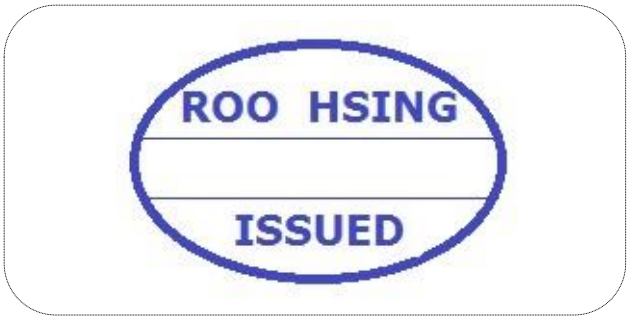
如興股份有限公司	制定單位	資訊中心
	制修訂日	2021/2/22
	編號/版本	09-0600 v1.1
	文件密等	普通件

09-0600 資訊安全政策

版本：1.1

文件代號：1



公司文件控制中心受控文件

未經許可不得複印或取離本公司

目錄：

文件修正一覽表

文 件 修 正 一 覽 表

次數	修訂日期	版本	修改內容
1	2018.01.07	1.0	制訂發行
2	2021.02.22	1.1	文件更新

1. 目的

如興股份有限公司（以下簡稱本公司）為強化資訊安全管理，確保公司正常營運，保護本公司核心業務相關資訊資產（資訊資產包括資料、系統、設備、軟體授權等）之安全，及防範資訊運用過程發生影響資訊及系統機密性、完整性及可用性之安全事件，確保本公司資訊處理作業能安全有效地運作，特制訂資訊安全政策。

2. 適用範圍

2.1 舉凡本公司執行業務相關的資訊資產（包括資料、系統、設備、網路、及軟體授權等）、人員與作業程序等均適用本資訊安全政策。

3. 名詞定義：

無。

4. 權責單位

4.1 總經理

負責資訊安全政策之決策與指導。

4.2 資訊中心

本作業程序之制修訂及主要執行部門。

4.3 各部室

各使用單位依規定保護資訊資產、通報資安事件、遵循公司資訊安全之責。

5. 作業程序

政策宣言：本政策考量公司業務上實際需求，進行本資訊安全管理規範訂定。

5.1 成立資訊安全小組與應變小組

5.1.1 資訊處主管為資訊安全小組（以下簡稱資安小組）與應變小組的召集人。相關成員應含括可確保本公司營運、聯繫作業正常進行之公司內部主管、工作人員。

5.1.2 資安小組與應變小組之公司內部成員應確實知悉各項資安管理、執行之工作內容。

5.1.3 資訊處主管應將上述小組成員的名單、聯絡方式與所負責事項，建立於如附件 8.1 的「資訊安全小組名單」與「應變小組名單」，發送給資訊處同仁、資訊處上一級主管與總經理，並留有傳送或簽認記錄，更新時亦同。

5.1.4 「資訊安全小組名單」與「應變小組名單」應由資訊處主管指定專人保管與

維護，並於異

動時隨時更新，未有異動時至少每季確認一次聯絡人資訊之正確性，並留有確認紀錄。

5.2 人員安全管理及教育訓練

5.2.1 人員進用之評估

(1)人員進用之安全評估

進用之人員，如工作職責須使用敏感性、機密性資訊的科技設施，或須處理機密性及敏感性資訊者，應另外簽署保密切結書，並予以歸檔交由管理部管理。

5.2.2 使用者資訊安全教育訓練

(1)資訊安全教育訓練

1.應定期對員工進行資訊安全教育及訓練,促使員工瞭解資訊安全的重要性,各種可能的安全風險,以提高員工資訊安全意識,促其遵守資訊安全規定。

2.應以人員角色及職能為基礎，針對不同層級的人員，進行適當的資訊安全教育及訓練；資訊安全教育及訓練的內容應包括：資訊安全政策、資訊安全法令規定、資訊安全作業程序，以及如何正確使用資訊科技設施之訓練等。

