AMAX HOLDING CO., LTD

資通安全政策執行情形

本公司配合主管機關金管會對於資訊安全管理機制要求，將上市（櫃）公司分為三級。本公司已按所屬第二級標準規定已完成設置資訊安全專責單位、主管及資訊安全人員，專門負責資訊安全事務，進行資訊安全制度之規劃、監控及執行資訊安全管理作業，持續優化與改善可能發生之資安風險。

資通安全政策及具體管理方案

AMAX 管理層致力於保護組織內所有實體和電子資訊資產的機密性、完整性和可用性，以維護競爭優勢、法律遵循以及商業道德。AMAX 由資安長監督資訊和網路安全流程的實施和管理。並建立與維護資訊安全管理系統，為公司識別、評估、評定和控制資訊相關風險提供了基礎。另有風險主管負責管理和維護風險處理計劃，並在必要時進行額外風險評估，以確定針對特定風險的適當控制措施。

AMAX 的資訊安全政策包括保護員工及消費者個人資訊、整體資訊安全、數據治理和分類、存貨及設備資產管理以及訪問控制和身份管理。業務連續性和應急計劃、災難恢復計劃及資源、系統操作和可用性、系統及網路安全、系統監控等也是其中的重要部分。此外，為確保供應商和第三方服務的管理、實體安全性、環境控制，並妥善處理資訊安全事件，AMAX 針對不同層面的風險訂定相應管理流程，致力於實現具體明確的資訊安全目標。所有員工被要求遵守該政策和管理系統，並接受強制性訓練，以確保其了解和遵從政策要求。若有違反行為，將依公司內部紀律和與第三方協議進行相應處置。

■ 資訊安全管理計畫

資安管理項目	說明
終端電腦管理	● 安全的 VPN 連線 ● 端點防護，如防毒軟體、惡意軟體掃描和執行安全性漏洞更新 ● 用戶存取權管理，如多重要素驗證、基於角色的存取控制和定期檢閱存取權
系統存取控制	● 同仁使用系統，須經管理員依所申請的功能權限做授權

資安管理項目	說明
	● 密碼設置規定適當強度、字數 ● 同仁離（休）職進行各系統帳號刪除作業 ● 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
資訊機房管理	● 資料備份和修復，如定期備份、異地備份和災難復原測試 ● 設備均設置於專用機房，並實施人員進行控管及保留進出紀錄存查 ● 機房內部備有獨立空調，維持電腦設備於適當的溫度 ● 機房主機配置不斷電與穩壓設備
防毒和防駭管理	● 配置網路防火牆、駭客入侵偵測與預防系統 ● 安裝端點防護/反惡意軟體 ● 定期辦理弱點掃描及滲透測試，於系統上線前執行源碼掃描安全檢測 ● 配置託管式資通安全威脅偵測管理機制
網路安全管理	● 配置企業級防火牆，阻擋駭客非法入侵，2024 年未發生被攻擊事件 ● 遠端登入公司內網存取須申請 VPN 帳號 ● 訂定人員裝置使用管理規範，如：軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則
社交演練與資安教育訓練	● 定期辦理社交演練，如模擬網路釣魚郵件活動 ● 定期辦理資訊安全意識訓練，如辦理年度教育訓練與測驗和資安政策溝通宣導
確保系統的永續運作	● 遵循 ISO 27001：2013 資訊安全管理系統定期執行內部稽核，確保控制設計及執行之有效性。 ● 鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標(RTO)及資料復原時間點目標（RPO)，設置適當之備份機制及備援計畫 ● 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，演練內容包含核心業務備援措施、人員職責、應變作業程

資安管理項目	說明
	序、資源調配及演練結果檢討改善

2.3.3 資安事件通報與因應流程(GRI 418-1)

當發生資訊安全事件時，員工必須立即按照《資訊安全事件報告和處理程序》向其主管報告。團隊負責人將事件報告給資訊暨資安管理處專責人員，後者根據內部程序對資訊安全事件進行分級。如果事件符合重大異常事件的條件，則將報告上報給資安長和執行長。對於涉嫌資訊洩露的重大異常事件，同時需通知人力資源部門和審計辦公室。如果確認發生洩露，資訊暨資安管理處將根據法律要求或內部政策處理此案。對於所有安全事件，必須填寫「資訊異常事件報告」並提交給資訊暨資安管理處主管、資安長或更高級別的管理人員，以評估事件之影響及相對應之措施。2024 年，AMAX 並未發生重大資訊安全事件，亦無接獲客戶隱私侵犯或資訊洩漏相關之外部投訴事件。

2.3.4 資安教育訓練

AMAX 定期會進行社交工程演練，例如模擬網路釣魚郵件活動，以提高員工意識並加強網路安全防禦，每次演練平均約有 153 名參與者。該計畫包含詳細的實施措施，並追蹤執行頻率、參與情況和結果，以評估監控有效性。資訊暨資安管理處定期審查結果，以指導持續的培訓和政策改進。

