# 中興電工機械股份有限公司

# 資訊安全管理辦法

民國 109 年 5 月 21 日
資字第 1090024 號

第一條：目的

建立安全及可信賴之資訊化作業環境，確保本公司電腦資料、系統、設備及網路安全，以維持本公司業務之正常運作及永續發展，並在兼顧資訊安全與作業效率下 ，建立資料處理、交換及安全控管機制，擬定本公司之資訊安全管理政策。

第二條：範圍：

一、人員

本辦法所指人員或員工係包含本公司編制內人員、約聘僱人員、臨時人員本公司有合作關係或業務往來之公司、廠商、自然人及廠商派任執行本公司各項作業之相關人員，因業務之需而必須蒐集、處理或利用本公司、本公司之客戶或專案相關之個人資料者，均屬本辦法涵蓋之對象。

二、系統

本辦法所指系統係包含本公司現行及未來建置之各項資訊相關系統。

三、內容

本辦法內容包括如下：

1. 資訊安全組織及權責分工。
2. 人員管理及資訊安全教育訓練。
3. 電腦系統安全管理。
4. 網路安全管理。
5. 系統存取控制管理。
6. 系統發展及維護安全管理。
7. 資訊資產安全管理。

8. 實體及環境安全管理。
9. 業務永續運作計畫管理。
10.個人資料保護管理。
11.其他資訊安全管理事項。

第三條：資訊安全組織及權責分工：

一、 資訊安全組織

本公司之資訊安全相關政策由資訊單位負責制定：

1. 資訊單位之職責：

負責訂定及檢討公司資訊安全政策規劃，針對各項資訊安全措施辦理風險評估，監督資訊安全管理事項、進行資訊安全政策符合性檢查。

2. 資訊安全工作之權責與分工：

(1) 規劃作業：負責資訊安全政策、計畫及技術要點之研擬、建置及評估等事項，由資訊單位辦理。

(2) 安全控管：負責資料及資訊系統之安全需求研議、使用管理及保護等事項，由資訊單位配合各事業單位代表辦理。

(3) 個資控管：負責本公司個人資料保護政策之擬訂及推展，由資訊單位配合各事業單位代表辦理。

(4) 資安稽核：負責資訊機密維護及資訊安全之稽核事項，由稽核單位會同資訊單位及各業務相關單位辦理。

(5) 門禁管制：依照公司廠區門禁管理辦法。

(6) 委外、第三方與協力廠商：依據合約內容配合本公司資訊安全運作。

第四條：人員管理及資訊安全教育訓練：

一、 人員安全管理

1. 本公司對於新進用及調派之人員，倘其工作職掌須使用或處理敏感性資訊的資訊科技設施或涉及機密性及敏感性資訊者，應經適當的安全評估程序，並簽署保密協議書。

2. 本公司各級主管應負責督導所屬人員之資訊作業安全，防範不法及不當行為；對可存取機密性、敏感性資訊或系統者及配賦系統存取特別權限之人員，應妥適分工，分散權責。

3. 本公司資訊安全政策應以書面、電子或其他方式告知員工，員工應遵守本辦法及其他相關資訊安全規定。員工若違反資訊安全相關規定，得依情節輕重予以處分。

4. 本公司員工應遵守維護公務機密之相關法令規定；在職及離退職後，均不得洩漏所知悉之業務機密，或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