5.3 電腦系統安全管理

5.3.1 電腦系統作業程序及責任

（1）電腦系統作業程序之訂定

1.依照公司電子計算機作業循環規定進行之。

2. 如果遭遇非預期的電腦系統作業技術問題時，應即時通知資訊單位。

5.3.2 資訊委外作業

辦理資訊業務委外作業，應與委外廠商簽訂相關資訊保密合約；相關合約內容需經公司法務單位進行審閱後，行相關用印程序作業。合約用印完成後，

依照公司合約管理進行歸檔作業。

5.3.3 **電腦病毒及惡意軟體之防範**

(1) 應於公司所屬主機設備、網路環境進行事前預防及保護措施，防制及偵測電腦病毒、特洛依木馬等惡意軟體的侵入。資訊單位並應備妥公司網絡拓樸圖，以利管理。

(2) 不應保有及使用未取得授權的軟體

5.3.4 **電腦系統及資料檔案之保護**

(1) 公司文件及執行業務相關之資料應儲存在公司內部檔案伺服器內。檔案伺服器應定期進行進行相關備份作業。

(1.1)伺服器-作虛擬主機備份

(1.2)資料庫-上班日進行差異備份、每週六進行全備份。

(1.3)檔案伺服器-系統每日進行差異備份，每週六進行全備份。

(2) 檔案資料依照各部門單位所屬權限分別管理。

5.4 網路安全管理

5.4.1 **網路安全規劃與管理**

(1) 網路安全規劃作業

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、動態密碼、防火牆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) 網路服務之管理

1.網路系統管理人員應執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性。

2.對任何網路安全事件，網路系統管理人員應立即向電腦安全事件緊急處理小組反應。

(3) 網路使用者之管理

1.被授權的網路使用者（以下簡稱網路使用者），只能在授權範圍內存取網路

資源(例如：網域內的使用者)。

2.網路使用者應遵守資訊安全政策，其密碼至少必須含括英文+特殊字元+數字至少八碼，每90天變更。

3.網路使用者不得將自己的登入身份識別與登入網路的密碼交付他人使用。

4.應禁止網路使用者以任何方法竊取他人的登入身份與登入網路通行碼。

5.資訊人員離職，須於離職當日進行所屬管轄之設備，全面密碼變更作業。

（4）主機安全防護

1.存放機密性及敏感性資料之大型主機或伺服器主機(如Domain Name Server、防火牆等)，除作業系統既有的安全設定外，應規劃安全等級較高之密碼辨識系統，以強化身份辨識之安全機制。其密碼至少必須含括英文+特殊字元+數字至少12碼。

（5）防火牆政策

1.公司與外界網路連接的網點，應加裝防火牆，以控管外界與公司內部網路之間的資料傳輸與資源存取。

2.標準政策如下所述：

2.1防火牆密碼設定等同重大主機設定之規定。

2.2內部服務器對外之服務,其服務主機IP設定須為內部IP,禁止使用對外IP，暴露位址增加安全風險。

2.3須建立網路服務轉送指定內部伺服器策略（即NAT)，藉此提供E-Mail、FTP(**F**ile **T**ransfer **P**rotocol)、WWW(**W**orld **W**ide **W**eb)等網路服務。

2.4外點單位如有總部內部服務需求，須採用IP-SEC(**I**nternet **P**rotocol **Sec**urity)加密模式進行連線；並指定允許網段進行連線服務。

