文件編碼	聯穎科技股份有限公司	生效日期	2023/11/01
T-WI-110200-005		版　　次	A
文件名稱	**資通安全政策**	頁　　次	1/2

一、資通安全風險管理架構

本公司資訊安全權責單位為資訊管理處，負責制定公司資通安全政策，建立安全及可靠之公司作業環境，確保資料、系統和網路環境的安全。稽核處為資訊安全監理之查核單位，稽核資訊安全規範，並定期查核是否落實資安規定，以降低資安風險、損害。

二、資通安全政策

1. 需登入帳號及密碼方可使用公司系統資源並設定密碼長度、密碼歷程記錄、密碼最長之效期限制、登入失敗鎖定機制，且僅能在有授權的範圍內作業，以維護系統之安全性與可控性。
2. 使用者密碼，可隨時自行更新，資訊管理處定期加強宣導使用者變更密碼及宣導資訊安全政策及規定。
3. 各項網路服務之使用依資通安全政策執行，不同的部門屬性賦予不同的權限設定。
4. 定期檢視防火牆和郵件閘道器的設定並適時的補強其安全機制，確保公司網路環境和郵件傳遞的安全。
5. 作業系統、網路環境和電子郵件即時自動偵測和掃描病毒。
6. 定期更新防毒軟體版本及隨時更新保持最新之病毒碼。
7. 每日定時自動執行系統資料備份作業。
8. 重要備份之外接儲存媒體，資訊管理處另存放於公營或商譽良好的民營銀行保險箱，且每周至少需更新一次存放的外接儲存媒體。
9. 重要系統之資料，建立異地備援機制，並存放於提供異地備援服務公司的 IDC 機房。
10. 資訊安全之主管及人員，接受資訊安全相關訓練。
11. 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。

三、具體管理方案

1. 硬體設備及機房管理
   (1)未經資訊人員許可，不得私自移動或拆解電腦、主機、顯示器等電腦週邊相關設備。
   (2)不得私自變更電腦系統相關設定，必要時，需經由資訊人員協助處理。
   (3)機房設置獨立空調、備援空調、消防設備、監控錄影、門禁、不斷電系統，並定期設備保養、維護，使其能持續提供正常、安全運作。
   (4)進出機房時需有本公司資訊人員陪同並填寫電腦機房門禁管制表。

(5)廠商進行軟硬體設備維護時，需由本公司資訊人員陪同、監督下始可為之。

2.軟體版本管理

(1)非經合法程序取得之軟體系統嚴禁於本公司使用，並建置軟體盤點系統，查看軟體使用情形。

(2)非經資訊單位確認之軟體，無論合不合法，不得安裝於本公司之電腦設備。

(3)公用軟體及文件存放於資訊管理處安全之處所，並經適當保管。

3.病毒暨非法入侵及電子郵件管理

(1)本公司內部全體人員使用的個人電腦和伺服器設備均安裝防毒軟體，並使用防毒軟體偵測外來儲存媒體之病毒和使用弱點利用防禦，且自動更新最新版本之病毒碼。本公司有垃圾郵件防護設備，且透過本公司電子郵件伺服器傳送或接收之電子郵件及其附加檔，則每封將會掃毒檢測無誤後才會傳送或接收，機敏性電子郵件使用者將使用電子郵件加密方式寄出。

(2)全天候偵測並阻隔所有非法入侵本公司之網路行為，並適時的調整防禦機制。

4.重大災變緊急應變及復原計劃管理

為因應突發性事故導致系統無法正常運作，本公司制定災難復原計畫；針對類似狀況模擬系統緊急應變及復原計劃並定期測試，記錄測試程序及結果，並分析改善程序，以使公司資訊運作所受災變影響程度降至最低。

四、投入資通安全管理之資源

每年編列資訊預算維持並強化資訊安全防護，如軟硬體維護續約、機房相關設備汰舊。

五、本政策依文書文件文書及文件管理制度規定核准後公告。