資訊安全不僅攸關企業內部營運效率，也可能直接影響客戶信任、供應鏈穩定性與企業聲譽。為降低潛在資安風險，公司依據實務情境與外部資安通報，定期評估資訊安全衝擊來源，並強化制度性控管與技術防護作法，以提升事件應變能力。

資安意識培訓與宣導

資訊安全不僅是技術防線，更需全體員工共同維護。為此，公司持續推動資訊安全意識內化與教育制度建置，透過定期訓練與模擬演練提升組織資安防禦力。2024 年度，公司辦理多場資訊安全宣導，涵蓋資訊資產保護、網路使用安全、社交工程辨識等內容。我們透過以下方式增強員工的資安能力：

- 資訊安全通識訓練：所有員工皆須接受資訊安全與個資保護訓練，並視情況調整課程內容。
- 開發人員資安培訓：安排開發人員參加安全程式碼開發課程，通過測驗後可參與核心系統開發。

執行成效

執行項目	對象	執行方式	執行情形
資安應變通報說明	業務與行政單位	簡報及實務操作流程分享	2024 年度導入內部異常通報機制
密碼與權限管理提醒	系統使用者	內部信件與操作系統提示	每季提醒並進行抽查
外部攻擊案例解析	管理階層與資訊人員	簡報與案例分享會議	2024 年進行多次資安宣導

2024 年度**無發生重大資通安全事件。無任何因資安事件造成之營運損失或客戶資料外洩事件**，確保企業營運穩健，並維持良好的客戶信任度。

個人資料與隱私保護機制

川寶科技依據《個人資料保護法》相關規定，建立基本個資保護原則，確保所有蒐集、處理與利用個人資料的行為皆符合法規與倫理標準。於員工、客戶及供應商接觸個人資料之情境中，皆明確揭示蒐集目的與範圍，並取得當事人之知情同意。

數據隱私治理專責單位

我們已逐步建立涵蓋個人資料與機敏性營運資訊的隱私保護管理架構，隱私管理由資訊安全小組負責整體制度推動與監督，並定期向高階管理團隊彙報執行情形。

- 執行層面則由資訊部門與人事單位共同負責
- 資訊部門聚焦系統層級存取控管、資料備份與資安防護規劃
- 人事部門則負責處理包含員工基本資料、考勤與薪資紀錄等敏感性個資的保存、授權、調閱與封存銷毀作業，並建立調閱授權流程與查核留存紀錄。

將持續強化隱私治理的制度化與紀錄管理機制，並適時依業務型態或法規變動滾動式修正制度內容，以維持個資處理流程的安全性與法遵完整性。

數據隱私政策與權限管理

依循國內外標準，針對機密與個人資料管理，公司已實施下列制度化控管措施：

- 最小權限控管：對於所有含有個人資料或機密營運資訊之系統、檔案與設備，均設定操作授權層級，僅限必要人員操作，並依職務異動或年度盤點結果進行權限審查與調整。
- 紙本與電子資料分級保管：人事部門保管之書面資料均鎖櫃管理，僅限核准人員操作；其他單位如稽核、部門主管需查閱時，應依授權程序查閱所屬或特定查核人員資料。電子個資則集中儲存於專責設備，採密碼登入控制與使用者操作留痕。
- 存取紀錄與稽核機制：針對所有涉及個資存取與下載操作行為，系統自動留存使用紀錄，並由資訊單位或人事主管定期查核存取紀錄，確保資料處理行為符合內部政策與法規要求。

數據存儲與加密防護

- 加密防護
- 在數據收集、傳輸及存儲過程中逐步進行資訊保密防護，確保即使資料於傳輸途中遭截取，外部人員也無法讀取或解密
- 資料存儲隔離與多層保護
- 機密資料存放於獨立伺服器區域，並搭配多層防火牆及訪問控制，與一般業務數據完全隔離，有效防範內部系統漏洞或外部攻擊。
- 數據保留與刪除機制
- 依照法規與業務需求，明訂數據保存期限，確保到期後資料可安全刪除或匿名化處理，針對過期或不再需要的數據，按照既定流程進行安全銷毀，確保數據在生命周期結束後不留存風險。

第三方資料處理與數據防護管理

我們於日常營運中涉及特定資訊與外部供應商或合作單位之資料交換，為降低外部洩漏或過度授權風險，已逐步建構涵蓋授權、存取、加密與刪除等面向的資料處理管理機制，並採取分層防護原則。

- 資料存取授權與調閱控制

  目前公司對於所有涉及個人資料、商業機密或其他機敏資訊之存取與跨部門使用，均採「最小授權原則」，並設有明確簽核流程：

  - 外部供應商若需存取內部資訊，僅限特定目的、時效與資料類別，並於使用前完成加密處理與授權記錄。
  - 所有部門若有跨單位調閱書面或電子個資需求，須經單位主管簽署核准後方可存取，並留存完整紀錄以利追蹤。
- 數據加密與存儲隔離策略

  為強化資料傳輸與儲存過程的保密性與完整性，公司已逐步導入資料加密與分層存取控管措施：

  - 重要資料於蒐集、傳輸與儲存過程中均進行加密處理，防止資訊於傳輸過程中遭截取後被解讀或重構。

- 機敏資料集中存放於獨立伺服器環境，設有多層防火牆、身份驗證與訪問控制，與一般業務數據完全隔離，降低內部錯誤與外部滲透風險。

◆ 數據保留與刪除機制

針對各類資料，公司依據法規規定與業務實務需求設定保存期限，定期進行資料盤點與清理作業：

- 過期或不再使用之數據將依照流程進行銷毀或匿名化處理，避免遺留未管理之歷史資料成為潛在風險來源。
- 數據刪除作業由資訊部門負責執行，並保留作業紀錄，以利稽核與合規檢查。