2.5遠端桌面連線策略僅提供允諾之來方IP(Internet Protocol)位址進行連線。如有需增加連線IP，需求單位需透過資訊服務單申請，申請核准後由資訊

人員進行設定。

2.6防火牆禁止非網域帳號進行郵件RELAY功能，公司郵件服務器僅允許內部帳號人員，才可進行郵件服務功能。

2.7防火牆設備，必須確保在保修內。確保可更新原廠提供之防護策略修正。

2.8防火牆策略修訂、韌體更新前，需備份現有策略條件乙份至T:\\資訊管理中心>對內資料>防火牆備份內，修訂後也需重新備份乙份至指定位址。

2.9防火牆日誌需每天由資訊人員連線審閱，並記錄在每日網路檢查內。

2.10防火牆管理須列入災難演練，該部分需要依照「災害系統復原計畫及測試作業程序」進行之。

2.11防火牆修正策略應透過「系統程式修改申請單」進行。

2.12應每季(3、6、9、12月，第四週)檢查防火牆策略是否符合現有實際作業，如有檢查應記錄在當日防火牆檢查紀錄表中。

3.防火牆應由網路系統管理人員執行控管設定

4.防火牆設置完成時，應測試防火牆是否依設定的功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定的安全目標。

5.網路系統管理人員應配合資訊安全政策及規定的更新，以及網路設備的變動，隨時檢討及調整防火牆系統的設定，調整系統存取權限，以反應最新的狀況。

6.防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。

(6) 網路資訊之管理

1.機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

2.網路系統管理人員應負責監督網路使用情形，並透過系統自動記錄資料(如log資料)進行每日檢查。

5.對外開放的資訊系統所提供之網路服務(HTTPS(**H**yper **T**ext **T**ransfer

Protocol over **S**ecure Socket Layer),E-Mail,HTTP(**H**yper **T**ext **T**ransfer **P**rotocol)等)，應做適當的存取控管，以維護系統正常運作。

5.4.2電子郵件之安全管理

（1）電子郵件安全管理機制

1.應依資訊安全政策及規定，使用電子郵件。

2.應建立電子郵件的安全管理設備或軟體(如 SPAM 軟體)，以降低電子郵件可能帶來的業務上及安全上的風險。

3.為防範假冒機關員工名義發送電子郵件，並達到身分辨識及不可否認的目地，必須透過身分驗證等形式通過，才予以使用電子郵件服務。

4.電子郵件附加之檔案，同仁應事前檢視內容重要性後方可傳送。

5.對來路不明的電子郵件，應交由網路系統管理者處理，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

5.4.3 外點連線公司內部資訊網之安全管理

外點單位或人員出差作業，需連線回公司內部，宜經由防火牆與總部進行VPN(**V**irtual **P**rivate **N**etwork)連線作業(IP-SEC)或個人透過SSL-VPN(**S**ecure **S**ockets **L**ayer)處理，以確保資料的安全性。

