新竹市警察局
「資訊安全管理系統」
資訊安全政策

機密等級：一般

編　　號：**HCCP-IS-01-001**

版本編號：1.0

修訂日期：106.10.18

使用本文件前, 如對版本有疑問, 請與修訂者確認最新版次

本文件歷次變更紀錄：

版次	修訂日	修訂者	說　　明	核准者
1.0	106.10.18	資安執行小組	ISO 27001:2013 版文件發行	李建廣副局長

本政策由資安執行小組負責維護。

目錄：

1 目的

1.1 新竹市警察局（以下簡稱本局）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，以提供本局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 本局各行政單位。

2.2 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，對本局帶來各種可能之風險及危害。管理事項如下：

2.2.1 資訊安全政策訂定與評估。
2.2.2 資訊安全組織。
2.2.3 人力資源安全。
2.2.4 資產管理。
2.2.5 存取控制安全。
2.2.6 密碼安全。
2.2.7 實體與環境安全。
2.2.8 作業安全。
2.2.9 通訊安全。
2.2.10 系統獲取、開發與維護之安全。
2.2.11 供應者關係管理。
2.2.12 資訊安全事件之反應及處理。
2.2.13 營運持續運作管理。
2.2.14 相關法規與施行單位政策之符合性。

本局之內部人員、委外服務廠商與訪客皆應遵守本政策。

3 定義

3.1 資訊資產：係指為維持本局資訊業務正常運作之硬體、軟體、資料、文件、環境、通訊及人員。

3.2 營運持續運作之資訊環境：係指為維持本局各項業務正常運作所需之資訊作業環境。

4 政策

4.1 本局資訊安全管理政策：

確保資料安全、強化資安教育
防制資安風險、維繫業務運作

5 目標

5.1 在配合本局資訊安全政策要求，維護本局資訊資產之機密性、完整性與

可用性，並考量風險評鑑結果與適用之資訊安全要求事項制訂下列資訊安全目標，藉由全體同仁共同努力來達成：

5.1.1 保護本局業務活動資訊，避免未經授權的存取。

5.1.2 保護本局業務活動資訊，避免未經授權的修改，確保其正確完整。

5.1.3 建立資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保本局具備可供業務持續運作之資訊環境。

5.1.4 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。

5.1.5 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。

5.1.6 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。

5.1.7 本局之業務活動執行須符合相關法令或法規之要求。

6 責任

6.1 本局的管理階層建立及審查此政策。

6.2 資訊安全管理者透過適當的標準和程序以實施此政策。

6.3 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。

6.4 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。

6.5 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局之相關規定進行懲處。

7 審查

7.1 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，以確保本局永續運作及資訊安全實務作業能力。

8 實施

8.1 資訊安全政策配合每年資訊安全管理審查會議進行資訊安全政策審核。

8.2 本政策經「資訊安全組織召集人」核定後實施，修訂時亦同。