1 目的

悠遊卡股份有限公司(以下簡稱本公司)為確保資訊處理之正確性、資訊相關系統與設備及網路之安全性，特訂定本政策，以宣示管理階層支持資訊安全之決心，並利相關人員有所依循，以降低任何資訊安全事件所可能帶來之衝擊，並持續運作及改善資訊安全管理制度同時保障本公司與客戶之權益。

2 範圍

資訊安全管理制度(Information Security Management System，以下簡稱ISMS)實施範圍涵蓋本公司主要之資訊作業流程與環境，適用對象包含本公司所有內部員工(涵蓋依本公司員工任用辦法所任用之人員)、委外廠商等。

3 名詞定義

3.1 資訊安全(Information Security)

即確保資訊的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)，使資訊能安全地、正確地、適切地及可靠地運用於達成本公司經營目標之規劃、執行、管理及相關作為上。

3.2 風險(Risk)

潛在或顯現之不確定事件，將會影響組織策略、內部管制作業、財務或其它目標達成之因素者。

4 相關文件

無。

5 權責

資訊安全管理制度下之所有人員，皆應瞭解並切實遵守。

6 內容

6.1 資訊安全管理制度

6.1.1 通則

6.1.1.1 為展現貫徹資訊安全管理的決心，確保本公司資訊與資訊系統獲得適當保護，特依據 ISO 27001 資訊安全管理國際標準之要求建立、記載、實施及維護資訊安全管理制度，持續改進制度的有效性。

6.1.1.2 本節說明資訊安全管理制度之建置方式、文件系統架構、文件管制與紀錄管理程序。

6.1.2 資訊安全管理 PDCA 循環機制

本資訊安全管理制度係為確保本公司重要資訊資產之安全，藉由成立資訊安全組織，制訂標準規範及作業程序，控制潛在之威脅及漏洞，規劃風險評估、設計與建置控管機制、遵行覆核檢查及檢討改善等四大階段，持續強化資訊安全管理機能。

6.1.2.1 規劃評估(Plan)

對影響資訊資產安全之威脅、漏洞及現行控管機制進行風險評估。

6.1.2.2 設計建置(Do)

依據評估結果設計、修正及建置應有之控管機制。

6.1.2.3 覆核檢查(Check)

定期實施資訊安全查核，確保資訊安全管理之有效性；透過管理審查，落實資訊安全控管。

6.1.2.4 檢討改善(Act)

根據查核之結果，執行矯正措施，改善並執行應有之控管機制，對相關人員實施資訊安全宣導與訓練。

6.1.3 瞭解內、外部議題與利害相關團體之需求與期望

應考量並決議下列事項，以利決定資訊安全管理制度實施範圍、設計相對應管控並執行之。

6.1.3.1　來自內外部與資訊安全相關之議題

6.1.3.2　資訊安全管理體系之利害相關團體

6.1.3.3　與上述利害相關團體相關之資訊安全要求

6.1.4　組織與權責

為確保資訊安全管理制度之有效性，設置資訊安全推動委員會，以推動及維持資訊安全管理制度各類管理、執行與查核等工作之進行，其職責應依相關規定辦理。

6.1.5　文件系統

6.1.5.1　文件系統架構

(A) 第一階、政策：說明資訊安全政策與資訊安全管理制度作業原則。

(B) 第二階、規範：說明資訊安全管理制度之作業方法、流程與部門間的關係。

(C) 第三階、程序：部門層級專屬之支援性作業規定，說明之執行細節。

(D) 第四階、表單/附件：記錄各項資訊安全活動之證明，確保資訊安全作業之有效執行。

6.1.5.2　文件管制

資訊安全管理制度相關文件之管制方式，第一至四階資訊安全文件之管制、核發與變更均應依據相關規定辦理。

6.1.5.3　紀錄管制

資訊安全管理制度運作所產生之任何文件、表單及紀錄，部門應指定資訊安全紀錄保存人員，依紀錄管理程序妥善保管，訂定保存期限與核閱權限，以利追蹤制度執行狀況，維護制度有效運作。

