2.3.2 資訊安全管理

漢田生技視資訊安全為企業基本責任，為保障員工與合作夥伴之資訊資產不受侵害，本公司建置完善的資訊安全管理體系，確保資訊處理的正確性與可用性，並持續強化系統、設備和網絡之安全防護。

重大主題 資訊安全管理與客戶隱私	
重大主題意義	漢田生技為保障客戶資料安全、確保交易資訊不受未經授權存取或侵害，持續強化資訊安全風險管理，將潛在衝擊降至最低，提升整體網路韌性與資訊治理效能。
政策／承諾	遵守政府相關法規，並配合內部訂定之《資訊安全政策》加以強化資安防護措施。
目標	短期 ▶ 提升全員資安意識，透過持續社交工程測試演練強化防護警覺。 ▶ 完整盤點個資資產並持續評估風險，制定有效改善計畫。
	中長期 ▶ 持續強化資訊安全管理體系，確保各項作業符合 ISO 27001 標準要求。導入自動化監控與威脅偵測工具，持續優化資安制度與內控流程以提升資安防護效率。
行動辦法	▶ 合約全面導入系統管理，設有定期更新與檢討機制，由業務、法務及高階主管共同參與審核與簽署，確保合約內容合規並因應市場變化。本公司亦定期追蹤合約履行狀況，針對即將到期者主動啟動續約或修訂流程，維持合作穩定性與彈性。 ▶ 資訊部門及專責人員定期檢視與評估資安管理措施，針對涉及個人資料蒐集、處理與儲存之業務流程，執行個資保護影響評估，預先辨識資料外洩或誤用風險。 ▶ 導入多項資訊安全防護機制，並透過定期資安教育訓練與宣導活動，提升全體員工資安意識，有效降低資訊風險發生的可能性與影響程度。
2024 年實際績效	▶ 無發生經證實侵犯客戶隱私或遺失客戶資料之投訴。 ▶ 委託專業資訊安全顧問公司辦理弱點掃描，並依提供之技術報告進行修正與改善，後續亦已執行複次掃描以確認重大弱點均已排除，確保系統安全性與穩定性。
申訴機制 / 溝通管道	▶ 客戶可透過包括電話、電子郵件及官方網站提出意見或申訴，本公司將依據「客戶意見管理程序」進行調查與回應，確保客戶問題獲得妥善處理。 ▶ 如遇資訊安全事件依內部程序進行處理。

資安政策與組織

漢田生技設立資安室，隸屬於總經理室，由專責人員負責資訊安全規劃與執行，全面統籌資訊安全政策的規劃與落實。為保障資訊資產的機密性、完整性及可用性，本公司制定《資訊安全政策》及《資訊循環內控辦法》，涵蓋資訊設備防護、偵測與回復等措施，導入制度化流程與國際標準，強化資訊在取得、處理、儲存與傳輸各階段的安全控管，降低營運中斷及資安風險，確保本公司及客戶資料安全無虞。

資訊安全管理體系係依據 ISO/IEC 27001 標準架構與指標進行規劃與執行，並配合日常維運作業持續精進，包括每日資料備份與系統監控、每週異常流量及防火牆紀錄整理、每月系統版本更新與安全修補，亦視專案或事件召開資安會議，建構具韌性之資安管理體系。

資訊防護政策與落實

1. 資訊資產管理

- 建立設備、系統、資產清冊
- 控管資料存取權限

2. 存取與權限管理

- 規範帳號建立、變更與停用流程
- 實施多因素驗證與密碼政策

3. 員工安全與教育

- 定期進行資訊安全訓練（如防社交工程）

4. 作業安全管理

- 日常作業有紀錄與稽核
- 系統定期更新與修補
- 備份與日誌記錄受控管理

5. 通訊與網路安全

- 資料傳輸加密（如 VPN）
- 建置防火牆設備
- 定期弱點掃描測試

6. 資安事件應變

- 建立資安事件通報與回應流程

7. 業務持續與備援

- 定期執行災難復原計畫

8. 合規與稽核

- 建立內部稽核制度，確保符合法規

個資隱私

漢田生技重視個人資料保護，視其為保障員工、客戶及合作夥伴基本權益的重要企業責任。為確保個資於蒐集、處理與利用各階段皆符合法規並落實管理，本公司已制定《個人資料保護管理辦法》以防範資料濫用與促進個資之合理、合法使用，強化資訊安全與信任關係。

