博瑞達應用材料股份有限公司
資訊安全管理辦法

規章編號：PAM-10110

發佈日期：20250711

第一章 總則

一、目的

為建立資訊安全管理制度，保護博瑞達集團資訊資產的機密性、完整性及可用性，降低資訊風險，確保業務持續營運，特訂定本辦法。

二、適用範圍

本辦法適用於博瑞達集團(以下簡稱本公司)全體員工、契約人員、外包廠商及使用公司資訊資產之人員。

三、資訊安全政策

本公司致力於建立完善之資訊安全管理制度，確保資訊資產的機密性、完整性與可用性。資訊安全管理應納入公司治理與日常營運流程中，並符合相關法令與利害關係人之期望。全體同仁應共同維護資訊安全，防範內外部威脅與弱點，以降低資安風險。

四、資訊安全目標

1. 每年至少進行一次資安自我檢查，改善率達 100%。
2. 所有作業系統與應用程式，重大弱點修補完成率達 95% 以上。
3. 遇資安事件，通報與處置時間不得超過 4 小時。
4. 每年全體人員資安訓練覆蓋率達 100%。

五、資訊安全原則

資訊安全管理應遵循以下原則：

1. 最小權限原則。

2. 持續改善原則。
3. 資訊資產風險導向管理原則。
4. 員工資安意識與責任並重。

六、法令與契約遵循要求

本公司推動資訊安全管理制度，應遵循下列國內外法令、政策與契約義務，以確保資訊資產的機密性、完整性與可用性，並符合對利害關係人之承諾與責任：

1. 公開發行公司建立內部控制制度處理準則
2. 上市上櫃公司資通安全管控指引
3. 個人資料保護法
4. 本公司與客戶、合作夥伴、委外廠商間所簽署之契約中涉及資訊安全、保密、個人資料處理、服務水準協議（SLA）等條款

第二章 組織與責任

一、資訊安全管理架構

本公司資訊安全管理由下列人員共同負責執行與監督：

1. 總經理
2. 資安管理委員會：由總經理指派一位副總級主管擔任主委，召集兩位一級主管組成。
3. 資安執行小組：由資訊單位及各部門主管推派之代表組成，資訊單位主管擔任資安專責主管。

二、各角色職責

1. 總經理：

   (1) 核定資訊安全政策與目標。
   (2) 支持資安資源配置與制度推動。

2. 資安管理委員會：

   (1) 核定資產識別與風險評估結果。
   (2) 監督資訊安全管理事項執行情形。
   (3) 監督重大資安事件處理。

3. 資安專責主管：

   (1) 集團資訊安全政策之擬訂。

（2）定期檢討資安執行情形與改善建議。
（3）主導資安事件通報與應變。

4. 資安執行小組

（1）撰寫與維護資安管理文件。
（2）執行風險評估與控制措施。
（3）監控系統安全狀況與異常事件。
（4）規劃並執行資安教育訓練。

三、外部支援

遇資訊安全專業不足或需要進行資安稽核、弱點掃描、事故鑑識等事項時，得委託外部專業機構協助辦理。

第三章 資產識別與風險管理

一、核心業務識別

本公司之核心業務定義如下：

核心業務	**業務內容簡述**	業務失效影響說明	最大可容忍中斷時間
報價與接單	接收客戶訂單、製作報價單並與客戶往返確認報價與數量	無法即時報價或接單將導致客戶流失、商機喪失，損害公司營收與商業信譽	24H
客戶關係管理	管理客戶聯絡資訊、交易紀錄與商務需求	客戶資料遺失將影響後續交易、客服作業與客戶信任，造成客源流失	24H
出貨與物流追蹤	出貨安排、物流公司聯繫、貨物追蹤、報關與運輸文件處理	出貨延誤或資料錯誤將影響合約履行、引發客訴與索賠，影響公司信用與客戶關係	24H
付款與收款處理	處理 TT 匯款、L/C 開狀、信用證處理與財務文件傳遞	延誤或錯誤將導致收款失敗或客戶違約，甚至產生金錢損失與法律風險	24H

