標題	資訊安全管理準則

1. 資訊安全目標：
   建立安全及可信賴之電腦化作業環境，確保本公司電腦資料、系統、設備及網路安全，以保障股東權益及公司業務永續運作。
2. 資訊安全管理作業：
   2.1 人員安全管理及教育訓練
   (1)在系統使用者尚未完成正式授權程序前，資訊部門不得對其提供系統存取服務。
   (2)應以書面、電子或其他方式賦予使用者系統存取權限。
   (3)使用者不得將個人登入身份識別碼與密碼交付他人使用，亦不得以任何方法竊取他人的登入身份識別碼與密碼。
   (4)當有跡象足以顯示使用者密碼可能遭破解時，應立即更改密碼。
   (5)使用者調整職務及離（休）職時，應立即取銷其系統存取權限。
   (6)資訊部門應定期對員工辦理資訊安全相關教育訓練課程。
   (7)資訊部門因應資安狀況，不定期公告資訊安全相關信息。
   2.2 電腦主機安全管理
   (1)各項伺服器及電腦主機均應指定專人管理，非經核准不得任意使用、拆卸及更動零組件。
   (2)各類伺服器及電腦主機皆應設定密碼。
   (3)伺服器及主要電腦主機之作業環境如溫度、溼度及電源供應之品質等，應隨時監測，並採取必要的防護補救措施。
   (4)應防範電腦病毒及惡意軟體之攻擊。
      a. 禁止使用未經授權之軟體，並遵守智慧財產權相關規定。
      b. 嚴禁使用或開啟來路不明及內容不確定之軟體、媒體或電子郵件。
      c. 使用儲存媒體時，應在使用前詳加檢查是否感染電腦病毒。
      e. 應建置防火牆及防毒軟體以區隔內部網路與網際網路間之連結，阻絕電腦病毒及惡意攻擊性軟體之非法入侵或非法存取資料。
      f. 應定期修補作業系統程式漏洞及更新電腦病毒碼與防制軟體。
   2.3 資料安全管理
   (1)應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。
   (2)應落實定期備份作業及電腦媒體異地備援之規定，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。
   (3)應依使用者所負責業務性質及職掌，賦予不同資料存取權限。
   (4)應安全管理電腦媒體與資料文件，存放至安全場所，由專人保管。
   (5)可重複使用的資料儲存媒體，不再繼續使用時，應將儲存的內容消除。
   (6)委外處理的電腦文件、軟體設計、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗的機構作為委辦對象。
   (7)應依據個人資料保護法及相關資料保密規定，促使相關人員應負資料保護責任，及遵守之作業程序，以確保個人資料安全。
   2.4 系統開發維護安全管理
   (1)新發展的資訊系統，或是現有系統功能之強化，應將安全需求納入系統功能。
   (2)系統發展之正式作業及測試作業，應分別在不同資訊環境運作及測試，以避免軟體或資料遭意竄改或不當使用。
   (3)新開發或修正更新之系統，須經查驗系統運作正確或測試結果無誤後，再予轉置正式環境執行。
   (4)應用系統使用者須設定通行密碼，並限制使用權限。
   (5)系統的最高使用權限，應經權責主管人員審慎評估後，交付系統管理人員管理。
   (6)資訊業務委外時，應於事前審慎評估可能的潛在安全風險，應與廠商簽訂資訊安全協定，將相關的安全管理責任納入契約條款。
   2.5 網路安全管理

(1)網路設備須有專人管理，隨時監測網路的狀況。
(2)連外網路須安裝安全防護措施，注意可能的漏洞。
(3)網路主機應關閉非必要的服務程式，並隨時更新程式版本。
(4)應禁止及防範網路使用者以任何儀器設備或軟體工具竊取網路上的通訊。
(5)網路系統管理人員未經權責主管人員許可，不得閱覽使用者之私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權檢查其檔案。
(6)網路硬體設備應加裝不斷電系統，以預防不正常的斷電狀況。

2.6 網路存取及遠距視訊之安全控制

(1)網路連線作業需透過路由器及防火牆設定安全防護過濾規則予以通訊。
(2)網路連線使用者應遵守相關安全規定，如有違反，依相關法規處理，並取消其網路資源存取權限。
(3)遠距視訊軟體應為有安全機制及正式版權之通訊軟體。
(4)遠距視訊使用者需遵守個人資料保護法及相關資料保密規定，避免討論機密性話題及文件。

2.7 系統與網路入侵之處理

(1)應隨時檢討網路安全措施及修正防火牆的設定，以防禦網路的入侵與攻擊。
(2)當防護網被突破時，系統應立即切斷入侵者的連接，拒絕入侵者存取動作，防止災害繼續擴大。
(3)對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並聯合相關單位追蹤入侵者。
(4)入侵者之行為若觸犯法律規定，構成犯罪事實，應立即通知檢警單位，請其處理入侵者之犯罪事實調查。

