晉泰科技股份有限公司
Genesis Technology, Inc.

晉泰資訊安全政策

文件編號	IS-T-A-MIS-01	制定單位	資訊服務處
機密等級	一般	版次	V2.1
建立日期	2019/12/23	修改日期	2023/02/16

目　錄

壹、目的

晉泰科技股份有限公司（以下簡稱本公司）為強化資訊安全管理，確保本公司所屬之資訊資產（包含人員、設備、資料與文件等）的機密性、完整性及可用性，以保障資訊服務業務不中斷的持續運作，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，提升客戶服務品質與客戶最佳服務體驗，特定此政策規範。

貳、適用範圍

本公司依實際需要及符合政府與相關法令要求建立資訊安全管理系統。為確保資訊之機密性、完整性、及可用性，透過 SWOT 分析與利害關係對應表，將本系統適用範圍設定為資訊安全管理系統操作與維運；包括：資訊服務處、智慧服務維運中心(新竹)、資訊機房、巨雲通-行動協作雲服務(mCS)及巨雲通-視訊協作雲服務(vCS)，資訊安全管理系統之雲服務安全控制管理、操作與維運；包括：巨雲通-行動協作雲服務(mCS)及巨雲通-視訊協作雲服務(vCS)；並包含雲端事故之及時復原與雲端服務權責設施之管理與維護。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，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。並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「特定主題政策」(Specific Policies)如下，以能接續相對應之控制項目或措施：

1. 確實執行存取控制管理。
2. 有效執行重要資訊遮罩。
3. 貫徹實體及環境安全管控，含重要區域之監控。
4. 進行資訊資產管理。
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. 資訊安全事件管理。
10. 確實執行備份管理。
11. 執行金鑰管理。
12. 妥善進行資訊分類及處理。
13. 定期實施技術漏洞管理。
14. 執行系統開發安全管控。
15. 須建立及執行雲服務資訊安全管理機制。

參、權責

1、本公司資訊服務處負責擬定此政策，並呈管理階層審查核准後實施。
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、所有人員和委外服務廠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，若因而防止可能發生之資訊安全威脅事件，得視情況予以適當獎勵。
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。

肆、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硬體、軟體、文件及人員。
2、業務持續運作之資訊環境：係指為維持本公司各項業務正常運作所需之電腦作業環境。

伍、作業說明

維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。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、確保雲服務客戶間，具備安全之隔離。
4、雲服務相關人員，於雲服務過程中不得及無法接觸客戶資產，如因作業需要，須取得客戶同意。雲服務提供者之內部作業及管理環境須與雲服務客戶之作業環境明顯區隔。
5、客戶及相關人員，於進入雲服務系統時，需透過身分驗證過程，以確保雲服務之資訊安全。
6、雲服務作業過程如有變更，依合約要求通知雲服務客戶，或進行必要溝通。
7、雲服務虛擬化作業，須具備雲端資訊安全之考量。
8、當客戶終止接受雲服務時，權責單位須將該客戶之所有資訊資產清除，以確保客戶權益及雲服務資訊安全。
9、當不符合事項發生或違規行為發生時，須與客戶進行必要之溝通，並視需要提供調查結果及相關資訊。

10、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。

11、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。

12、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。

13、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。

14、本公司之業務活動執行須符合相關法令或法規之要求。

15、雲服務提供者及雲服務客戶，雙方應訂定資訊安全責任與規定。

16、雲服務提供者應於協議（合約）中清楚定義相關資訊安全措施，以確保雙方之間不會有任何誤解。

17、雲服務提供者應於相關文件中定義雙方間，資訊安全事件之責任歸屬。

18、雲服務提供者須針對客戶資料及雲服務功能作有效維護，並設定存取權限機制。

19、持續改善資訊安全管理系統之承諾：本公司全體同仁，均須依照相關資訊安全管理程序來落實資訊安全政策。同仁皆有責任報告資訊安全事件或提出強化資訊安全之建議，若因而防止可能發生之資訊安全威脅事件，將視情況予以適當獎勵。同時若有從事任何危及資訊安全之行為，也將視情節輕重依本公司之相關規定進行懲處，以維護本公司資訊資產，並保障公司與客戶資料隱私與安全。

陸、相關文件

無。