二、 資訊安全教育訓練

1. 依員工角色及職務層級，進行適當的資訊安全講習，促使員工瞭解資訊安全的重要性及各種可能的安全風險，以提高員工資訊安全意識。

2. 安排從事資訊安全業務之資訊相關人員定期進行資安相關課程之教育課程進修，以獲知最新之資安技術與知識。

3. 員工必須瞭解單位之資訊安全政策。

4. 隨時公告資訊安全相關訊息及防範措施。

5. 不定期派員參與外界舉辦相關訓練、研討會。

6. 發生資訊安全事件，應通報資訊單位人員，並記錄處理與追蹤。

第五條：電腦系統安全管理：

一、電腦主機管理

1. 電腦主機及伺服器操作程序，應以書面或電子方式載明，以確保員工正確及安全的操作使用電腦。

2. 各項電腦主機及伺服器均應指定專人管理，非經核准不得任意使用、拆卸及更動零組件。

3. 各類電腦主機、伺服器及重要之個人電腦皆應設定足夠強度之密碼。

4. 訂定電腦主機停機之回復標準作業程序。

5. 各主機及伺服器均接上不斷電裝置，以防不正常的停電狀況發生。

6. 電腦主機及伺服器儲存之重要資料應依規定定時進行備份作業。

7. 個人電腦禁止外接未經核准之行動裝置，各電腦系統的 USB 接孔依業務需要經核準後開放或取消，以防止透過 USB 裝置存取公司電子資料。

二、 電腦軟體及病毒防禦管理

1. 嚴禁安裝未經核准可安裝的軟體。

2. 嚴禁使用未經授權之軟體，並遵守智慧財產權相關規定。

3. 嚴禁使用或開啟來路不明及內容不確定之軟體、磁性媒體或電子郵件。

4. 建置防火牆及防毒軟體以區隔內部網路與網際網路間之非法連結，阻絕電腦病毒及惡意攻擊性軟體之非法入侵或非法存取資料。

5. 電腦病毒碼及防制軟體應定期更新。

6. 定期修補系統漏洞程式。

第六條：網路安全管理：

一、 網路設備

1. 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

2. 禁止及防範網路使用者以任何儀器設備或軟體工具竊取網路上的通訊。

3. 網路主機應關閉非必要的服務程式，並隨時更新程式版本。

二、 網路行為

1. 本公司員工經申請帳號後成為合法授權的網路使用者並在授權範圍內存取網路資源。

2. 提供給內部人員使用的網路服務，與開放業務有關人員從遠端登入內部網路系統的網路服務，應執行嚴謹的身分辨識作業，或使用資訊相關設備進行安全控管。

3. 網路系統管理人員未經權責主管人員許可，不得閱覽使用者之私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權檢查其檔案。

4. 公司人員禁止利用公司網路從事不法及侵害他人權利之情事。

5. 公司之網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。

6. 公司人員禁止私接任何網路設備妨害網路系統的正常運作。

7. 訪客所攜帶之資訊設備、行動裝置，非經允許不得連上公司內部網路。

三、 電子郵件

1. 機密性資料及文件不得以本公司以外之電子郵件或其他電子方式傳送。

2. 不可隨意開啟來路不明的電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞；收到來路不明的電子郵件時應通知系統管理者處理。

3. 禁止發送垃圾郵件騷擾他人，導致其他使用者之不安與不便。

4. 禁止發送匿名信，或偽造他人名義發送電子郵件。

第七條：系統存取控制管理：

一、 人員存取管理

1. 使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。

2. 使用者應確實瞭解系統存取的各項條件及要求，並在授權範圍內存取系統資源。

3. 對系統服務廠商以遠端登入方式進行系統維修者，應建立人員名冊加強安全控管，並要求其相關安全保密責任。

二、 資料存取管理

1. 重要資料之委外建檔，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

2. 存放機密性及敏感性資料之電腦主機或伺服器，除作業系統既有的安全設定外，應強化身份辨識之安全機制，防止非法使用者透過遠端撥接或網際網路傳送資料時，被偷窺或截取登入密碼，及防制假冒合法使用者身分登入主機進行偷竊或破壞等情事。

3. 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

4. 為保護及防止不當使用向其他單位索取錄製之個人資料電腦檔案，凡涉及個人資料之電腦檔案，其操作使用及安全維護將依據「個人資料保護法」及其他相關法令規定辦理，上開法令修正時亦同。

三、 帳號及密碼管理

1. 建立系統使用者帳號管理制度，加強使用者通行密碼管理，設定足夠強度之密碼，並定時更換。

2. 離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

第八條：系統發展及維護安全管理：

一、 系統發展及維護管理

1. 公司自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

2. 各單位對於廠商之軟硬體系統建置及維護人員，應要求及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即

