寶雅國際股份有限公司
資訊安全政策

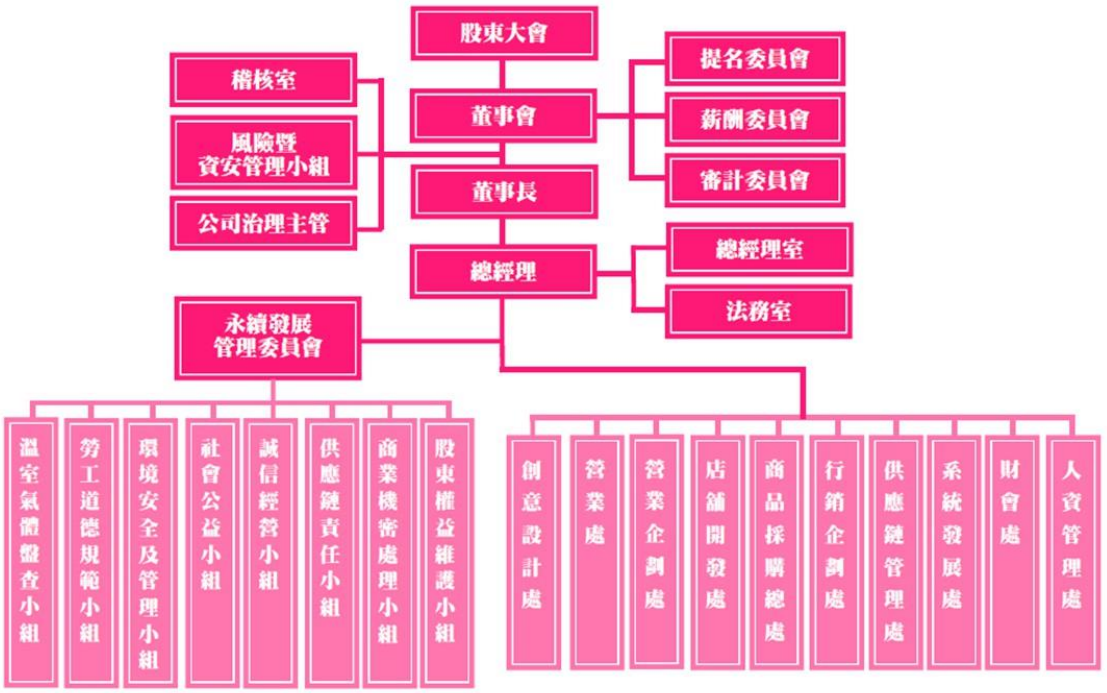
第一條 資訊安全目的與範圍

目的：為建置本公司安全及可信賴的資訊運作環境，維持業務持續運作，降低資訊作業風險，保障資訊服務使用者之權益，建立資訊安全管理系統，規範本程序為最高指導方針，以達成資訊安全管理的目標。

對象：包括員工，客戶，供應商和股東等利害關係人，及營運相關資訊軟硬體設備。

範圍：本公司之資訊安全相關業務作業，包含核心業務、資訊安全作業程序、資訊系統盤點及風險評估、資訊系統發展及維護安全、資訊安全防護、資訊作業委外辦理、資訊安全事件通報應變及情資評估因應、資訊安全之持續精進及績效管理、法規要求等。

第二條 組織架構與職責



一、董事會
董事會為資訊安全管理之最高決策單位，核定資訊安全政策與架構，監督資訊安全管理機制之有效運作。

二、稽核室：依據資訊安全政策及風險評估結果擬訂年度稽核計畫，依計畫執行各項制度稽核作業，協助董事會監督及控管執行決策可能潛在之風險，確保各作業風險均獲得有效管控，並適時提出改善建議。

三、風險暨資安管理小組：本公司於110年7月新增「風險暨資安管理小組」，由總經理擔任召集人。本小組為跨部門小組，負責審視各業務單位之資訊安全政策之治理、規劃、督導及執行情形，以建構出資訊安全防衛能力及同仁良好的資訊安全意識，並每年定期向董事會報告執行情形。

