員提供專業資安課程。

技術精進:

10. 新型技術研究,定期研討與評估新世代資安產品，維持技術領先。

投入資通安全管理之資源與執行成效

本公司致力於構建堅韌的資通安全環境，目前已建置完善的治理架構，設置資安專責主管及專責人員，負責統籌整體安全策略。

在技術防護層面，本年度積極落實資安健檢與弱點掃描，並針對偵測結果完成漏洞修補作業；此外，已全面導入 VPN 雙因子認證（MFA）並完成無線網路系統安全升級，強化存取管理。本公司亦積極參與外部聯防，加入 TWCERT/CC 資安情資分享平台，掌握即時威脅資訊。在管理與演練方面，落實定期系統備份與災難復原演練，確保營運韌性。114 年度內辦理 8 場資安宣導講習及社交工程演練，全體員工均完成資安認知教育訓練；資安人員皆達成 6 小時以上專業職能訓練。114 年度至 115 年 1 月 8 日前無發生重大資通安全事件，展現穩健的資安防護成效。