宇環科技股份有限公司

YEU HWAN TECHNOLOGY CO.,LTD.

資通安全辦法

文件編號：WI-CM-002
制訂日期：92 / 07 / 24
版　　本： A

管制編號：

宇環科技股份有限公司

YEU HWAN TECHNOLOGY CO.,LTD.

資通安全辦法	文件編號		WI-CM-002	
	版 次	A1	頁 次	1
	制訂日期		92 / 07 / 24	

1.目的：

資訊安全事件是十分昂貴的成本，包括喪失企業重要的資源，喪失客戶及交易夥伴的信心，舞弊及系統的無法使用，均是公司無法忍受的；為確保公司資料之安全性，建立、監督、稽核整體資訊安全為首要要務。

2.範圍：

舉凡公司管理軟、硬體、作業系統及其使用者，應用於工作場合中均屬之。

3.內容：

3.1 安全組織：

3.1.1 應指定專責人員，負責推動、協調及督導下列資訊安全管理事項：

a.資訊安全政策之核定、核轉、宣導及督導。

b.資訊安全責任之分配及協調。

c.資訊資產保護事項之監督。

d.資訊安全事件之檢討及監督，應每週審核安全事件報告。

e.定期之 IT 及 ISMS 之安全稽核計劃制定、資訊風險評估及不定期之資訊安全測試。

f.其他資訊安全事項之核定。

3.1.2 應指定專責人員，負責電腦病毒威脅之管理事項：

a.研議、應用各種安全防毒之軟體，以確保本公司之資訊安全。

b.應提供防毒技術之指導予相關技術支援部門，以協助使用者。

c.整體防毒安全措施之協調研議及支援。

d.建立、維護病毒及因病毒所造成資訊安全風險事件之資料庫。

3.1.3 應指定專責人員，負責電腦系統安全之管理事項：

a.應用適當工具或方法以確保各系統有恰當之存取控制。

b.確保各資料貯存系統對可用性、機密性及資料完整性有適當之保護措施。

c.整體系統安全措施之協調研議及支援。

d.應提供系統安全技術之指導予相關技術支援部門，以協助使用者保護資料之安全。

e.建立、維護新系統安全及因系統所造成之資訊安全風險事件之資料庫。

3.1.4 應指定專責人員，負責電腦通訊安全之管理事項：

a.應用適當工具或方法以確保各通訊網路系統有恰當之存取控制。

b.整體通訊安全措施之協調研議及支援。

c.確保各外接網路系統及數據機有完整之資料登錄，並有適當之保護措施。

d.整體網路安全系統措施之協調研議及支援。

e.應提供網路安全系統技術之指導予相關技術支援部門，以協助使用者保護網路資料之安全。

f.建立、維護新網路系統安全及因網路系統所造成之資訊安全風險事件之資料庫。

3.1.5 應指定專責人員，負責管制資訊安全區域的安全事項：

a. 建立並定義管制資訊安全區域。

b. 授權使用者出入管制區域。

c. 確認管制區域有適當的控管機制。

d. 定期檢核管制區域授權使用者的權限是否適當。

3.2 第三方網路存取：

3.2.1 第三者存取本公司之資訊設施，應於實際存取作業前，提出正式申請，經審查通過後，簽訂正式的契約或協定，俟契約或約定生效後始能提供存取服務。

3.2.2 契約之審查應包含技術與風險評估，並需經本公司專責人員同意後，方可實施。

3.2.3 契約應有期限，期滿後若需繼續使用，應重新申請。

3.2.4 契約或協定內容應規定第三者須遵守之資訊安全規定、標準及必要的連線條件。

3.2.5 本公司只提供絕對必要之連線通訊協定與服務項目予契約使用者，且該等協定與服務皆不得違反或抵觸本公司相關規定。

3.2.6 本公司資訊系統與網路管理人員應與契約用戶定期核對使用者名單，以確保其正確性。

3.2.7 本公司資訊安全主管應定期檢查所有契約用戶之使用情形，若發現有違反規定或對本公司資訊安全有危害時，應先中斷連線，直至改善完畢後，方可恢復。

3.3 資訊資產之責任：

3.3.1 資訊資產目錄之建立及保護：

a. 應該建立與資訊系統有關的資訊資產目錄，訂定本公司資訊資產的項目、擁有者及安全管理等。

b. 資訊資產定義參考項目如下：

ⓐ資訊資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、軟體資產、實體資產及技術服務資產等。

ⓑ軟體資產：應用軟體、系統軟體、發展工具、公用程式及磁性媒體資料等。

ⓒ實體資產：電腦及通訊設備、及其他技術設備。

ⓓ技術服務資產：電腦及通信服務、其他技術性服務（電源及空調）。

c. 資訊資產應予以分類，並定期予以盤點及列示剩餘殘值，其中實體資產應予以貼示標籤。

3.3.2 資訊資產之管理：

a. 資訊資產之保管：

ⓐ資訊資產所有者之確認：重要資訊資產應標明所有者、種類、原廠其它資料說明、驗收、備註說明，以作為盤點及控管之依據。

ⓑ應建置統一資料庫列管資訊資產財產目錄。

ⓒ對於儲存媒體原始資料及重要產出報表應規劃設置專屬儲存空間，指派專人管理及適當備援，且其銷毀應有專人負責，必要時應有適當人員監督下進行。