二、資訊資產分類與清冊

為有效管理資訊資產，本公司依資產性質分類如下，並建立資訊資產清冊（由 MIS 維護）：

資產類型	說明	管理單位
硬體設備	伺服器、筆電、網路設備等	MIS
軟體系統	ERP、BPM、CRM、郵件系統、資安工具等	MIS
資料資產	客戶資料、財務報表、設定檔等	各部門
雲端服務	Azure、SaaS 平台等	MIS
文件與紀錄	合約、政策文件、稽核紀錄等	各部門

資訊資產清冊應每年定期盤點與更新，並標註資產之擁有者、使用者、機敏性等級。

三、機敏性資料識別

本公司將下列資訊列為機敏性資料，需加強保護：

- 客戶個人資料（如姓名、聯絡方式、帳號資訊）
- 公司財務與營運資料
- 系統管理帳號與密碼
- 威脅偵測與分析報告
- 尚未公開之產品規劃與技術文件

四、風險評估原則

資訊安全負責人應每年至少辦理一次資訊安全風險評估，針對公司關鍵資訊資產、系統、網路與外包作業進行評估，評估項目應涵蓋潛在威脅、脆弱點、現行控制措施與風險影響程度。

五、風險評估流程

風險評估應依下列步驟進行：

1. 資產盤點：確認評估範圍內之資訊資產。
2. 威脅與弱點識別：分析可能影響資產之威脅來源與系統弱點。
3. 風險分析：依據資產價值、威脅可能性與衝擊程度，評估風險等級（高、中、低）。
4. 風險處置建議：針對高風險項目，採取以下一種或多種處理方式：
   (1) 風險降低（如加強控管、修補弱點）
   (2) 風險接受（經管理階層同意）
   (3) 風險移轉（如保險、委外）
   (4) 風險迴避（如取消高風險作業）
5. 文件化與存查：完整記錄評估結果與處置建議，存檔至少三年。

六、風險再評估時機

遇下列情形之一時，應進行臨時性風險再評估：

1. 系統或設備環境重大變更。
2. 發生重大資安事件後。
3. 新系統或新服務上線前。
4. 法規或營運環境重大變更時。

第四章 系統開發與維運安全

一、系統開發安全

為確保本公司自行開發或委外開發之系統具備基本資安防護能力，應遵循以下原則：

1. 安全設計原則：系統設計階段即應納入資安需求，如存取控制、資料加密、日誌記錄、錯誤處理等。
2. 權限最小化：系統帳號與功能模組應依使用者職責設定最小必要權限。
3. 程式碼管理：開發人員應使用版本控制工具（如 Git），並避免將機敏資訊寫入程式碼中。
4. 測試與驗證：系統上線前應進行功能測試與資安測試（如 OWASP TOP 10 等基本安全性檢查）。

二、系統維運安全

本公司資訊系統之日常維運應符合以下安全管理措施：

1. 帳號與密碼管理：
   (1) 僅授權人員得申請系統帳號。
   (2) 密碼原則須符合「IT 使用者規章」《伍、系統安全》第一條之規定。
   (3) 離職或職務異動人員之帳號應即時停用或調整權限。
   (4) 使用雲端服務(如 Azure、SaaS 平台…等)時，應啟用多因素驗證與存取控制。
2. 日誌記錄與監控：
   (1) 關鍵系統應保留存取與異常行為日誌，保存期限至少 6 個月。
   (2) MIS 每半年應定期檢視日誌，發現異常應立即通報。
3. 變更管理：
   (1) 系統設定或程式異動應經主管核准，並保留異動紀錄。