漢田生技以保障個資安全為責任核心，並依循以下原則建構管理架構：

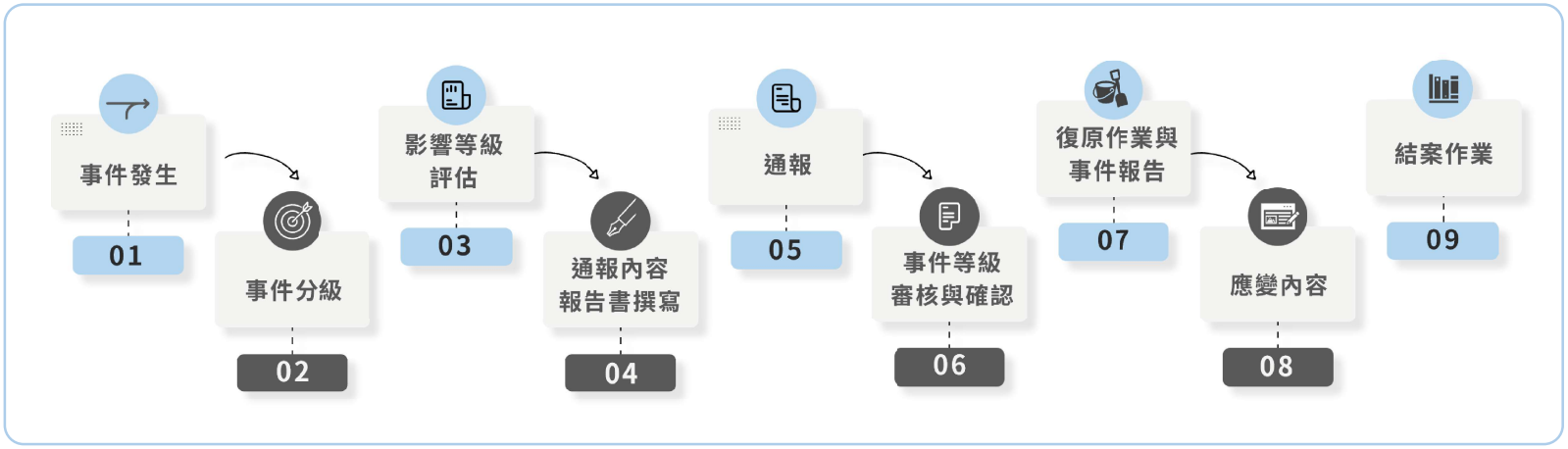
- 合法蒐集與清楚告知：於蒐集個人資料前，清楚揭露蒐集目的、使用範圍與保存期間，並依法取得當事人同意。
- 安全處理與風險控管：採取適當的技術與管理措施，防止個資遺失、竄改、洩漏或遭未經授權使用。
- 責任分工與制度推動：設立個資保護管理單位，並指定專責人員負責制度推行、員工教育訓練及政策落實。

資訊安全處理流程

漢田生技制定《資通安全事件通報及應變辦法》，建立系統化之資安事件應變流程，以降低資通安全事件對營運造成之損失與影響，確保公司營運之穩定性與持續性。為強化資安事件之應變效率與風險控管能力，本公司依據事件之影響程度區分為四個等級，自第一級（輕微）至第四級（災難性），涵蓋資訊洩漏、系統中斷、資料竄改等情境。針對不同等級之事件，明訂通報與審核時效，資訊單位於知悉事件一小時內須完成初步通報，並依事件等級於二至八小時內完成審核與確認。

此應變機制有助於即時掌握事件狀況、迅速展開因應措施，降低損害範圍，並確保關鍵業務持續運作，展現漢田生技在資安治理、營運韌性及企業永續推動上的積極作為。

漢田生技資訊安全事件處理流程圖



資訊安全管控措施

面對資訊環境快速變遷與資安威脅日益嚴峻，漢田生技深刻意識到資訊資產保護對於維持營運穩定及實現企業永續發展的重要性。為此，本公司積極導入資訊安全管理制度，並持續強化各項資安防護措施，從制度面、技術面及人員面多層次構築防禦機制。

透過建構系統化與前瞻性的風險管理架構，漢田生技致力於降低營運中斷風險，提升組織韌性與資安應變能力。資訊安全管理機制整合日常營運流程與資安治理重點，實現全方位的風險監控與持續改善，確保資訊系統穩定、安全運作，鞏固利害關係人對本公司的信賴，如下為本公司資訊安全管理機制：

分類	管控項目	執行措施
制度面	▶ 密碼政策管理	▶ 密碼須每 90 日更新，並包含大寫、小寫、數字及特殊符號，以提升帳號安全。
	▶ 權限分層與定期檢討	▶ 根據職務需求設定權限，每年定期進行至少兩次檢討，避免權限過度授予。
	▶ 資料分級與控管政策	▶ 依據資料敏感性進行分級管理，機密資料需加密並限制存取權限。
	▶ VPN 使用管理	▶ 員工遠端連線需事先申請 VPN 帳號，登入行為將記錄並保留稽核軌跡。
	▶ 郵件與通訊政策	▶ 郵件伺服器設有病毒防護與垃圾信過濾機制，風險事件將即時通報並處理。

資訊安全管控措施 (續)