四、系統發展處：負責推展並落實執行資訊安全管理制度。

五、財會處：負責資安事件企業衝擊評估、重訊發佈。

六、人資管理處：負責人才招募、教育訓練。

七、法務室：負責個人資料保護維護、推廣、鑑別適用性法規。

第三條 資訊安全政策目標

一、確保本公司營運業務持續運作，且本公司提供的資訊服務可穩定使用。

二、確保本公司所保管的資訊資產之機密性、完整性與可用性，並保障利害關係人之隱私。

三、建立資訊業務永續運作計畫，執行符合相關法令或法規要求之資訊業務活動運作。

四、藉由Plan-Do-Check-Act(PDCA)管理循環，持續改善資訊安全管理機制。

第四條 資訊安全政策與具體管理措施

一、資訊安全政策

1.資安治理：制定完整管理制度，強化教育訓練、資訊安全基礎架構設計及保護技術。確保資訊之系統可用性、限制權管及存取管理、抵抗外部威脅。

2.法令遵循：建立符合規範機制，定期檢視及修訂相關作業規範以符合資安標準。

二、風險評估

1. 定期盤點資訊系統，並建立核心系統資訊資產清冊。

2. 鑑別並定期檢視本公司核心業務及應保護之機敏性資料、應遵守之法令。

3. 定期辦理資安風險評估，檢視資訊安全控制措施。

4. 鑑別可能造成營運中斷事件之發生機率及影響程度，設置備份機制及備援計畫並制定核心業務持續運作計畫，定期辦理核心業務持續運作演練。

三、資訊安全控制措施

1. 資訊系統開發及維護應評估資安風險。

2. 妥善儲存及管理資訊系統開發及維護相關文件。

3. 對核心資訊系統每年定期辦理安全性檢測（如：弱點掃描、滲透測試、源碼掃描等），並進行系統弱點修補。

4. 依網路服務需要區隔獨立的邏輯網域，並將開發、測試及正式作業環境

區隔，且針對不同作業環境、機敏性資料建立資安防護控制措施。

5. 訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項及資訊設備使用管理規範。
6. 建立使用者通行碼管理之作業規定。
7. 定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。
8. 建立資訊系統及相關設備監控措施，並針對日誌建立保護機制。
9. 針對電腦機房及重要區域之安全控制、人員進出管控、環境等建立管理措施。
10. 關注安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。
11. 訂定資訊設備回收再使用及汰除之安全控制作業程序。
12. 每年定期辦理電子郵件社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。

四、委外管理

1. 訂定資訊作業委外安全管理程序，包含委外選商、監督管理及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資訊安全管理措施。
2. 訂定系統委外廠商之資訊安全責任及保密規定，依據專案需求於採購文件中載明服務水準協議(SLA)、資安要求及對委外廠商資安稽核權。
3. 委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。

五、資訊安全事件管控及預防措施

1. 訂定資安事件應變處置及通報作業程序(附件一)，包含資安事件識別、判定事件影響、內外部通報流程、事件排除及矯正預防措施。
2. 加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊。

六、資訊安全持續精進管理機制

1. 風險暨資安管理小組定期向董事會報告資訊安全執行情形，確保運作之適切性及有效性。
2. 定期辦理內部及委外廠商之資安稽核，並就發現事項擬訂改善措施，且定期追蹤改善情形。

七、具體管理措施

資訊安全管理類型	相關作業
系統可用性	1.監控系統、網路可用狀態 2.資料異地備份，確保完整資訊可復原 3.定期演練災害發生，系統還原程序
外部威脅	1.偵測病毒與惡性程式攻擊，防範資訊受損 2.電腦主機弱點檢測及更新 3.防毒軟體 4.郵件過濾機制 5.入侵偵測及防禦機制 6.應用程式防火牆 7.進階持續性滲透攻擊防禦機制 8.資訊安全威脅偵測管理機制

權限管理	1.人員帳號及權限之設定管理 2.定期檢查盤點帳號及必要業務之使用權限 3.重要機房出入權限管理
存取控管	1.管制資訊檔案存取 2.資料存取紀錄 3.檔案加密機制 4.定期進行內、外部稽核，並租用 ISO 27001 資訊安全驗證合格之電信骨幹網路機房，確保伺服器與網路服務之可用度 5.網路防火牆

第五條 資安宣導與教育訓練

一、提醒宣導：要求員工定期更換系統密碼，以維帳號安全。

二、講座宣導：不定期對內部員工實施資訊安全相關的教育訓練課程。

第六條 資安管理報導與資訊揭露

為充分紀錄資訊安全管控程序及其執行結果，風險暨資安管理小組應至少一年一次向董事會報告資安管控狀況以供管理參考。

本公司除應主管機關規定揭露相關資訊外，亦宜於年報、永續報告書或公司官網揭露資安管理有關資訊。

第七條 核准與修訂

本政策未盡事宜，悉依有關法令及本公司相關規定辦理。本政策經董事會決議通過後施行，修正時亦同。本政策於中華民國一一0年七月二十六日公布施行，第一次修訂於112年10月30日。

附件一、資安事件應變處置及通報作業程序