6.2 管理階層責任

6.2.1 管理階層承諾

管理階層應確保完成下列工作，表示對資訊安全管理發展及增進的充分支持：

A. 制定資訊安全政策。

B. 確認資訊安全指標之建立。

C. 訂定資訊安全之角色與職責。

D. 宣導遵守資訊安全政策與法令規章、達成資訊安全指標及持續改善之重要性。

E. 提供資訊安全管理制度各項作業所需之資源。

F. 決定風險可接受水準。

G. 執行資訊安全管理制度之管理審查作業。

6.2.2 資源管理

6.2.2.1　提供資源

應確認並提供執行下列事項所需之資源：

(A) 建立及維護資訊安全管理制度。

(B) 確認資訊安全程序能符合營運之需求。

(C) 闡明法令規章之要求與契約之安全義務。

(D) 正確運用管制措施，確實維護資訊安全。

(E) 執行必要之審查，對結果做適當之處理與追蹤。

(F) 改善資訊安全管理制度之有效性。

6.2.2.2 教育訓練

依下列程序確認參與資訊安全管理制度作業之人員均具備工作所需之相關職能，以提昇資訊安全認知觀念與防護能力：

(A) 確立資訊安全管理制度運作相關人員必須具備之職能。

(B) 提供職能訓練，必要時得聘任可滿足職能需求的人員。

(C) 評估職能訓練與相關措施之有效性。

(D) 建立並維護教育訓練、技能、經驗與資格之相關紀錄。

6.3 資訊安全指標

資訊安全指標包含以文件說明如何量測所選擇控制措施之有效性，具體說明如何使用這些量測去評鑑控制措施及量測時機，產生可比較與可再製的結果。資訊安全指標應涵蓋機密性、完整性與可用性三個構面，與資訊安全政策聲明作適當結合。

6.4 內部稽核

資訊安全管理制度應定期進行安全稽核，以檢討控制目標、控制措施與程序是否遵循相關標準、法令規章或資訊安全需求，並依預期規劃有效執行與維持。內部稽核作業之規劃應考量稽核對象或範圍之重要性與現況，定義稽核之標準、範圍、頻率與方法，確認稽核人員之客觀與公正，並妥善保存相關紀錄。受稽核單位對於不符合事項應及時採行改善措施，並追蹤驗證其有效性。

6.5 資訊安全管理制度管理階層審查

6.5.1 通則

6.5.1.1 資訊安全推動委員會應每年至少執行一次管理審查，確保

資訊安全管理制度持續運作的適用性、適切性及有效性。

6.5.1.2 管理審查會議之決議事項，交由資訊安全推動小組及各相關單位配合執行，由資訊安全推動小組負責執行狀況之追蹤及評估。

6.5.2 審查項目

管理審查作業之項目包括下列資訊：

(A) 前次管理審查之後續追蹤。

(B) 可能影響資訊安全管理制度之內部或外部環境之改變。

(C) 資訊安全管理制度執行之回饋如：不符合事項及矯正措施、監控及量測結果、稽核結果、有效性量測指標。

(D) 來自利害相關團體之回應或要求事項。

(E) 風險評鑑結果與風險處理計畫之狀態。

(F) 其它持續改進之建議。

6.6 資訊安全管理制度之持續改進

6.6.1 持續改進

應經由資訊安全政策、安全指標、內外部資訊安全查核結果、事件監控之分析、矯正與預防措施以及管理階層審查等機制，以持續改進資訊安全管理制度之有效性。

6.6.2 矯正措施

應採取適當的控管措施，以減少資訊安全管理制度建置與運作過程中所發現之不符合事項，防止再度發生。矯正措施之作業程序如下：

A. 指出資訊安全管理制度建置與運作之不符合事項。

B. 確認不符合事項的原因。

C. 評估為防範再發生所需採行之措施。

D. 決定及實作所需之矯正措施。

E. 記錄矯正措施之執行結果。

F. 審查矯正措施之執行結果。

6.6.3 矯正措施之實行時機

6.6.3.1 資訊安全管理制度查核、主管機關或其它單位查核提出之不符合事項，由權責單位負責追蹤矯正措施以及不符合事項之改善進度。

6.6.3.2 影響本公司商譽之資訊安全事件發生，如客戶資訊外洩或違反法令等。

6.6.3.3 重大異常事件應有適當的紀錄，交由相關單位負責追蹤矯正措施及相關改善進度。

6.7 政策指導與覆核

本資訊安全政策為本公司資訊安全管理之最高指導原則，並據以制定資訊安全作業程序，本資訊安全政策必須經由資訊安全推動委員會每年至少評估一次，檢討覆核與修訂，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。

6.8 政策補遺

資訊安全政策若有未盡事宜，應依循制定之精神及資訊安全管理之原則，以確保本公司資訊資產之機密性、完整性及可用性，落實資訊安全管理。

6.9 政策宣導

應由資訊安全推動小組指定相關人員以政令宣導、教育訓練等方式，公布和傳達至所有員工，使員工能有所認知並遵循。

6.10 違反資訊安全政策之處置

本公司所有內部員工均須遵循資訊安全政策之規範，違反者須依本公司相關規定予以處分，如涉有相關刑責或法律責任者，將衡酌情節追訴其法律責任，由員工自行負責。

6.11 實施與修訂

本政策經資訊安全推動委員會審核後，提報董事會核定後公告實施，修訂時亦同。