分類	管控項目	執行措施
技術面	▶ 系統備份管理	▶ 每日備份關鍵系統與設定檔，並儲存於異地備援系統，確保災後可恢復。
	▶ 郵件防毒與更新	▶ 郵件伺服器自動更新防毒系統與病毒定義，降低郵件病毒入侵風險。
	▶ 防火牆與防毒系統更新	▶ 定期更新病毒庫與防火牆規則，強化邊界防護能力。
	▶ HiNet 防駭守門員企業版	▶ 透過 ISP 端阻擋殭屍網路、勒索軟體等惡意連線，同時檢測終端安全狀態，有效降低受駭風險。
人員面	▶ 資安意識與教育訓練	▶ 定期辦理資安教育訓練與社交工程演練，提升員工防範意識與實務應對能力。
	▶ VPN 使用遵循 (含帳號申請與紀錄)	▶ 員工須遵循申請與登入規範，避免違規使用並強化行為稽核能力。

為強化資訊安全防護能力，漢田生技持續投入資源於資訊安全體系之建置與優化，透過多項技術升級與制度化管理，全面提升資訊系統之穩定性與韌性。本公司已完成伺服器作業系統與資料庫系統升級，強化系統穩定性與平台相容性；導入叢集式高可用主機架構與擴充備份儲存容量，有效強化服務持續性與資料保存能力。此外，亦完成主機虛擬化平台升級與授權續約，確保系統可長期穩定運作。

在資安風險管理方面，漢田生技定期執行弱點掃描作業與災難還原演練，強化潛在風險之預防及應變處置能力。透過上述資安措施的落實與優化，本公司資訊系統之整體防護能力與營運韌性持續精進，有效支撐企業營運目標與永續發展策略。 2024 年度本公司資訊安全系統相關支出說明如右：

資訊安全系統	使用說明	金額
作業系統版本升級	升級伺服器作業系統以提升穩定性與安全性。	152,000
資料庫系統版本升級	升級伺服器資料庫系統軟體，確保相容性與效能。	170,000
高可用資訊設備升級	升級為叢集式高可用主機架構，提升服務持續性。	716,000
備援空間升級	擴充備份儲存空間，強化資料保存能力。	60,000
虛擬化機制	主機虛擬化平台版本升級並完成授權續約，確保系統穩定運作。	270,000
弱點掃描	定期執行弱點掃描，強化系統防護能力。	22,000
災難還原演練	定期進行災難還原演練，驗證備援機制的可行性與應變能力。	74,000

供應鏈安全防護

隨著業務規模擴大，漢田生技持續強化供應鏈資訊安全管理，降低潛在資安風險，提升整體營運韌性，針對關鍵 EC 主機平台，因應資安負載成長，本公司正評估遷移至防護等級較高之主機環境，以提升系統穩定性與資料安全性。

同時，已初步建立供應商資訊風險評估流程，針對與本公司系統介接之高風險供應商進行管理，並委託會計師事務所進行電子稽核，並持續檢討精進，引入更完整的第三方資安稽核或驗證服務。

展望未來，本公司將持續強化供應鏈資安風險辨識與監控作業，建構可持續及具韌性的資訊合作環境，確保供應鏈整體的安全與穩定。

資訊安全教育訓練與演練

為強化員工資訊安全意識，本公司由資安室定期辦理社交工程演練，檢視全體同仁對釣魚郵件、可疑連結等攻擊手法的辨識與應對能力。2024 年針對 15 個部門共 84 個帳號，寄送 336 封模擬演練信件，並分析開信、點擊、輸入資訊等行為數據，作為教育訓練與績效衡量依據，針對在演練中有觸發行為之人員，安排補強課程說明，協助其了解風險來源並提升應對能力。

資安宣導則透過早會機制實施，每半年至少舉行一次，並搭配案例說明與製作電子海報、桌布與螢幕保護程式，提升日常警覺。，針對演練結果進行追蹤，必要時安排個別說明與補充說明，協助同仁強化風險意識與正確應對行為，所有訓練紀錄亦納入稽核與管理評估，逐步建立正向資安文化。

為確保重大異常或突發事件下能迅速恢復營運。已建立完整的災難復原計畫（DRP），明確規範應變流程與責任分工。每年定期辦理災難復原演練，涵蓋主要營運系統，並由原廠系統廠商協助進行實地還原測試，確保資料備份機制（RPO）與恢復時間目標（RTO）達成標準。演練對象將依年度輪替不同關鍵系統（如 ERP、APS 等），逐步強化跨系統之復原能力，提升面對多元災難情境時的營運持續性與應變能力。

透過定期演練及宣導課程 2024 年未發生同仁通報資訊安全事件，顯示本公司實施資訊安全管理措施已見顯著成效。

單位：人次；小時

單位 / 部門	訓練主題	受訓人數	總受訓時數
各部門	社交工程演練教育訓練	16	1
各部門	社交工程演練教育訓練	20	1
全體員工	早會宣導 -113 年度 漢田社交演練報告	70	0.5