

富育榮網股份有限公司

制訂部門	管 理 部	資 訊 安 全 管 理 辦 法	編 號	TSC900-1
制訂日期	111 年 11 月 10 日		頁 次	第 1 頁，共 4 頁

第一條 (目的)

為強化資訊安全管理，保護本公司資訊資產，免於遭受內部或外部以及來自人為、蓄意或意外之破壞，制定本資訊安全管理辦法，供相關人員共同遵循。

本辦法由資訊單位負責辦理，定期進行評估，以反映本資訊安全管理規則、相關法令規範、資訊技術環境及業務之最新狀況，確保資訊安全之實務作業確實遵守資訊安全政策，且確保資訊安全實務運作之可行性及有效性。

為落實相關的資訊安全管理，執行作業以書面或電子方式告知公司員工及提供資訊服務之廠商共同遵行。

第二條 (適用範圍)

本資訊安全管理辦法適用範圍為本公司的全體員工，對於資訊系統的產生、修改、消滅與使用上應遵循的安全規範，除特定作業之另行頒佈不適用聲明外，相關資訊安全規範及程序的產生均以此為資訊安全規則基準，將安全保護措施的規則應用於電腦系統，並使電腦系統可正常無誤的運作。

第三條(帳號管理)

1. 資訊系統均需有帳號及密碼登入管理功能，每位同仁各設有帳號及密碼。
2. 使用者須妥善保管個人帳號、密碼，若發現外洩應即更改，以確保資訊安全。
3. 同仁異動經權責主管核定後，應依其異動狀況停用或刪除其帳號及許可權。

第四條(資料存取)

1. 系統資料庫由資料庫管理者依使用者訂定不同權限，無權限者不得存取資料庫內容。
2. 系統應依資料之重要性設定安全機制，並應可追蹤資料流及使用者操作記錄。
3. 系統資料儲存異常時，應有自動警報或回復功能。
4. 資料依重要性區分，設定不同的保存或銷毀期限，除另有規定外，保存期限至少五年以上。
5. 使用單位經由系統所取得之機密性資料均應嚴加管制，限制傳閱、影印、複製、攝影、轉出或以其他方式記錄。
6. 系統資料轉出應經權責主管核定後始得辦理

第五條 (網路安全管理)

1. 網路應安裝監控系統，監控通訊線路、通訊協定、資料流量、資料內容及使用物件，由管理部門指定專人辦理，開放外部廠商維護作業時，應明定其應遵守之資訊安全規定、標準、程序及應負之責任。
2. 重要伺服器均應裝置於公司受到保護的網路內，內、外網路須安裝安全防護設備(防火牆)區隔，並依業務所需設定安全存取權限。

富育榮網股份有限公司

制訂部門	管 理 部	資 訊 安 全 管 理 辦 法	編 號	TSC900-1
制訂日期	111 年 11 月 10 日		頁 次	第 2 頁，共 4 頁

3. 各單位利用網際網路及全球資訊網公布及流通資訊，應評估資料安全等級，機密性、敏感性及未經當事人或公司同意之隱私，機密資料及文件，不得上網公布。
4. 經由公司電腦傳輸機密資料時，應採取資料加密機制。
5. 防火牆系統軟體，應定期更新版本，有關網路安全之事項或議題將不定期公告。

第六條（電子郵件安全管理）

1. 本公司之網路使用者禁止以電子郵件騷擾他人、發送匿名郵件、偽造他人名義發送郵件或惡意發送大量不當郵件。
2. 郵件使用者不應開啟不明來源寄件者或信件標題異常之電子郵件，不開啟用途不明之附件，不開啟廣告信或垃圾信件，不點選電子郵件內容中不明連結。
3. 電子郵件寄件請重複檢查收件者是否正確，避免誤寄敏感或機密資訊給不適當的收件者。
4. 電子郵件寄發時，應在信件中均附上免責聲明與公司給予之個人訊息。。

第七條（備份作業管理）

1. 為確保公司資訊系統之資料完整與正確，應設有三層備份資料保護機制，確保災害發生時，能根據不同等級的損害進行資訊資料的重建工作。
 - (1) 本機資料備份：存放於運行中的主機上。
 - (2) 異機資料備份：存放於同機房的其他主機上。
 - (3) 異地資料備份：存放於 NAS 伺服器。
2. 公司全體員工使用之個人電腦，應每季備份至 NAS 伺服器的個人資料夾。
3. 備份軟體須確保備份資料的完整性及安全性。
4. 備份以 NAS 伺服器為主，隨身硬碟為輔，並須存放於隔熱防火、防潮整潔之場所，且應與主機異地安全保存。

