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、VPN 機房、Cloud 服務、NOC 維運作業系統及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。

本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)。

資訊安全管理涵蓋 14 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。管理事項如下：

1、安全政策
2、資訊安全的組織
3、人力資源安全
4、資產管理
5、存取控制
6、加密
7、實體與環境安全
8、營運安全
9、通訊安全
10、資訊系統獲取、開發及維護
11、供應商關係
12、資訊安全事件管理

13、有關於資訊安全方面的營運持續管理

14、適法性

本公司之內部人員、供應商與訪客皆應遵守本政策。

本公司資訊安全內外部議題及關注事項對應表，如下：

內外部 利害關係方	期盼、關懷及議題 （資訊安全方面）	政策	對應事項及文件	目標及指標
1. 國家通訊傳播委員會(NCC)	確保網路及通訊運作之資訊安全	1. 資訊安全政策 2. 資訊安全之組織政策 3. 資產管理政策 4. 人力資源安全政策 5. 存取控制政策 6. 實體與環境安全政策 7. 通訊及作業管理政策 8. 資訊系統獲取、開發及維護政策 9. 資訊安全事故管理政策 10.營運持續管理政策 11.遵循性政策	1. IS-A-001 資訊安全政策 2. IS-B-001 資訊安全組織程序書 3. IS-B-003 資訊資產管理作業程序 4. IS-B-004 風險評鑑與管理作業程序 5. IS-B-005 人員安全與教育訓練作業程序 6. IS-B-006 實體安全管理作業程序 7. IS-B-007 通信與作業管理作業程序 8. IS-B-008 存取控制管理作業程序 9. IS-B-009 系統開發與維護作業程序 10.IS-B-010 供應商管理作業程序 11.IS-B-011 安全事件管理作業程序 12.IS-B-012 營運持續管理作業程序 13.IS-B-013 資訊安全稽核作業作業程序 14.IS-B-014 矯正及預防管理作業程序 15.IS-B-015 營運持續計畫作業程序	A.5 資訊安全政策訂定與評估 1.資訊安全政策審查次數 2.資訊安全政策宣導次數 A.6 資訊安全組織 1.有否確實簽署保密協議 2.管理審查會議召開次數 A.7 人力資源安全 1.檢查資通訊人員資安教育訓練時數 2.檢查業務人員資安教育訓練時數 3.檢查主管、一般人員資安教育訓練時數 4.離退人員帳號確實刪除 A.8 資訊資產管理 1.資訊資產清冊更新 2.資訊資產清冊符合分級與標示規定 A.9 存取控制安全 1.定期審查重要系統存取權限 2.未授權存取重要系統機敏性資料之次數 A.10 加密 1.定期變更電腦登入系統密碼 A.11 實體與環境安全 1.檢查有否遵守機房門禁規定 2.檢查消防器材有否定期保養 3.檢查 UPS 有否定期保養 A.12 營運安全 1.定期監控網路重要伺服器執行作業之系統容量（例如 CPU、RAM、硬碟） 2.檢查病毒碼是否即時更新 3.定期備份重要系統資料 A.13 通訊安全 1.內部網路斷線次數(年) 2.檢查重要系統時間是否同步 3.檢查防火牆設定是否與防火牆設定紀錄表資料相符 4.弱點掃瞄次數 A.14 資訊系統獲取、開發及維護 1.重要系統更新/上線前經測試