取消其使用權限。

3. 各單位委託廠商建置及維護重要之軟硬體設施，應在機關相關人員監督及陪同下始得為之。

二、 資訊委外作業服務管理

1. 資訊作業委外時，應於事前評估潛在風險與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款。
2. 資訊委外服務契約應註明事項如下：
   (1) 涉及機密性、敏感性或關鍵性的應用系統之機密等級。
   (2) 須經核准方得執行的事項。
   (3) 業者應遵守的資訊安全要點及標準，評鑑業者的項目及程序。
   (4) 業者處理及通報事件的責任及程序。
   (5) 業者應配合事項並簽定保密切結書及智財相關協議書。

第九條：資訊資產安全管理：

一、 資訊資產目錄之建立

1. 主管財產管理業務單位應會同主管資訊業務單位建立資訊資產目錄，目錄內容應包括資訊資產的項目、保管者等。
2. 資訊資產包括項目如下：
   (1) 資料：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業及支援程序、備援回復作業計畫等。
   (2) 軟體：應用軟體、系統軟體、發展工具及公用程式等。
   (3) 硬體：電腦及通訊設備、資料儲存媒體等。
   (4) 其他相關設備。

二、 資訊資產安全之等級分類及標示

1. 資訊安全分類原則上依據「國家機密保護法」、「電腦處理個人資料保護法」及「行政資訊公開辦法」等相關法規，建立資訊安全等級之分類標準，上開法令修正時亦同。

2. 資訊資產安全分類標準，應考量資訊分享及資料的機密性、正確性及安全等級，由業務單位或指定的系統管理者負責界定。

3. 已列入安全等級分類的資訊及系統之輸出資料，應以文字及顏色標示適當的安全等級以利使用者遵循。

第十條：實體及環境安全管理：

一、一般辦公環境之安全保護

1. 實體環境的安全保護，應以事前劃定的各項資訊設施為基礎，並設置必要的身分識別程序，以達成安全控管的目的。

2. 每項資訊設備的實體保護程度，以及實體身分識別程序，應依資訊資產等級及其安全風險價值決定。

3. 電腦相關軟硬體設備或資料，須經主管資訊業務單位人員確認及核准後，方可帶離辦公場所，各業務單位自行開發之系統及建置之資料亦應於單位主管之核准後，方可帶離辦公場所。

4. 個人電腦及電腦終端機不再使用時，應關機、上鎖或是其他控制措施保護。

5. 個人電腦嚴禁使用非經授權及來路不明之軟硬體。

6. 列印之文件及磁性媒體在不使用或非上班時段，應存放在櫃子內，機密性及敏感性資訊並應上鎖保護。

二、電腦機房之安全管理

1. 電腦機房應考量火災、自然災害等的實體安全防護措施，並考量鄰近空間的可能安全威脅。

2. 危險性及易燃性的物品，應存放在遠離電腦機房的安全地點。

3. 人員進入電腦機房應予適當的管制，並記錄進出時間；人員只有在特定的目的或是被授權情形下，才能進入電腦機房。

4. 建置機房火警、空調、溫溼度、電源供應等警示自動通報系統，全天候掌控機房運作情況，以確保機房設施安全。

5. 安裝適當的安全偵測及防制設備，例如熱度及煙霧偵測設備，火災警報設備、滅火設備及火災逃生設備；各項安全設

備依廠商的使用說明書定期檢查。

第十一條：業務永續運作之規劃：

一、人為及天然災害處理

為因應各種人為及天然災害造成業務運作受影響，依公司「重大緊急事故處理辦法」使各項業務得以永續運作。

二、資安事件通報

1. 各單位在發生資訊安全事件時，應依公司「重大緊急事故處理辦法」之規定處理程序並採取反應措施，必要時得聯繫檢警調單位協助偵查。

2. 有關公司「資通安全事件緊急應變計畫暨作業處理程序」授權由公司資訊單位參照公司「重大緊急事故處理辦法」及本辦法之精神訂定之。

第十二條：有關資訊作業涉及個人資料者，悉依個人資料保護法或相關法令規定辦理，本辦法並授權由資訊單位就個人資料之範圍、具體保護措施及銷毀方法等細節性或技術性事項於呈准後以公告或訂定實施電子文件作業管制細則方式規定之，修正或廢止時亦同。

第十三條：實施與修訂

本辦法之制、修訂，經董事會決議後公佈實施，廢止時亦同。