(2) 重大變更應安排非上班時段進行，並備妥還原機制。

4. 備份與還原：
   (1) 關鍵資料每日備份，並定期測試還原功能。
   (2) 備份資料應限制存取，並與主系統分離保存。

第五章 資通安全與防護措施

一、系統更新與弱點修補

1. 所有作業系統與應用程式應定期更新安全修補。
2. 留意資安情資與威脅訊息(如：訂閱 TWCERT/CC 電子報)，於高風險弱點公告後 30 日內完成修補。
3. 修補紀錄須予以保存至少一年。

二、網路安全防護

1. 防火牆應設置於網路邊界，限制未授權存取。
2. 提供外部存取服務的主機應設置於 DMZ 區域。
3. 外部網路、DMZ 與內部網路之間的網路通訊，皆須經過防火牆。
4. 集團各分公司或辦公據點與總公司之間的網路通訊，需透過 Site to site VPN 進行連線。

三、遠端存取管理

1. 遠端存取適用對象

本公司遠端存取服務係提供予因工作需要需於非公司網域環境連線之人員使用，包含：

(1) 本公司正式任用之員工。
(2) 經資訊主管核准之委外廠商人員，且具專案或維運需要者。

2. 遠端存取授權與管理

(1) 申請遠端存取服務者，須經部門主管及資訊安全負責人核准。
(2) 員工使用 Azure Entra ID 進行登入。
(3) 委外人員應申請個人帳號登入，並記錄存取行為，嚴禁共用帳號。
(4) 遠端存取應採取多因素驗證機制。
(5) 須依最小權限原則設定，限縮可遠端存取之系統與資源範圍。
(6) 對委外人員之連線授權應設定明確期限與目的，專案結束或人員離任應即終止帳號。

四、特權帳號管理

1. 特權帳號定義

特權帳號係指擁有系統管理、資料庫管理、網路設備設定或其他可變更系統核心設定與使用者權限之帳號，包含但不限於：

(1) 作業系統（如 Windows/Linux）之 Administrator 或 root 帳號。
(2) 資料庫管理帳號（如 sa、oracle）。
(3) 網路設備（如交換器、防火牆）之管理帳號。
(4) 雲端平台（如 AWS、Microsoft 365）管理帳號。
(5) 第三方委外廠商所申請之維護專用帳號。

2. 帳號使用原則

(1) 特權帳號僅限經授權之人員使用，使用時須基於維運、設定或必要性操作。
(2) 禁止使用特權帳號從事日常性作業，如一般文書、瀏覽網頁或收發郵件。
(3) 特權帳號不得由多位管理者共同使用，應以個別名義登入。

3. 帳號異動與停用

(1) 特權帳號如不再使用，應立即停用或刪除，並留存紀錄。
(2) 員工異動或離職時，其所使用具之特權帳號須即時停權。

第六章 資通安全事件通報與應變

一、資安事件定義

1. 資安事件係指任何可能危害本公司資訊資產之機密性、完整性或可用性之異常情況，包括但不限於：

(1) 惡意程式感染（如病毒、勒索軟體）
(2) 未經授權之存取或異常登入行為
(3) 資料外洩
(4) 系統異常或服務中斷
(5) 雲端服務或委外廠商之服務異常而影響本公司營運作業
(6) 他人通報之資訊安全問題

2. 資安事件分級

依照資安事件影響的嚴重性劃分為四個等級：

分級	定義
一級	影響部分資訊設備，組織仍可持續營運
二級	非核心業務受影響，組織仍可持續營運
三級	部分核心業務受影響
四級	組織核心業務停擺

二、通報原則

1. 員工如發現可疑或已知資安事件，應立即通報資安執行小組。
2. 資安事件一經發現，須於 4 小時內完成通報，並記錄事件概要。
3. 通報方式可透過公司既有通訊機制（如 Email、電話、即時訊息等）。
4. 若資安事件符合法令應通報條件，應依規定向主管機關完成通報。

三、應變處理流程

資安事件應依下列步驟進行應變處理：

1. 初步確認與分類：

   (1) 資訊人員確認事件真偽、影響範圍與初步性質（如是否涉及資料洩漏、服務中斷）
   (2) 依資安事件分級定義進行事件等級分類，並依等級由資安專責主管決定是否啟動重大應變程序
   (3) 若判定為資安事件，須立即通知母公司資安管理單位。
   (4) 若判定為三級以上重大事件，應立即通知高階管理層。

