國揚實業股份有限公司

電腦資訊及資訊安全管理辦法

民國八十六年一月一日訂定施行。
民國九十八年十二月十六日第一次修正施行。
民國一一二年十二月十八日第二次修正施行。

第一條　資訊部與使用者部門之權責劃分

一、本公司資訊部之權責及職責主要為電腦化之前置準備及電腦週邊相關硬體之維護。
二、使用單位從事應用系統資料輸入、更正及報表之輸出。

第二條　資訊部之功能及權責之劃分

一、本公司資訊部負責系統維護及備份。
二、自行開發系統之程式撰寫或委由外部軟體公司設計、購置、租用等套裝軟體。

第三條　系統開發及程式修改控制

一、系統開發或購置套裝軟體時，應有獨立或可控制之測試環境。
二、系統委外開發或購置套裝軟體時，應由使用單位提出需求，並請資訊部會同參與遴選。
三、採購之套裝軟體使用者需對使用程序加以測試，經測試後選擇合適之軟體。
四、軟體公司之選擇應考慮其可靠性、財務狀況及其服務之項目。
五、程式修改之申請，應經使用單位主管核准後，由單位主管指定專人與軟體公司溝通。
六、程式修改及測試完畢應由使用單位驗收並留下記錄。
七、程式之緊急修護應由資訊部記錄並呈主管覆核。

第四條　系統文書之控制

於採購應用軟體時，應注意使用版權、範圍及年限。

內部文件請勿外流

第五條　程式資料存取之控制

一、資料之存取：

(一)資料之存取權限由電腦程式或系統控制，應符合內部控制規章處理。

(二)資訊人員不得存取正式上線之應用系統資料。

(三)程式之修改應經主管核准後始可進行修改。資訊部複查歸檔備查。

(四)重點資料應每日備份，一份留在機房備用，一份於其他地點異地存放。

二、資料輸入方式：

資料輸入方式可區分為個別輸入，批次輸入二種：

(一)批次輸入時利用檔案轉換，涉及到整批異動資料庫，由資訊部負責且事先預作資料備份及輸入之資料檢核，並列印清單核對。

(二)個人輸入資料，須由程式作資料檢核，並須顯示錯誤訊息及處理方法。

三、線上查詢：

查詢程式應與異動程式分開處理以避免資料遭異動，且線上查詢應考慮安全控制，非相關部門人員不得任意查詢其他部門資料。

四、資料異動：

如遇有因系統問題或操作不當，導致資料錯誤，須直接異動資料庫時，須經部門主管核准後方可異動。

五、公司人員因業務需要使用電腦作業時，公司會自動授予處理權限，惟使用者首次使用系統，需更改使用者密碼。

六、使用者若有其他權限項目之使用需求，最少須經部門主管核可，方得使用。

七、人員離職時，應知會資訊部停用使用者代號。

八、使用者之密碼應限制其最低字元含數英大小寫特殊符號等，並定期更改密碼。

九、供應商之使用代號於軟硬體維護完成後應立即刪除。

十、資訊部應定時檢測系統日誌供系統操作員記載系統作業之情況。

內部文件請勿外流

十一、作業系統應備置 Audit Log 以記錄使用者使用系統之情形，並由系統管理員定期覆核及追蹤。

第六條　資料輸出、輸入之控制

一、原始輸入之單據或系統產生之單據應依日期序號編列。
二、資料異動
資料登錄完成後，資料需更正時敘明原因，經單位主管核准後始可為之。
三、具機密性之報表，單位主管應指定專人印製及保管。
四、應定期列異動明細，以供核對及調整原始輸入憑證並呈主管審核；若有例外或異常交易時，應由主管指定專人負責處理。
五、原始憑證及輸出資料經審核後，經由專人按規定保存。

第七條　資料處理之控制

一、系統應檢核重要資料是否序號排列。
二、應由專人定期列印報表，覆核所有為系統接受及系統內部自動產生之交易的完整性及正確性，並覆核會計期間歸屬是否適當。

第八條　檔案及設備之安全

一、所有檔案資料應定期做一次完整備份。
二、每次定期備份後，應檢視其備份狀況。
三、異地備份地點，應遠離主機房之其他建築物中。
四、備份儲存媒體之借調應填具「檔案借閱申請表」（CE01-F03）呈使用單位主管核准後始得調借。
五、電腦主機應連接不斷電系統(UPS)，並設置消防設備、穩壓設備及防範水災或其他災害之設施。
六、主機房應設置獨立之空調設備以維持機房溫度之適當性。
七、資訊部未經授權人員不得任意進出。
八、PC 及 PC 網路
(一)應適當防止未經授權之存取並使用 PC 硬碟，網路伺服器或資料儲存媒體。
(二)應隨時自動偵測病毒。

