版次	3
修訂日期	112/9/12

亞洲電材股份有限公司

資訊安全風險管理政策

第一條 目的

本公司為確保公司電腦主機、服務器、網絡設備、辦公設備通訊安全，降低因爲人爲疏忽、蓄意、天然災害等導致公司資訊被偷竊、洩露、篡改或者破壞等風險；確保公司資訊機密性、完整性、可用性；機密性：確保資訊只能由被授權之人才能使用；完整性：確保資訊正確無誤、未被篡改；可用性：確保資訊可用性，特製訂本政策。

第二條 資訊安全風險管理架構

本公司資訊安全的權責部門為資訊部，有資訊主管、專業的資訊工程師，負責制定公司資訊安全政策，規劃資訊安全措施，並執行相關資訊安全作業。

第三條 資訊安全及管理政策

為強化資訊安全管理，確保資訊的機密性、完整性、可用性，並避免遭受內部、外部的蓄意或者意外的威脅，資訊安全設施與管理方式分爲六大項，闡述如下：

一、服務器及網絡設備安全管理：

(一)公司服務器主機、主網絡設備全部設置在資訊機房，機房門禁採用鑰匙進出管理。

(二)公司資訊主機房設置有空調設備，維持服務器主機、網絡設備於適當的溫度環境下運行。

(三)機房服務器主機、網絡設備配置不間斷電源 UPS 系統，避免因爲意外斷電造成的系統當機，確保停電時不會中斷服務器應用服務。

(四)針對具有存儲功能的設備,不限於硬碟、 U 盤，在移轉、報廢時對其進行重置處理。

二、網絡安全管理：

(一)加強網絡管控，企業對外網絡入口，配置了企業級防火墻，阻擋駭客非法入侵。

(二)東台雅森與昆山雅森通過中國移動專綫進行連接，臺灣亞電、東莞分

公司、廈門辦事處通過專業廠商 MPLS VPN 線路，其具有相關資質，保證我們公司的 VPN 線路服務穩定、安全、可靠。

(三)公司員工遠端登錄公司內部查看系統相關資源，必須申請 VPN 帳號，經授權後方能訪問。

(四)公司內部配置有上網行爲管理設備，能夠控管網際網絡存取，可遮罩有害的、有木馬病毒的網站，強化網絡安全，防止網絡頻寬被不當的應用佔用。

三、病毒防護與管理：

(一)服務器與辦公電腦設備均安裝有病毒防護軟體，公司購買病毒防護軟體，病毒碼可自動更新，確保能阻擋最新型病毒，同時可以偵測、防止具有潛在威脅性的軟體安裝。

(二)電子郵件服務器前端配置有病毒郵件、垃圾郵件過濾服務器，能夠有效阻擋垃圾郵件、病毒郵件進入郵件服務器。

(三)公司企業級防火墻能夠檢測到異常電腦木馬病毒，提供相關的日誌資訊。

四、系統存取控制：

(一)公司員工對各應用系統使用，需透過公司內部 BPM 系統資訊權限申請表單進行申請，經權責主管核准後，由資訊部建立系統帳號，並依據所申請職務權限進行系統權限設置。

(二)帳號密碼設置，規定適當的強度、字數，包含文字、數字、特殊符號混雜，電腦帳戶密碼三個月更改一次。

(三)同仁辦理離(休)職手續時，會簽資訊部，進行各系統帳號的停用、刪除作業。

(四)對於個人資料（不限於企業內部人員、客戶、廠商、求職者），在存取、傳遞、銷毀等環節加強資安管理。

五、確保系統的安全性：

(一)系統備份：公司重要數據庫每天備份，公司電腦機房 NAS 備份一份及異地 NAS 備份一份。

(二)災害復原演練：系統每年實施一次演練，選定還原日期基準點後，由備份 MAS 回存於系統主機，再驗證資料的正確性，確保備份媒體的正確性與有效性。

六、資安宣導與教育訓練：

(一)定期宣導。要求同仁定期更換系統密碼，以確保帳號安全。

(二)資訊安全培訓。每年對內部同仁實施資訊安全相關教育訓練課程,提高員工資安安全意識。

第四條 投入資通安全管理之資源:

為實踐六大項資通安全政策，投入之資源如下：

一、網路硬體設備如企業防火牆、垃圾郵件過濾設備、上網行爲管理設備、核心交換機、可管理交換機等。

二、軟體系統如終端殺毒軟體、備份軟體。

三、投入人力如: 每日各系統狀態檢查、每週定期備份及異地備份、每年資訊安全教育培訓課程、每年系統災難復原執行演練。

第五條 適用範圍

本辦法適用於昆山雅森電子材科技有限公司，雅森電子材料科技(東台)有限公司。

第六條 實施與修訂

本辦法經總經理核准後實施；修訂時亦同。

本辦法初版訂於 111 年 12 月 26 日，修訂日期 112 年 9 月 12 日。