2.8 設備安全管理

(1)重要資訊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未經授權存取系統的機會。
(2)應定期檢查及評估電力供應、火災、水災、地震、灰塵、煙、化學效應、電磁幅射等可能的風險。
(3)電腦作業區應禁止抽煙及飲用食物。
(4)資訊設備電力供應設置，應符合設備規格、穩定電源及定期進行檢測。
(5)重要資訊設備應考量安置預備電源，使用不斷電系統。
(6)設備報廢應依報廢程序處理，含有儲存媒體的設備，應在報廢處理前詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體確認已經被移除。
(7)嚴禁資訊設備被不當使用，造成資訊安全漏洞，使用單位應作適當的監督管控及紀律管理。

2.9 實體環境安全管理

(1)資訊設備環境應事前規劃基礎設施，以確保設備安全及防護，依機密性，必要時可設置人員進出身分識別門禁管控。
(2)電腦機房應考量火災、水災、地震等災害的實體安全防護措施，並考量鄰近空間的可能安全威脅。
(3)危險性及易燃性的物品，應遠離電腦機房。
(4)備援作業用的設備及備援媒體，應存放在安全距離以外的地點，以免資訊電腦機房受到損害時也一併受到毀損。
(5)人員進入電腦機房應予適當的管制，並記錄進出時間；人員只有在特定的目的或是被授權情形下，才能進入電腦機房。
(6)電腦機房應安裝適當的安全偵測及防制設備等警示自動通報系統，並依各項使用說明書定期檢查，以確保機房設施安全。

2.10 業務永續運作計畫管理

(1)為因應人為及天然災害造成業務運作受影響，須確實做好各項備份工作。

(2)各單位應依業務性質研擬緊急應變計畫，使各項業務得以永續運作。
(3)緊急應變應分為緊急時段、過渡時期及回復時期之作業程序，使業務得以順利銜接不致中斷。
(4)應就緊急應變程序及作業流程，進行相關員工教育及訓練。
(5)應定期測試及更新緊急應變計畫，以確保計畫持續有效。
(6)各項業務緊急應變計畫，應指定適當的單位或人員負責。

3. 組織職掌及分工：
以常態任務編組方式設「資訊安全處理小組」，協同辦理本公司資訊安全預防及危機處理相關事項。惟為因應緊急突發安全事故或辦理安全政策評估修正時，得另委請資訊專業人員，提供資訊安全技術支援及諮詢服務。
3.1 由公司高階主管擔任「資訊安全處理小組」召集人，負責推動、協調、核定及督導資訊安全管理事項。
3.2 由公司資訊部門主管擔任「資訊安全處理小組」總幹事，並負責督導「危機處理分組」，規劃危機處理程序、查明危機事件原因、確定影響範圍及損失評估、執行緊急應變措施、辦理危機通報、執行解決辦法等有關資訊安全政策、計畫及技術規範之研議、建置及評估事項，暨資訊安全相關會議之作業事項。
3.3 由本公司資訊部副主管擔任「資訊安全處理小組」執行秘書，並負責督導「安全預防分組」，辦理蒐集資通安全資訊、訂定本公司系統安全等級、建置資通安全措施、執行資通安全監控等有關資訊機密維護及稽核使用管理事項。
3.4 由本公司資訊部同仁擔任「資訊安全處理小組」應變處理及演練測試推動組員。

4. 資訊安全事故處理：
本公司所有同仁均負資訊安全事故通報之責任，狀況發生時先通知資訊部同仁，經「資訊安全處理小組」及資訊安全顧問共同判定確為資訊安全事故，立即啟動「資訊安全緊急應變措施」，並依各項安全等級處理程序處理。

資訊安全事故等級		A	B	C	D
事故狀況		影響公共安全社會秩序及國民生命財產	資訊系統完全停頓業務無法運作	業務中斷影響系統效率	業務短暫停頓可立即修復
處理單位	資訊安全處理小組	◎	◎	◎	◎
	資訊系統維護廠商	◎	◎	◎	
	國家資通安全會報	◎			

資訊安全緊急處理作業程序應定期演練及測試。

5. 評估與修正：
本準則由本公司「資訊安全處理小組」依本公司資訊作業安全事項辦理重行評估與修正事宜，以反映相關法令、資訊技術及本公司業務發展現況，俾使本準則切實符合安全需求。

6. 訓練與宣導：
本準則公佈於公司網頁及內部網路之電子布告欄內供同仁上網查閱，資訊部門負責相關訓練與宣導課程，並利用全公司同仁資訊教育訓練時，辦理擴大宣導說明公司資訊安全政策；新進人員則於報到時依人事單位相關程序進行資訊安全教育及訓練。

7. 實施：
本準則自公告後自動生效實施，修正時亦同。