資訊安全政策

壹、 目的

是方電訊股份有限公司（以下簡稱本公司）為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司資訊運作所需之環境與架構，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特制定此政策規範。

貳、 適用範圍

本公司依實際需要及符合相關法令要求建立資訊安全管理系統，以確保資訊之機密性、完整性及可用性。本系統適用範圍設定為本公司 IDC 機房服務、NOC 維運作業、VPN 服務、TPIX 服務 (含 TPIX 平台系統、TPIX 監控系統、TPIX 認證系統)、雲計算服務、雲端資料管理儲存服務及是方雲端自助線上平台之相關營運操作系統及範圍內之相關部門與維運管理人員，以充份掌握資訊運作及管理過程並滿足各項安全要求與期盼。

公司於建置資訊安全管理系統之初衷及系統執行之結果，均應將內外部單位對資訊安全方面之議題，包括雲端服務資訊安全及雲端個人隱私保護，及關注方對資訊安全管理系統之期盼與要求納入考量，並列入目標與成效評估範圍。這些資訊安全相關議題、期盼或要求，應列入風險評估及風險管理，以確保資訊安全管理系統能達成預期效果及持續改善。本公司於風險評鑑過程中必須要能識別風險擁有者。

本公司應於相關部門及層級建立資訊安全目標，並可與資訊安全政策對應或連結，且必須 (1)可以量測 (2)成效量測方式 (3)需訂定完成日期 (4)需有負責人員(負責單位)。

本公司之內部人員、供應商與訪客皆應遵守本政策。

本公司資訊安全政策訂定如下：

1. 有效確保重要資訊應有之機密性、完整性、可用性及適法性。
2. 資訊安全目標須與政策一致性，並須定期評估其適用性。
3. 須清楚定義資訊安全相關工作職掌及權限。
4. 資訊安全管理系統之運作，需滿足及達成內外部利害關係方之要求與期盼，包括法令及相關協議之要求。
5. 資訊安全管理之操作，須依本管理系統所訂定之各項作業規範，落實執行。
6. 當系統或程序進行變更時，不得影響既定之資訊安全承諾與協議。
7. 本公司資訊安全管理系統，理當持續改善與精進。

為能有效支持上述高階政策之展開，本公司訂定「主題特定政策」如下，以能接續相對應之控制項目或措施：

1. 進行資訊資產管理。
2. 執行人員安全管理。
3. 貫徹實體及環境安全管控，含重要區域之監控。
4. 確實執行存取控制管理。
5. 確保資訊傳輸安全。
6. 安全配置及處理使用者終端裝置。
7. 執行網路安全管控。
8. 網路作業須妥予執行監視活動。
9. 確實執行備份管理。
10. 執行金鑰管理。
11. 妥善進行資訊分類及處理。
12. 定期實施技術漏洞管理。
13. 有效執行重要資訊遮罩。
14. 執行系統開發安全管控。
15. 資訊安全事件管理。
16. 建立及執行雲服務資訊安全管理機制。

參、 名詞定義

1. 資訊資產：係指為維持本公司資訊業務正常運作之環境、硬體、軟體、資料及人員。

肆、 權責

1. 本公司的管理階層建立及審查此政策。
2. 資訊安全管理者透過適當的標準和程序以實施此政策。
3. 所有人員和供應商均須依照相關安全管理程序以維護資訊安全政策。
4. 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
5. 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行懲處。

伍、 目標

維護本公司資訊資產之機密性、完整性與可用性，並保障使用者之個人隱私。藉由全體同仁共同努力來達成下列目標：

1. 保護本公司業務活動資訊，避免未經授權的存取含雲端服務之存取與控制。
2. 保護本公司業務活動資訊，避免未經授權的修改，確保其正確完整。
3. 建立跨部門之資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保本公司具備可供業務持續運作之資訊環境。
4. 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
5. 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
6. 重要的資訊安全設施應視需要評估建立備援架構，以確保系統可用性。
7. 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。
8. 本公司之業務活動執行須符合相關法令或法規之要求。
9. 供應商提供之服務，應對其服務之項目及內容進行控管、查核及驗收管理。
10. 公司應建立內部、外部溝通協調機制。
11. 公司應對資訊安全管理系統定期檢視並持續改善。
12. 針對雲端服務資訊安全之要求，本公司必須妥予規劃與執行。
13. 本公司對雲端服務內部授權人員，須做妥善之風險管理。
14. 本公司雲端服務對於供應商與客戶之間、客戶與客戶之間，須妥予區隔。
15. 雲端服務之存取控制人員，其權責須做完善之規定與管理。
16. 當雲端服務之相關管理及作業規定有變動及影響雲端服務時，須告知客戶。
17. 雲端服務之客戶資料，須予以妥善保存。
18. 應針對雲端服務之客戶，做好生命週期管理。
19. 當雲端服務有事件或事故發生時，須有明確之調查及處理規範，並通知主管單位及受影響之利害關係方。
20. 雲端服務之作業過程，個人資料處理者，須負個人隱私保護之直接責任。
21. 雲端服務之作業過程，個人資料管理者，亦須負個人隱私之保護責任。
22. 雲端服務個人隱私保護要求須於合約中明述；合約內容與要求可依雙方需求而設定。

23. 配合「資通安全管理法」及相關子法規範，所屬關鍵基礎設施資通安全責任等級之要求，並考量所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資訊安全管理作業。

陸、 相關文件

1. IS-D-046 內外部關注議題與要求對應表