第八條（資訊系統可用性管理）

1. 監控機制
 - (1) 需設有監控平台，可隨時監看當下系統妥善狀態。
 - (2) 每月定期提供系統可用性報表。
2. 異地備援
 - (1) 應訂定異地備援計劃。
 - (2) 備援地點不可與運作中的機房為同一棟大樓，且須具備運行系統服務的硬體設備。
3. 災害復原
 - (1) 應訂定災害復原計劃。
 - (2) 資訊系統災害復原需定期演練，過程需有文件和紀錄備查。

富育榮網股份有限公司

制訂部門	管 理 部	資 訊 安 全 管 理 辦 法	編 號	TSC900-1
制訂日期	111 年 11 月 10 日		頁 次	第 3 頁，共 4 頁

第九條 (病毒防治)

1. 公司所有伺服器主機、個人電腦、筆記型電腦均應安裝規定之防毒軟體，掃毒紀錄應由專人檢視，並採取必要之措施；所有伺服器亦應 1 年執行掃毒作業，並將紀錄留存備查，以防制及偵測電腦病毒與惡意軟體等的侵入。
2. 對來路不明及內容不確定的資訊媒體，應在使用前詳加檢查是否感染電腦病毒。
3. 定期將必要的資料及軟體予以備份。
4. 電腦設備如遭病毒感染，應立即離線(拔除網路線連結)，並通知管理部門處理，直到確認病毒已消除後，方可重新連線。

第十條 (資訊安全事件通報處理)

1. 資訊安全事件通報，各單位人員都有責任，以便權責單位迅速有效處理資訊安全事件。
2. 資訊安全事件通報，含括電腦當機及中斷服務、業務資料不完整或資料不正確導致的作業錯誤、及機密性資料外洩..等。
3. 應以審慎及正式的行政程序，處理資訊安全及電腦當機事件。
4. 以最短的時間內，回復正常作業的系統及安全控制系統的完整性及正確性。
5. 回報最高權責單位主管報告緊急處理情形，並對事件探討分析，針對原因進行檢討改正。。

第十一條(系統開發維護及委外管理)

1. 停電：若停電時間預計會超過 10 分鐘時，應準備進行所有電腦伺服器、網路設備關機作業，恢復供電後，不可立即開機，須等待一段時間(上班時間五分鐘，非上班時間二十分鐘)應立即檢查所有硬體設備運作正常。
2. 空調故障：若發現空調設備停止運轉導致機房溫溼度超過規定範圍，應連絡廠商前來修護。
3. 天然災害：如因(落雷)颱風、水災、火警、地震等人為不可抗拒所造成之災害，應於災害發生後檢視機房設備、設施受損情形，儘速復原。
4. 其他：因系統、網路或機件發生異常現象，經檢查確認必須緊急通知維護合約廠商進行處理。

第十二條(個人資料保護)

1. 為避免洩漏個人資料，傳送包含個人資料之電子郵件，資料檔應加密碼保護，密碼需另外通知對方不可使用相同郵件告知密碼。
2. 處理個人資料之資訊設備，需設置使用者帳號及密碼，如需離開工作崗位時應登出帳號或螢幕保護鎖定。
3. 為避免個人資料被竊取、竄改，儲存個人資料之資訊設備應放置於設有門禁控管之實體安全區域，網路通訊需設置防火牆及防毒軟體，避免有心人士或非授權人員存取。
4. 儲存個人資料之電腦或設備如需報廢或轉移他用時，資訊單位應確實刪除該設備所儲

富育榮網股份有限公司

制訂部門	管 理 部	資 訊 安 全 管 理 辦 法	編 號	TSC900-1
制訂日期	111 年 11 月 10 日		頁 次	第 4 頁，共 4 頁

存之個人資料檔案。

5. 處理個人資料檔案人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員應重置相關系統密碼及使用者帳號識別。
6. 為避免資料毀損、滅失，儲存個人資料之電腦主機應建立備援機制，以確保資料無法讀取及回復。

第十三條(修訂記錄)

1. 管理部門應制定系統使用規範，並防止內、外非相關人員取得機密資訊或影響系統正常運作；同仁不得利用系統進行非正常或未經許可之作業，以獲取不當之資訊或利益。
2. 同仁應遵守公司資訊安全政策之相關規定，違者按情節輕重依「員工工作守則-獎懲辦法」相關規定予以處分。
3. 同仁應遵守業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資訊機密，或為不當之使用，違者按情節輕重依「員工工作守則-獎懲辦法」相關規定予以處分，必要時並得追究相關法律責任。

第十四條(修訂記錄)

本作業程序制訂於民國 111 年 11 月 10 日。