本公司因應資訊安全之管理及稽查，擬定資訊安全規範並訂有運作管理計畫(參閱後附潤弘精密工程事業股份有限公司資訊安全規範,內含實施辦法及施行細則、運作計畫管理及罰則等)，以利網路資訊安全之管理及稽核標準化作業。

另考量資安險仍是新興險種，涉及資安等級檢測機構、理賠鑑識機構及不理賠條件等相關配套，因此尚在進行資安險的評估，本公司已訂定資訊安全規範，後續目標則是持續強化資安防護與建立聯防機制，尤其在培訓優質資安人才，提升專業職能及訂定相關培訓計畫等，集團資訊處組織職掌列示如下:

■ **管理組執掌**

(1)主機及伺服器的管理和維護

(2)個人電腦及周邊的管理和維護

(3)各關係企業用戶支援與問題解決

(4)企業集團網路之架設、維護和管理

(5)電子郵件的管理及應用

(6)遠端及網際網路連線的管理

(7)建議使用單位可行方案並執行採構

(8)廠商選擇、詢價管理、合約管理

(9)新技術之研發與導入

■ **系統組執掌**

(1)使用單位的需求分析及建議

(2)系統分析及設計

(3)應用系統開發與維護

(4)協助執行教育訓練

(5)資訊應用的安全管理與密碼管理

(6)資訊開放的設計與安全控制

(7)資訊異常的處理

(8)資料庫的管理與維護

(9)企業資訊整合的分析與開發

■ **教育訓練執掌**

(1)電腦相關課程的安排、與相關單位的協調溝通

(2)電腦課程場地、講義、相關軟體、講師的安排

(3)課程後問卷的回收統計

(4)課程後的測驗安排、閱卷、統計分析

潤弘精密工程事業股份有限公司資訊安全規範

中華民國九十七年二月一日

一、資訊安全規範之目的：

(一)爲確保本公司資訊資料、系統、設備及網路通訊安全，有效降低因人爲疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資訊安全管理方向。

(二)確保本公司業務資訊之機密性、完整性與可用性。

1. 機密性：確保被授權之人員才可使用資訊。
2. 完整性：確保使用之資訊正確無誤、未遭竄改。
3. 可用性：確保被授權之人員能取得所需資訊。

二、資訊安全規範管轄內容：

(一) 本公司各項資訊安全管理規範必須遵守政府相關法規(如：刑法、國家機密保護法、營業秘密法、專利法、商標法、著作權法、電腦處理個人資料保護法等)之規定。

(二) 維護資訊硬體設施及軟體之管理機制，以統籌分配、運用公司資源。

(三) 明確規範資訊系統及網路服務之使用權限，防止未經授權之存取動作。

(四) 訂定資訊作業安全內部查核計畫，不定期檢視本公司人員個人電腦使用情形。

(五) 研擬資訊作業安全災變回復程序，確保公司業務持續運作。

(六) 公司所有人員負有維持資訊安全之責任，且應遵守相關之資訊安全管理規定。

三、資訊安全規範之評估：

資訊安全規範應定期進行評估，以反映資訊安全管理規章、法令、技術及本公司業務之最新狀況，並確保本公司資訊安全實務作業的可行性及有效性。

四、資訊安全權責分工：

(一) 資訊安全規範、計畫及技術之研議、建置及評估等事項，由資訊單位負責辦理。

李志宏 970214

(二) 個人端資料及資訊系統之使用管理及安全保護等事項，由使用者個人負責。

(三) 資訊機密維護及查核使用管理事項，由資訊單位會同相關單位負責辦理。

五、資訊安全規範實施辦法：

(一) 管理端資訊安全規範施行細則：

1. 實體及環境安全管理：

(1). 資訊設備須置於進出人員可受管制之室內，並禁止非必要人員操作。

(2). 應考量天然災害等因素所造成之設備損害可能性，使用中與庫存之設備均應置於穩固之平面，避免直接置於地面或窗邊；電力不穩定之場所應設有防突波或電力穩壓設備；工務所應設有防止雷擊之相關設施。

2. 資訊資產安全管理：

(1). 爲防斷電時造成系統毀損或資料流失，主機房須配置不斷電系統因應斷電時有足夠時間做存檔與正常關機。

(2). 網路主機須設置防火牆。

3. 系統存取控制管理：

(1). 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過六個月爲原則。

(2). 建立資訊安全查核制度，進行資訊安全查核作業。

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

(4). 訂定系統存取及授權規定，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。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。

(5). 人員職務調整及調動，應依系統存取授權規定，於異動生效時依實際狀況調整其權限。

(6). 未滿三個月之新進人員與約聘人員，應適度開放其系統存取權限。

李志宏 97.02.14

4. 系統發展及維護安全管理：

(1). 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；系統之開發、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). 對廠商之軟硬體系統建置及維護人員，應規範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。如基於實際作業需要，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). 委託廠商建置及維護重要之軟硬體設施，應在公司相關人員監督及陪同下始得為之。