5.4.4 網路設備備援與系統備援

1.為維持網路的持續正常運作，各重要網路設備應有備援。

2.為確保內部網路與外界的服務持續暢通，內部網路與外界網路的連接，應有一個以上的替代路徑。

5.5 系統存取控制

5.5.1 資訊系統存取控制規定

1.系統存取政策及各級人員之存取權限應予明確規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。

2.應將業務系統之存取控制需求，依公司相關規範明確告知系統服務提供者，以利其執行及維持有效的存取控制機制。

5.5.2 使用者之存取管理

（1）使用者註冊管理

1.對於多人使用的資訊系統，應建立正式的使用者註冊管理程序。

2.使用者註冊管理程序，應考量的事項如下：

2.1 查核使用者是否已經取得使用該資訊系統之正式授權。

2.2 查核使用者被授權的程度是否與業務目的相稱，是否符合資訊安全政策及規定（例如:有無違反權責分散原則。）

2.3 應以書面、電子或其他方式，告知使用者之系統存取權限。

2.4 在系統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。

2.5 應建立及維持系統使用者之註冊資料紀錄，以備日後查考。

2.7 使用者調整職務及離(退)職時，應儘速註銷其系統存取權利。

2.8 應定期檢查及取消閒置不用的識別碼及帳號。

5.5.3 網路存取之安全控制

（1）網路服務之限制

使用者應在授權範圍內存取網路系統服務事項。

（2）強制性的通道

應建立強制性的通道(例如：IP-SEC、SSL-VPN)，防止未被授權的使用者從不同的管道進入電腦系統。

（3）遠端連線作業埠之控制：對廠商、公司員工以遠端登入方式進入電腦網路系統進行作業，應採取安全控管機制(例如：身分驗證機制)。

（4）網路連線作業之控制

為確保系統安全，跨企業的網路系統可限制使用者之連線作業能力。例如，以防火牆技術依事前訂定之系統存取規定，過濾網路之傳輸作業。

5.5.4 電腦系統之存取控制

（1）應建立自動化的端末機身分鑑別系統，以鑑別從特定位址連上網路的使用者身分。

（2）使用者端電腦登入程序

1.使用者存取電腦系統，應經由安全的系統登入程序(例如：透過網域使用者管理架構、主機使用者帳號管理架構)。

2.登入程序應具備下列的功能：

2.1 不應顯示系統及應用系統識別碼，直到成功登入系統。

2.2 系統不應在登入程序中，提供未經授權的使用者有關登入系統的說明或協助性的訊息。

2.3 只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性。

2.4 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

5.5.5 應用系統之存取控制

（1）資訊存取之限制

1.應依資訊存取規定，配賦應用系統的使用者（包括應用系統支援人員）與業務需求相稱的資料存取及應用系統使用權限。並適當地編輯作業手冊，限制使用者僅能獲知或取得授權範圍內的資料及系統存取知識。