ⓓ委外廠商至公司內進行系統維護時，應採取適當之安全管理，避免原始資料被竊、更動、外洩之不當情形產生。

b. 資訊資產之採購：

ⓐ採購資訊設備應依採購流程辦理。

ⓑ各分公司採購資訊設備應依採購流程辦理，分公司亦可擬定採購流程，並經提報總公司相關部門後施行。

3.4 安全事件報告之責任：

3.4.1 應建立處理資訊安全事件之作業程序，並賦予相關人員必要的責任，以便迅速有效處理資訊安全事件以期及時通報相關人員。

3.4.2 資訊安全事件之管理可區分為三大類：

a. 病毒事件之管理。

b. 資源及網路遭受空攻擊。

c. 作業疏失事件。

3.4.3 發生資訊安全事件之反應與處理作業程序，應納入下列事項：

a. 電腦當機及中斷服務。

b. 業務資料不完整，或資料不正確導致的作業錯誤。

c. 機密性資料遭侵犯。

3.4.4 除正常的應變計劃外（如：系統及服務之回復作業），資訊安全事件之處理程序，尚應納入下列事項：

a. 導致資訊安全事件原因之分析。

b. 防止類似事件再發生之補救措施的規劃及執行。

c. 電腦稽核軌跡及相關證據之蒐集。

d. 與使用者及其他受影響的人員，或是負責系統回復的人員進行溝通及瞭解。

3.4.5 電腦稽核軌跡及相關的證據，應以適當的方法保護，以利下列管理作業：

a. 作為研析問題之依據。

b. 作為研析是否違反契約或是違反資訊安全規定的證據。

c. 作為與軟體及硬體之供應商，協商如何補償之依據。

3.4.6 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。作業程序應該包括下列事項：

a. 應在最短的時間內，確認已回復正常作業的系統及安全控制系統，是否完整及正確。

b. 應向管理階層報告緊急處理情形，並對資訊安全事件詳加檢討評估，以找出原因及檢討改正。

c. 應限定只有被授權的人員，才可使用已回復正常作業的系統及資料。

d. 緊急處理的各項行動，應予詳細記載，以備日後查考。

3.5 電腦與網路之管理：

3.5.1 作業流程需提供適當的控制：

a. 相關作業流程應予設置並能達成適當控制之目的。

b. 所有的連接使用者及電腦的功能皆應依照控制程序執行，相關控制應包括下列項目：

ⓐ網路服務間的安全介面。

ⓑ遠端使用者及設備的強力認鑑機制。

ⓒ使用者 IT 服務存取的控制。

c. 服務的限制：所有員工的服務皆僅止於經授權的存取。

d. 使用者的認鑑：遠端使用者若經由公眾或是非正式組織連接網路時，需經由至少二層的認鑑。

e. 遠端診斷埠口之存取需經安全控管程序。

f. 使用者連接之效能需加以控制，使能支援正式應用系統之存取政策需求。

g. IT 服務之存取必須通過安全登入控制程序。

h. 所有的員工必需使用螢幕密碼保護程式當 PC 或終端諼備於持續連線或存取應用系統狀態而暫時須離開且無法加以注意時。

3.5.2 對於作業過程中所遇到之事故，應具正式之報告程序，且能適時通知專責人員，其流程需為有效。

a. 網路上各電腦之活動得以個別追蹤，並存至專屬記錄。

3.5.3 應予制訂相關網管控制變更之流程，其流程需經專責人員授權，且其流程需為有效。

a. 所有計劃連接公司網路的外部存取連接，必需事先經過專責人員的認可及複核。

3.5.4 應確認所有的電腦設備皆經病毒防範之設置，且於發現病毒時，其確認及處理程序應具時效性，下列控制程序應予以確認：

a. 防毒軟體已妥善安裝於每部個人電腦及檔案伺服器。

b. 至少每月執行乙次確認病毒之更新。

c. 應予設定自動偵測病毒之警示。

d. 所安裝之防毒軟體需具偵測未知病毒之警示。

e. 任何來自於外部的（包括原始廠商或網際網路）軟體或資料之取得，皆應先視為可疑且不得安裝、執行、使用或以其他方式的形成，直至通過所內標準防毒偵測軟體掃瞄後，始得進行。

3.5.5 所設置之網管控制程序對於網路上的資料需提供合理保證其安全性，例如：應考量其機密性、完整性及有效性，網路安全責任的指派需為適當，包括向專責人員之報告程序。

a. 所有的員工皆應知悉不得連接非經公司授權認可之網站。

b. 數據機建置的用途限於傳真及語音的使用，任何數據機的撥入需求皆應獲得專責人員的同意。

c. 所有的成員不得在違反國家或國際法律之情況下揭露或使用電腦上之個人資料，同樣的，所有的成員皆需知悉使用及管理所屬資料時係基於法律下之責任。

3.5.6 所設置之網管控制程序對於 E-MAIL 資料在傳遞的過程中需為安全的，並提供合理的保證，免於資料遺失、遭到篡改、誤用或敗露等情形的發生。

a. 所有的使用者及 IT 成員必需認知使用 E-MAIL 傳遞所可能產生與存在的風險，例如：機密性、完整性以及法律方面等之考量。

4. 參考文件：

4.1 災害復原計劃作業辦法　　WI-CM-001