2. 即時處置：

   (1) 隔離受影響系統（如關閉網路、帳號凍結、停止服務）。
   (2) 防止擴散與進一步損害（如封鎖來源 IP、停用漏洞服務）。

3. 調查分析：

   (1) 釐清事件來源、觸發原因與受影響範圍。
   (2) 匯整相關日誌、系統記錄、存證資訊
   (3) 必要時可請求外部資安廠商或顧問協助處理。

4. 復原與恢復：

   (1) 受影響系統應重新安裝作業系統。
   (2) 修補漏洞或錯誤設定。
   (3) 如需使用備份資料進行資料還原，應確認備份檔案並未受事件影響。
   (4) 進行安全性檢測，確認系統已無風險。

(5) 恢復系統服務與正常營運。
(6) 加強防護機制（如變更密碼、修補軟體）。

5. 後續報告與改善

(1) 填寫完整《資安事件應變紀錄表》與調查報告。
(2) 提報管理階層，研擬改進措施。
(3) 定期追蹤改善進度並存查。

四、紀錄與追蹤

1. 所有資安事件應留存完整紀錄，包括發現時間、通報者、處理流程、調查報告與預防改善作為。
2. 紀錄保存不得少於三年。
3. 資訊負責人每半年應彙整資安事件報表，供內部稽核與管理決策參考。

第七章 資安教育訓練與宣導

一、年度訓練

1. 公司每年至少辦理一次資訊安全教育訓練，提升全體人員資安意識。
2. 資訊單位成員每年應接受資訊安全專業課程訓練。

二、新進人員訓練

新進人員須於到職時簽署「IT 使用者規章」，於 3 個月內接受資訊安全基本訓練。

三、日常宣導

資安執行小組應定期推送電子郵件宣導資安觀念（如釣魚郵件識別、防社交工程等）。

第八章 委外管理

一、委外原則

1. 僅委託具備專業能力與良好信譽之廠商。
2. 與外部廠商簽訂資訊系統開發、維護或代管服務時，應在合約中明定資安義務，包括資料保密、存取限制、資安事件通報機制等。
3. 應視委外服務類型，於契約中納入適當之服務水準協議（SLA），如：系統可用性、回應時間等。

4. 涉及機敏資料之委外作業，應簽署保密協議（NDA）。

二、委外管理

1. 應定期進行委外廠商資訊安全稽核，檢視委外作業之資安風險與執行情形。
2. 發現廠商違反資安規範時，應立即通報並採取補救措施。
3. 委外契約終止或解除時，廠商應依合約規定返還、移交、刪除或銷毀所有與本公司相關之資料與帳號。

第九章 稽核與持續改善

一、自我檢查與稽核

每年至少辦理一次資訊安全自我檢查，並彙整改善建議；必要時得委託第三方進行資安稽核。

二、缺失追蹤

稽核發現之缺失，資訊安全負責人應列管追蹤，直至完成改善為止。

三、績效管理

1. 資安執行小組每年應彙整資訊安全績效指標執行情形，形成分析報告。
2. 針對未達標者應檢討原因，必要時納入年度改善計畫。
3. 每年應進行績效指標的檢討與修正，以反映風險趨勢或法規要求的變化。

四、管理階層參與

管理階層應定期（至少每年）審閱資訊安全執行情形(含績效指標)與風險狀況，並提供資源與決策支持。

五、政策修訂

本辦法應每年至少檢討一次，必要時得依實際需求修正。

第十章 附則

本辦法經總經理核定後施行，並公告全體人員遵循。

相關文件

1. 資訊資產清冊

2. 資產風險評估彙總表
3. 資安風險改善計畫表
4. IT 使用者規章
5. 資安事件應變紀錄表