（2）原始程式資源之存取控制

1.對應用系統原始程式資料之存取，應建立嚴格的安全控制機制。

2.原始程式資源之存取控制，應考量下列事項：

2.1 應用程式原始碼資料庫，應儘可能不要存放在作業系統的檔案中。

2.2 不應核發無限制存取應用程式原始碼之權限。

2.3 發展中或是維護中的應用程式，應與實務作業之程式原始碼資料庫區隔，不應放置在一起。

2.4 舊版的原始程式應妥慎典藏保管，並應保存所有的支援應用程式軟體、作業控制、資料定義及操作手冊等資訊。

5.5.6 系統存取及應用之監督

（1）事件記錄

系統自動建立例外事件及資訊安全事項的稽核軌跡，並保存半年的時間，以作隨時調查及監督之用。

（2）電腦作業時間校正：應定期校正電腦系統作業時間，以維持系統稽核紀錄的正確性及可信度，俾作為事後法律上或是紀律處理上的重要依據。

5.5.7 系統稽核規劃

（1）系統稽核控制

1.對作業系統進行查核之稽核需求及實際稽核作業，應審慎規劃，以免影響業務正常運作。

2.系統稽核應考量事項如下：

2.1 系統稽核查核時間，應提前告知以利其配合作業。

2.2 應限定以唯讀方式存取軟體及資料。

2.3 不能以唯讀方式進行系統存取時，應獨立複製另外一份系統檔案供稽核作業之用，且應於稽核作業完成後，立即消除檔案。

2.4 執行查核所需的技術資源，應於事前明確界定，並準備妥當。

2.5 執行特別的及額外的查核，應於事前明確界定需求及範圍，並與服務提供者協議。

5.6 系統發展及維護之安全管理

5.6.1 系統安全需求規劃

應在資訊系統規劃之需求分析階段，即將安全需求納入；新發展的資訊系統，或是現有系統功能之強化，皆應明定資訊安全需求，並將安全需求納入系統功能。

5.6.2 應用系統之安全

（1）資料輸入之驗證

輸進應用系統的資料，應在事前查驗，以確保資料的真確性。

（2）系統內部作業處理之驗證

系統內部的作業，應建立驗證資料正確性的作業程序，避免正確輸入資料到應用系統中，卻因系統處理錯誤或是人為因素而遭受破壞。

（3）資料加密

1.對高敏感性的資料，應在傳輸或儲存過程中以加密方法保護。

2.是否使用加密方法，應進行風險評估，以決定採取何種等級的安全保護措施。

3.使用加密技術時，如資訊專業人力及經驗不足，可請外界的資訊廠商提供技術諮詢服務。

5.6.3 應用系統檔案之安全

（1）作業軟體之控制

1.在作業系統上執行應用軟體，應限定只能由授權的管理人員才可執行。

2.執行碼尚未測試成功，且未被使用者接受前，不應在作業系統執行。

3.應保留舊版的軟體，以作為緊急應變措施之用。

（2）系統測試資料之保護

1.應保護及控制測試資料，避免以含有個人資料到真實資料庫進行測試；

2.在使用真實的資料進行測試時，測試完畢後，真實資料應立即從測試系統中刪除。

5.6.4 系統變更及維護環境之安全

任何的系統變更作業，皆應獲得權責主管人員的同意。並檢視系統安全控制，以確保系統變更作業不致影響或破壞系統原有的安全控制措施。

（1）作業系統變更之評估

1.作業系統應定期更新（例如安裝新的版本）；作業系統變更時，應評估其對應用系統是否造成負面的影響，或是產生安全問題。

2.作業系統變更之評估程序，應考量的事項如下：

2.1 作業系統變更的評估及測試結果，如須進行必要的調整，應納入年度計畫及預算。

2.2 作業系統的變更應即時通知資訊人員，以便在作業系統變更前，資訊人員可以進行適當及充分的評估作業。

（2）套裝軟體變更之限制

1.廠商提供的套裝軟體，應儘可能不要自行變更或修改，如因特殊需要須修改，應考量以下的事項：

1.1 是否會破壞系統內建的安全控制。

1.2 應取得套裝軟體開發廠商的同意。

1.3 應考量以標準化的系統更新方式，請廠商進行必要的變更。

1.4 應考量如自行變更套裝軟體，日後進行軟體維護的可能性。

1.5 套裝軟體如須變更，應保留原始的軟體，並將變更的資料予以記錄，以備日後軟體再更新之用。

5.7 資訊資產之安全管理

5.7.1 資訊資產目錄之建立及保護

建立一份與資訊系統有關的資訊資產目錄，訂定公司資訊資產的項目、擁有者等。

5.7.2 資訊安全之等級分類

（1）資訊安全分類原則

1.參考相關機關，建立資訊安全等級之分類標準，以及相對應的保護措施。

2.資訊安全分類標準，應考量資訊分享及限制的影響、未經授權的系統存取或是系統損害對機關業務的衝擊，尤其要考量資料的機密性、資料真確性及可用性。

5.8 實體及環境安全管理

5.8.1 設備安全管理

（1）設備安置地點之保護

1.設備應安置在適當的地點並予保護，以減少環境不安全引發的危險及減少未經授權存取系統的機會。

2.設備安置應遵循的原則如下：

2.1 需要特別保護的設備，應考量與一般的設備區隔，安置在獨立的區域。

2.2 應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應等可能的風險。

2.3 電腦作業區應禁上抽煙及飲用食物。

（2）電源供應

1.電腦設備之設置，應予保護，以防止斷電或其他電力不正常導致的傷害；電源供應依據製造廠商提供的規格設置。

2.應考量安置預備電源，並使用不斷電系統。

3.應謹慎使用電源延長線，以免電力無法負荷導致火災等危害安全情事。

（3）設備維護

1.應妥善地維護設備，以確保設備的完整性及可以持續使用。

2.設備維護的原則如下：

2.1 應依據廠商建議的維修服務期限及說明，進行設備維護。

2.2 設備的維護只能由授權的維護人員執行。

2.3 應將所有的錯誤或是懷疑的錯誤，予以明確記載。

（4）設備放置在外部空間之安全管理

設置在外部以支援業務運作的資訊設備,應同樣遵守資訊安全管理授權規定，維持與內部資訊設備一樣的安全水準。

（5）設備處理之安全措施

含有儲存媒體的設備項目（例如硬碟),應在處理前詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已經被移除。