員工數據隱私教育與內部管理機制

為降低內部資料處理風險，公司每年安排隱私教育與合規訓練，針對個人資料的收集、使用、存儲與刪除流程進行制度化宣導，協助同仁掌握正確的資料處理觀念與日常實務注意事項。

◆ 由人資單位與資訊部門安排定期教育訓練，強調資料處理合規、使用紀錄與保管義務。

◆ 針對實際系統操作人員，公司亦提供操作指引與資安規範手冊，並導入內部查核與回饋機制。

資料銷毀與存儲管理機制

為降低冗餘資料留存所帶來的潛在資訊風險，依據內部管理制度及個人資料保護法規，逐步完善包含數據保留、封存與銷毀在內的完整資料處理流程。針對不同資料型態，開始評估制定保存週期並執行定期檢核，避免過期資料產生潛在資安風險。

◆ 數據保留與封存原則

- 員工個人資料保存期間原則為五年，期滿後由人事單位統一清查與封存，並不予保留備份。
- 各部門書面個人資料於保存年限屆滿後由單位彙整封箱，統一交由具資安認證之第三方機構進行物理銷毀。

◆ 資料銷毀與除役流程

- 定期盤點過期資料，分類為機敏資料（如客戶基本資料、離職員工紀錄）、業務資料與合約等，並依據敏感性制定不同銷毀方式（如：物理粉碎、電子覆寫刪除）。
- 所有書面或電子檔案銷毀作業皆須填列紀錄表，經單位主管核備後交由專人執行，過程可追溯且留有稽核依據。
- 書面資料銷毀前建議經碎紙處理，防止外洩風險；電子資料則採物理刪除與磁碟覆寫，並禁用外接媒體留存。

事件應變與通報機制

為強化對潛在資訊安全與隱私事件的即時應變能力，我們已經逐步的透過基本事件通報與處理流程，要求所有同仁在發現異常存取、資料洩漏、系統入侵或其他可疑資安事件時，應依據內部規定流程即時通報，確保風險能於第一時間被掌握與處理。

階段	執行單位/責任	說明
異常發現與初步通報	全體員工，資訊部或資安室為通報窗口	員工回報異常狀況，如疑似資料外洩、系統異常、釣魚郵件等

事件受理與初判	資訊安全小組負責研判是否構成資安/隱私事件	進行初步事件分類、通報記錄、確認處理等級與進程
事件處理與應變	事件處理小組	依嚴重程度實施封鎖、備份還原、通報主管或停機應變等措施
事後分析與改善	事件小組負責 RCA 分析與改進建議，資訊部門追蹤執行	執行根本原因分析（RCA），提出防再發方案，規劃制度/技術強化
紀錄存檔與定期報告	資訊部門留存紀錄並彙報管理階層，必要時提報董事會	將事件及處理結果存檔，納入年度報告與內稽追蹤

隱私管理績效

截至 2024 年底，川寶科技未發生任何個人資料外洩、未經授權存取或隱私違規事件，亦未接獲主管機關查處或民眾申訴案件。

1-4.5 災害風險管控

面對極端氣候事件頻率上升與各類天然災害風險持續擴大，我們也逐步強化災害辨識與應變制度，以降低對員工安全、營運穩定與設施資產的潛在衝擊。

災害風險管理架構

目前，公司雖尚未全面建立災害風險分級分析與制度化災難應變框架，但已透過廠區經驗累積與參考產業規範，逐步推動避難演練、防災設備建置與異地備援機制，建立初步災害防護流程。由公司各部門主管負責災害風險政策統籌，並依不同廠區條件協調資源投入與應變人力配置。

下列重點災害情境：

災害風險類型	潛在衝擊	初步因應機制與應變措施
地震	員工傷害、廠房結構損毀、生產中斷	建立避難動線、定期消防與地震演練、建物耐震檢測與強化
水災 / 淹水	設備損壞、電力中斷、系統停擺	設置排水設備與抽水機、重要設備加裝防護、預留臨時電力與設備
火災	財產損失、供應鏈中斷、營運中斷	建置灑水設備與煙霧感測器、推動逃生訓練與通報演練
疫病傳播	勞動力短缺、供應中斷、員工健康風險	實施健康監測、遠距辦公制度、防疫物資管理與分流出勤

災害復原與業務持續流程

為提升企業面對災害風險時的應變彈性與營運延續能力，我們持續強化防災應變管理，並針對關鍵設施、作業流程與人力支援進行分階段風險分析與復原機制規劃。目前公司正逐步建立營運持續性管理架構，涵蓋災後人員安全確認、重要設備檢修、資料與系統恢復、內外部通訊協調等關鍵流程。

現階段已落實防災措施

- 備援機制：除資訊資料每日異地備份外，亦完成廠內重要設備備品盤點與異地存放；逐步建置電力與空壓備援設施。
- 通訊與應變分工：已設立跨部門災害聯絡人名冊與應變群組，針對災後停工、人員調度與產線評估等情境，訂定通報 SOP 與責任分工。