5. 電腦系統安全管理：

(1). 辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。

(2). 採購資訊軟硬體設施，應視資訊安全規範及需求，研提資訊安全需求，並列入採購規格。

(3). 依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。

(4). 對各種系統變更作業，應建立控管制度，並建立紀錄，以備查考。

6. 人員管理及資訊安全教育訓練：

(1). 各部門應針對管理、業務及資訊等不同工作類別之需求，依需要性適時辦理資訊安全教育訓練或宣導，建立員工資訊安全認知，提升資訊安全水準。

(2). 提供新進人員資訊安全說明文件，各部門視需要再施以部門所屬之資訊安全教育宣導。

(3). 加強資訊安全管理人力之培訓，提升資訊安全管理能力。

(4). 資訊安全人力或經驗如有不足，得經核可後洽請學者專家或專業機構、廠商等提供技術、設備或顧問諮詢服務。

李志豪 PM0214

(5). 負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立制衡機制、人力備援制度。

(6). 員工對於資訊安全認知尚有不足，致行爲有造成資安風險之虞時，應先行適當限制、調整其適用權限。

(7). 各部門主管及各級人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行爲。

7. 網路安全管理：

(1). 利用公眾網路傳送資訊或進行作業，應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求，並針對資料傳輸、撥接線路、網路線路與設備、接外連接介面及路由器等事項，研擬妥適的安全控管措施。

(2). 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。

(3). 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與部門內部網路之資料傳輸與資源存取。

(二) 使用者端資訊安全規範施行細則：

1. 實體及環境安全管理：

(1). 颱風經發佈警報後，工務所人員應遵守「工地電腦、網路及周邊設備應注意事項」，積極辦理並登記於防颱檢查表。

(2). 非資訊單位人員或維修人員，不得自行拆卸電腦機殼及更換內部零組件。

2. 資訊資產安全管理：

(1). 資訊設備移動、調撥、儲存時，應將屬該設備之週邊器材一併妥適處理以免遺毀。

(2). 電腦設備須裝置防毒軟體，並時常進行病毒碼與引擎之更新，且隨時開啓於即時掃瞄狀態；對所收電子郵件之附加檔案、外部儲存媒體、網路下載之檔案等，更須先經過掃瞄確

李志豪 110.2.14

定安全後始得開啓。

(3). 文件檔案存檔時須養成加密保護與備份習慣，若檔案需提供網路共享則必須以加密等方式加強控管，於喪失共享必要性後盡快解除共享狀態。

(4). 不得使用未經管制之外部儲存媒體(光碟、軟硬碟、隨身碟、MP3 隨身聽、記憶卡等)。具備外部儲存媒體存取能力之個人電腦，須受管理人員管制。

(5). 不得任意下載、複製或使用非公務需要、非經合法授權或有安全性疑慮之軟體程式。

3. 系統存取控制管理：

私有資訊設備非經許可，不得介接公司系統、網路、設備，或攜入工作環境作業。確有需要且經核可者，應確實遵守各項資訊安全相關規定，並對其加強查核與檢測。

4. 電腦系統安全管理：

採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。未受專人管制與授權之電腦，禁止使用 USB、IEEE1394 等連接埠介接存取資料。

5. 網路安全管理：

(1). 各部門利用網路公布及流通資訊，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等，不得任意散佈於網路環境中。

(2). 機密性資料及文件，不得以電子郵件、其他電子方式或經由公眾網路空間傳送散佈。

(3). 機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各部門應視需要以適當的加密或電子簽章等安全技術處理。

(4). 部門業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，應採用加密或電子簽章等安全技術處理。

(5). 對網際網路之瀏覽存取具必要者，由該部門主管核可後發給通行帳號密碼供使用者個人使用。嚴禁安裝使用各種 P2P 軟

李志豪 990219

體(FOXY、BT、eMule.....等)。非經許可不得使用即時通訊軟體。

(三) 業務永續運作計畫管理：

1. 爲因應各種人爲及天然災害造成業務運作受影響，須定期作備份處理。
2. 爲使正常業務運作受資安事件之影響降至最低，各單位應於資訊系統失常時具有一定程度之作業能力與備援方案。
3. 各部門單位、工地應由主管指派適當人選作爲資訊單位連繫窗口，並由資訊單位視情況施以教育訓練，以利資訊相關作業遂行。
4. 各單位在發生資訊安全事件時，應立即向權責主管單位或資訊單位系統管理人員通報，並於必要時聯繫檢警調單位協助偵查。

(四) 其他資訊安全管理事項：

1. 本規範應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。
2. 本資訊安全規範奉核可後實施，修正時亦同。

六、罰則：

怠忽資訊安全作業或違反相關法令致使公司蒙受損失時，視情節輕重及損害程度，依「潤泰企業集團・員工行爲準則」及「潤弘精密工程事業股份有限公司工作規則」等相關規定提報懲處並依法請求損害賠償。

李志豪 990214