內部文件請勿外流

(三)應定期更新偵測病毒軟體之版本，並訓練所有人員使用偵測病毒軟體偵測外部周邊設備之病毒。

第九條　硬體及系統軟體之購置、使用及維護

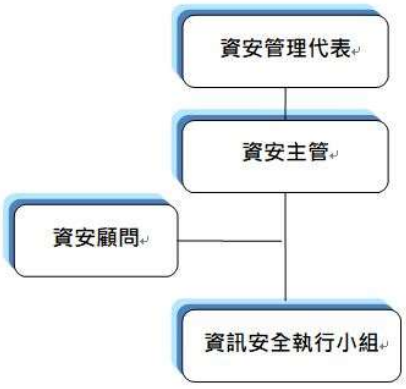
一、硬體之購置、保管依〔財產物品管理辦法〕之程序辦理。
二、系統軟體之購置應經使用單位測試後驗收。
三、軟硬體之維護應與供應廠商或相關單位簽訂定期維護合約。
四、應用系統廠商維護時應填寫維護記錄。

第十條　系統復原計劃及測試程序

本公司之系統復原計劃及測試程序依，「系統備份及復原計劃書」（CE01-F05）之規定辦理。

第十一條　資通安全管理

一、資通安全組織架構：



二、資通安全組織職掌：
(一)資安管理代表：總經理或部門主管，掌管資訊安全發展方向與策略。
(二)資安主管：規畫設計資訊安全軟硬體系統，訂定資訊安全管理辦法。
(三)資安顧問：提供資訊安全相關問題諮詢，以提高資訊安全系統可靠性。
(四)資訊安全執行小組：資訊安全維護及教育訓練。
三、範圍：
本公司之電腦登錄、軟體管理；各專案之土地開發資料、

內部資料外流

設計規劃方案圖說、工程設計圖說、工程預算、施工規範；業務之行銷策略、預算、客戶資料；財務之資金、損益預估、專案投資分析表；公司員工及股東資料等之管理。

四、資安資料之分級：

各部門應就部門特性編制資料安全層級，並決定開放權限，請資訊部門協助設定控管機制，以便合理確保公司機密性資料之安全。

五、資安資料之管理原則：

依各部門之分級並區分不同類別，擬定管理方式：

(一)人員之管理：各級成員應簽署「遵循公司個人電腦軟體使用政策聲明書」(CE01-F04)，以確保公司權益，避免公司被控侵權之行為。

(二)文件之管理：由部門核實控管部門內持有之機密文件；部門間之調閱應依規定簽准，並切結不得外漏；外部機構除業務上聯繫需要外，一律不准將文件影印、攝影、抄錄、攜出或以電子郵件方式傳送，違反規定者，一律從嚴處置。

(三)網路資訊安全：

1. 與外界連線端口，配置防火牆，阻擋駭客病毒入侵。
2. 員工由遠端登入使用公司系統資源，必須使用公司配發電腦，並透過 VPN 連線方可使用。
3. 無線網路須提供不同網段，以阻止外部人員侵入公司系統。

(四)病毒防護管理：

1. 伺服器與使用者端均安裝防毒軟體，並且需自動更新以阻擋最新型病毒侵犯。
2. 建立垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者電腦。

(五)電腦安全：

1. 公司員工一律使用公司提供電腦設備，並由公司網域管控，禁止使用非公司設備登入網域系統。
2. 公司電腦一律使用正版軟體，除合法外，並可更新問題，以提升安全性。

(六)系統存取控制：

內部文件 請勿外流

1. 同仁對各應用系統使用，需經過主管核准後，各系統管控帳號人員方得授權使用。
2. 網域系統密碼需有適當強度，必須八碼以上並含數字中英文大小寫及特殊符號四選三。
3. 員工離職必須立即停用帳號，及收回原來配發之電腦設備。

(七)系統永續：

1. 為確保系統安全度，每年須與相關資安顧問或合約廠商續約，以保持最新安全防護及諮詢。
2. 建立備份機制，並做異地備份。
3. 每年評估及模擬災害復原演練。
4. 汰舊過久設備，以避免零件故障而延誤公司營運，同時也須注意汰換廠商不再支援韌體更新之設備或系統版本。

(八)資安宣導與教育訓練：

1. 定期宣導各種詐騙、病毒等資訊。
2. 不定期執行釣魚等方式，以提高員工警覺性。

(九)即時通訊：公司網站除業務上需求外，一律不准從事與業務無關之上網事宜，本項即時通訊管理將以“機制管理”方式監控，以不定時調閱查核控管之。

六、控管之解除：

本公司之資訊業經於公開資訊網站發佈重大訊息者,或業經公司發言人對外發佈訊息者，視為解禁不再管制。

第十二條　本公司應依「臺灣證券交易所股份有限公司對有價證券上市公司及境外指數股票型基金上市之境外基金機構資訊申報作業辦法」之規定，向證券交易所申報之定期公開資訊及不定期公開資訊，其申報之期限，依該辦法之規定，於時限內，以網際網路連線方式向證券交易所申報。

第十三條　公司以網際網路連線申報作業流程

一、各相關承辦單位，編製申報文字檔。

二、定期公告以金管會規定公告之格式,依〔核決權限表〕呈核，不定期公告需呈董事長核准後，方可以網際網路連線申報。

內部文件請勿外流

三、申報完成後，須上公開資訊觀測站，印出申報結果，連同簽呈歸檔。

第十四條　本辦法由管理處訂定，經董事長核准後施行，修正時亦同。

內部文件 請勿外流