內外部 利害關係方	期盼、關懷及議題 （資訊安全方面）	政策	對應事項及文件	目標及指標
				2.重要系統開發或變更時應更新系統文件 3.重要系統上線具有緊急復原機制 A.15 供應商關係 1.是否確實簽署保密協議 A.16 資訊安全事件管理 1.發生資安事件未依規定通報之件數 2.檢查資通安全事件通報單，是否重複發生相同資安事故件數 A.17 有關於資訊安全方面的營運持續管理 1.檢討營運持續計畫演練執行情形 2.執行風險評鑑與營運衝擊分析 A.18 相關法規與施行單位政策之符合性 1.合法軟體之安裝 2.矯正預防措施於規定時間內改善完成
經濟部投審會及國家通訊傳播委員會(NCC)	赴大陸投資應取得 ISO27001 及 ISO27011 資安認證	1. 建立資訊安全管理系統並通過國際驗證	1. ISO 27001 及 TAF CNS27011 有效證書	1 TAF 證書號碼 ISMS031 2 DAkkS 證書號碼 44 121 110056
2. 公司管理階層	有效規劃及執行資訊安全教育訓練，以提升本公司資訊安全意識及專業知識。	1. 人力資源安全	1. IS-B-005 人員安全與教育訓練作業程序	A.7 人力資源安全 1.檢查資通訊人員資安教育訓練時數 2.檢查業務人員資安教育訓練時數 3.檢查主管、一般人員資安教育訓練時數 4.離退人員帳號確實刪除

內外部 利害關係方	期盼、關懷及議題 （資訊安全方面）	政策	對應事項及文件	目標及指標
	機房及網路管理安全	1.實體安全管理政策 2.通信與作業管理政策 3.營運持續管理政策	1. IS-B-006 實體安全管理作業程序 2. IS-B-007 通信與作業管理作業程序 3. IS-B-012 營運持續管理作業程序	A.11 實體與環境安全 1.檢查有否遵守機房門禁規定 2.檢查消防器材有否定期保養 3.檢查 UPS 有否定期保養 A.12 營運安全 1.定期監控網路重要伺服器執行作業之系統容量（例如 CPU、RAM、硬碟） 2.檢查病毒碼是否即時更新 3.定期備份重要系統資料 A.13 通訊安全 1.內部網路斷線次數(年) 2.檢查重要系統時間是否同步 3.檢查防火牆設定是否與防火牆設定紀錄表資料相符 4.弱點掃瞄次數 A.17 有關於資訊安全方面的營運持續管理 1.檢討營運持續計畫演練執行情形 2.執行風險評鑑與營運衝擊分析
3. 客戶	1. 機房及網路管理安全 2. 雲端服務資訊安全及個人隱私保護	1.實體安全管理政策 2.通信與作業管理政策 3.營運持續管理政策	1. IS-B-006 實體安全管理作業程序 2. IS-B-007 通信與作業管理作業程序 3. IS-B-012 營運持續管理作業程序	A.11 實體與環境安全 1.檢查有否遵守機房門禁規定 2.檢查消防器材有否定期保養 3.檢查 UPS 有否定期保養 A.12 營運安全 1.定期監控網路重要伺服器執行作業之系統容量（例如 CPU、RAM、硬碟） 2.檢查病毒碼是否即時更新 3.定期備份重要系統資料 A.13 通訊安全 1.內部網路斷線次數(年) 2.檢查重要系統時間是否同步 3.檢查防火牆設定是否與防火牆設定紀錄表資料相符 4.弱點掃瞄次數 A.17 有關於資訊安全方面的營運持續管理 1.檢討營運持續計畫演練執行情形 2.執行風險評鑑與營運衝擊分析

參、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、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、落實本公司 NOC 維運作業系統及相關部門與維運管理人員之標準作業程序，以確保本公司 IDC、VPN 機房及 Cloud 服務之機密性、完整性、及可用性，以符合利害相關團體之要求與期盼。
2、保護本公司業務活動資訊，避免未經授權的存取。
3、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。
4、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。
5、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。
6、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。
7、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。
8、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。
9、本公司之業務活動執行須符合相關法令或法規之要求。
10、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。
11、公司應建立內部、外部溝通協調機制。
12、公司應對資訊安全管理系統定期檢視並持續改善。
13、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。
14、本公司對雲端服務內部授權人員，須做妥善之風險管理。
15、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。
16、雲端服務之存取控制人員，其權責須做完善之規定與管理。
17、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。
18、雲端服務之客戶資料，須予以妥善保存。
19、應針對雲端服務之客戶，做好生命週期管理。
20、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。
21、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。
22、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。
23、雲端服務之個人隱私保護要求，須於合約中明述；合約內容與要求可依雙方需求而設定。

24、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。

伍、責任

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。