台灣特洛奇資訊有限公司

「資訊安全管理系統」
資訊安全政策

機密等級：一般

編號：IS-01-001

版本編號：1.0

修訂日期：115.01.07

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

目錄：

本資料為台灣特洛奇資訊有限公司專有之財產，非經書面許可，不准使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

1 目的

1.1 台灣特洛奇資訊有限公司(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，以提供本公司之資訊業務持續運作之資訊環境，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，特定此政策規範。

2 適用範圍

2.1 本公司之所有單位。

3 定義

3.1 所有人員：本公司人員與委外廠商。

4 願景與目標

4.1 資訊安全政策願景：

4.1.1 強化人員知能

4.1.2 避免資料外洩

4.1.3 落實日常維運

4.1.4 確保服務可用

4.2 依據資訊安全政策願景，擬定資訊安全目標如下：

4.2.1 辦理資訊安全教育訓練，推廣人員資訊安全之意識與強化其對相關責任之認知。

本資料為台灣特洛奇資訊有限公司專有之財產，非經書面許可，不准使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

4.2.2 保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整。

4.2.3 定期進行內部與外部稽核，確保相關作業皆能確實落實。

4.2.4 確保本公司關鍵業務系統維持一定水準的系統可用性。

4.3 應針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間以及結果評估方式與評估結果，相關監督與量測程序，應遵循本公司「監督與量測管理程序書」辦理。

4.4 資訊安全執行小組應於管理審查會議中，針對資訊安全目標有效性量測結果，向資訊安全委員會召集人進行報告。

5 責任

5.1 本公司的管理階層建立及審查此政策。

5.2 資訊安全執行小組透過標準和程序以實施此政策。

5.3 所有人員須依照相關安全管理程序以維護資訊安全政策。

5.4 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。

5.5 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。

5.6 資訊安全政策應傳達至內部及外部人員，並得透過內部公告、會議、教育訓練、官網、電子郵件等方式傳達。

本資料為台灣特洛奇資訊有限公司專有之財產，非經書面許可，不准使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

6 審查

6.1 本政策應至少每年審查一次，以反映政府法令、技術及業務等最新發展現況，以確保本公司永續運作及資訊安全實務作業能力。

7 實施

7.1 下年度資訊安全政策配合當年度管理審查會議進行審核。

7.2 本公司各單位基於業務屬性差異，執行資訊安全管理作業並互相支援。各單位負責項目請參考附表「ISMS 流程與組織對應表」。

7.3 各單位執行資訊安全管理作業，如下列項目需進行變更，應依規劃之方式執行變更：

7.3.1 資訊安全管理系統變更。

7.3.2 發生重大資安事故。

7.3.3 有新增、變更或移除資訊資產。

7.3.4 作業環境改變。

7.4 如需進行資訊安全管理系統變更，應考量下列事項：

7.4.1 變更的目的與其潛在之影響。

7.4.2 管理系統的完整性。

7.4.3 資源的可用性。

7.4.4 職責與權限之分配或重新分配。

本資料為台灣特洛奇資訊有限公司專有之財產，非經書面許可，不准使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

7.5 本政策經「資訊安全委員會」進行會審後，由召集人核定後實施，修訂時亦同。

本資料為台灣特洛奇資訊有限公司專有之財產，非經書面許可，不准使用本資料，亦不准複印，複製或轉變成任何其他形式使用。