5.8.2 周邊安全管理

實體環境的安全保護，應以事前劃定的各項周邊設施為基礎，並以設置必要的障礙（例如:使用密碼登入之安全門)，達成安全控管的目的。

（1）機房之安全管理

支援重要業務運作的電腦機房，應設立良好的實體安全措施；電腦機房地點的選定，應考量火災、水災、地震等自然及人為災害的可能性，並考量鄰近空間的可能安全威脅。

（2）辦公桌面之安全管理

為避免紙張文件及儲存媒體設備等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

1.應考量事項如下：

2.1 紙張文件及儲存媒體設備在不使用或是不上班時，應存放在櫃子內。

2.2 機密性資訊，不使用或下班時應該上鎖。

2.3 個人電腦及電腦終端機不再使用時，應以關機處理。

5.9 業務永續運作計畫之規劃及管理

5.9.1 業務永續運作之規劃

（1）業務永續運作之規劃程序

應訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及更新計畫。

1.業務永續運作計畫，應考量下列事項：

1.1 界定重要的業務作業程序，並訂定其優先順序。

1.2 評估各種災害對業務可能的衝擊。

1.3 維持永續運作之人員責任界定，以及緊急應變措施之安排。

1.4 應訂定**災害系統復原計劃及測試作業程序**

5.9.2 業務永續運作計畫之測試

1.業務永續運作計畫可能因事前的假設不正確、規劃不周全或設備及人員的職務調整變更，而無法發揮預期的作用，應定期測試及演練，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。

2.應擬訂測試作業的時程，定期進行測試，使應變計畫維持在有效及最新的狀態；測試計畫可以定期測試個別計畫的方式進行，以減少測試完整計畫的需

求及頻率。參閱災害系統復原計劃及測試作業程序。

5.9.3 業務永續運作計畫之更新

業務永續運作計畫應配合業務、組織及人員的調整變更而定期更新，以發揮計畫投資的效益及確保計畫持續有效。

6 附則

6.4.1 本作業程序未盡事宜處，得由權責單位視實際需要修訂呈報核准後辦理。

6.4.2 本作業程序經總經理核准後公告實施，修訂時亦同。

7 相關文件

7.4 內控制度-電子計算機作業循環-CEL100

7.5 災害系統復原計劃及測試作業程序

8 附件

「資訊安全小組名單」

類別	聯絡人員	負責事項	聯繫方式 （至少載明二種方式）
台北總部	部門: 職務: 姓名:		手機：家裡電話： 電子郵件： Line/Skype：
	部門: 職務: 姓名:		手機：家裡電話： 電子郵件： Line/Skype：
	部門: 職務: 姓名:		手機：家裡電話： 電子郵件： Line/Skype：

類別	聯絡人員	負責事項	聯繫方式 （至少載明二種方式）
	部門: **職務:** **姓名:**	**1.**	**手機：家裡電話：** **電子郵件：** **Line/Skype：**

主管： 經辦：

「應變小組名單」

類別	災害等級	聯絡人員	負責事項	聯繫方式 （至少載明二種方式）
公司內部	**L1 – L5**	**部門:** **職務:** **姓名:**		**手機：家裡電話：** **電子郵件：** **Line/Skype：**
	L1 – L5	**部門:** **職務:** **姓名:**		**手機：家裡電話：** **電子郵件：** **Line/Skype：**
外部支援	**L1 – L5**	**部門:** **職務:** **姓名:**		**手機：家裡電話：** **電子郵件：** **Line/Skype：**
	L1 – L5	**部門:** **職務:** **姓名:**		**手機：家裡電話：** **電子郵件：** **Line/Skype：**

主管： 經辦：

註：本表內容得由資訊處依其實務自行調整之。