資通安全管理執行情形

本公司重視資通安全治理，已建置完善之風險管理架構與控制機制，以確保資訊資產之機密性、完整性及可用性。公司依據國際標準導入 ISO 27001:2013 資訊安全管理系統，由 資訊暨資安管理處 統籌執行相關作業，並由 資安長 帶領團隊負責資訊安全管理之策劃與落實，涵蓋客戶資料、內部營運系統及各營運據點之實體與數位資產。公司每年或於重大變更後皆進行風險評估，建立存取控制、事件回應、風險處理及業務持續性計畫等措施，資訊安全事件將被記錄、審查及上報，並經正式流程追蹤改善，確保管理系統持續精進。

在資安政策與管理方案方面，公司管理層致力於維護資訊資產安全，並將保護員工及消費者個人資訊納入政策重點。資安長負責監督資訊與網路安全流程，另由風險主管執行風險處理計畫與定期評估，確保針對特定風險採取適當控制措施。公司之資訊安全政策涵蓋數據治理、設備資產管理、訪問控制與身分識別管理、業務連續與災難復原計畫、系統監控與可用性等面向，所有員工皆須遵守並接受資安教育訓練。

公司持續投入資源推動資通安全管理，2024 年度主要成果如下：

項目	內容
政策、承諾及重要性	隨著網路攻擊事件威脅不斷，資訊安全已成為全球企業營運之主要風險之一。為遵循資安法規與政策及避免遭受內、外部蓄意或意外之威脅，確保公司的持續營運，AMAX 導入 ISO 27001：2013 資訊安全管理系統，依照國際標準訂定資安政策，以保障公司與利害關係人之權益。AMAX 承諾維護資訊安全，持續監控資安管理成效，減少資訊安全事故之發生，強化本公司的資安韌性。
權責單位	資訊暨資安管理處
短中長期目標	■ 中期 1. 定期執行風險評估、資訊分類、權限控管及資安事件通報應變機制，並導入防火牆等技術性控制措施。 2. 2027 年 BitSight Internet security score 提升至 740 分。 3. 2028 年 Microsoft 365 安全分數提升至 88%。 4. 為所有 VPN 使用者設定雙重驗證。 ■ 長期 1. 2030 年 BitSight internet security score 提升至 760 分。 2. 2030 年 Microsoft 365 安全分數提升至 90%。 3. 備份伺服器設定雙重驗證。
行動計畫	1. 已導入 ISO 27001：2013 資訊安全管理系統，並取得獨立第三方驗證。 2. 每年進行資安相關教育訓練、社交工程郵件演練，強化員工的資安意識。 3. 每兩年進行攻擊模擬演練措施，維護組織的資安防護措施和應

	對能力。
2024 年績效	1. 系統弱點修補工具部署涵蓋率超過 91%。 2. 關鍵應用系統可用性達 99%。 3. 雲端應用系統可用性達 99.9%。 4. BitSight internet security score 720 分。 5. Microsoft 365 安全分數 84.98%。 6. 定期執行模擬網路釣魚郵件活動。 7. 辦理一場網路安全意識培訓(年度培訓項目),共有 131 人參與。 8. 本年度未發生重大資訊安全事件。
申訴機制	設有資安稽核制度與異常通報機制，追蹤資安措施執行。若有申訴事項，可直接向上級主管或資訊暨資安管理處反應。將由專責人員對主管報告該事件的影響範圍、損害程度進行分類與評估後，提出應急處理方案和建議，並將針對資訊安全紀錄相關問題，於事件解決後需保存相關證據，檢討事件並總結反思。

AMAX 實施符合 ISO 27001：2013 資訊安全管理系統標準，以保障其資訊資產的機密性、完整性和可用性。設有資訊暨資安管理處，由資安長帶領團隊負責統籌並執行資訊安全管理系統。此系統涵蓋所有客戶與內部數據處理部門，包括實體和數位資產。公司每年或在重大變更後進行風險評估，並基於管理系統，實施存取控制、事件回應、風險處理和業務持續性等控制措施。資訊安全事件將被記錄、審查及上報，並通過正式流程追蹤糾正措施。管理層定期審查系統的有效性，以確保持續改進。

- AMAX 美國總部取得 ISO 27001：2013 資訊安全管理系統認證。

SCB
SYSTEMS CERTIFICATION BODY

INFORMATION MANAGEMENT SYSTEMS CERTIFICATE

This certifies that the quality system of

AMAX Engineering Corporation

1565 Reliance Way, Fremont, CA 94539, USA

Systems Certification Body recognizes that the organization above has established and applies an Information Security Management System according to the Statement of Applicability for

ISO 27001:2013

Scope of Registration

The manufacturing and distribution of computing systems, such as servers, storages, clusters for OEM/ODM, enterprises, and the cloud market, including data center. The provision of technical supplies and servicing of computer systems for use in the medical device industry.

Certificate No: 1104771

Certificate Decision/Re-Issue Date:	07/26/2023
Certificate Issue Date:	07/26/2023
Certificate Expiry:	07/14/2026
Site Structure:	Single Site

SHIRLEY DEWI, SR. VICE PRESIDENT OF
MANAGEMENT SYSTEM REGISTRATION SERVICES

909.230.5526 | WWW.IAPMOSCB.ORG
5001 E. PHILADELPHIA ST, ONTARIO, CA 91761-2816

CERTIFIED BY SCB ISO 27001