彰化縣政府地政處暨各地政事務所

「資訊安全管理系統」
資通安全政策

機密等級：一般

編　　號：IS-N0-01-001

版本編號：2.0

制訂日期：112.08.01

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	105.12.21	資訊安全執行小組	初稿制訂(彰化縣政府 105.12.21 府地籍字第 1050442692 號函)	資訊安全委員會
1.1	108.2.21	資訊安全執行小組	增訂 7.1 及 7.2 保密規範(彰化縣政府 107.5.28 府地籍字第 1070178955 號函)	召集人
1.2	109.06.30	資通安全執行小組	修正「資訊安全」為「資通安全」以符合「資通安全管理法」要求	資通安全長
2.0	112.08.01	資通安全執行小組	因應 ISO/IEC 27001:2022 年版進行升級改版	資通安全長

本程序書由資通安全執行小組負責維護。

目錄：

1 目的

1.1 彰化縣政府地政處（以下簡稱本地政處）與所轄各地政事務所（以下簡稱各地所）為強化資通安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本地政處與各地所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 本地政處與各地所之所有單位。

2.2 資通安全管理涵蓋 4 個面向控制措施，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，對本地政處與各地所帶來各種可能之風險及危害。管理事項如下：

2.2.1 組織面控制措施。

2.2.2 人員面控制措施。

2.2.3 實體面控制措施。

2.2.4 技術面管理。

3 定義

3.1 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Information security management systems ,Requirements 資訊安全－網路安全與隱私保護－資訊安全管理系統－要求事項。

4 資通安全政策

為了使本地政處與各地所 ISMS（資訊安全管理系統）能切合實際需要，藉由維護本地政處與各地所重要資通系統之機密性、完整性與可用性，以支持業務之順遂，特頒布資通安全管理政策。本政策為本地政處與各地所資通安全管理之最高指導原則，所有同仁、委外廠商皆有義務積極參與推動資通安全管理政策，以確保所有資通系統安全維運，並期許所有人均能了解、實施與維持，以達資訊持續營運配合本地政處與各地所業務遂行的目標。

4.1 落實資通安全，強化資通服務品質

貫徹執行 ISMS，所有資訊作業相關措施，應確保資料之機密性、完整性及可用性，免於因相關資訊安全威脅遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度進行監控、審查及稽核資訊安全管理制度的工作，以完善的資通安全強化服務品質，提升服務水準。

4.2 加強資安訓練，符合法令要求規範

加強資安訓練，督導全體同仁落實資通安全管理，持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全相關法令要求之重要性，進而遵守法令及規定，藉此提高資通安全認知及能力，降低資通安全風險，達成資通安全管理法及個

人資料保護法等相關法令要求事項。

4.3 規劃持續營運，迅速完成災害復原

訂定關鍵性業務核心資通系統之緊急應變計畫及災害復原計畫，每項核心資通系統每兩年必須至少執行一次緊急應變流程演練，以確保資通系統失效或重大災害事件發生時，能迅速復原，保持關鍵性核心資通系統持續運作，達成本地政處及各地所主要業務順利執行。

4.4 合理利用個資、防範個人資料外洩

對個人資料進行分類和評估，以確定保護的需求和措施。建立存取控制機制，於個資傳輸及共享方面採用加密與安全措施，定期評估受託者的遵守能力，並與受託者簽訂合約和協議以確保個資安全。強化員工教育訓練，增強個資保護意識。建立監控和審查機制，持續監視個資的使用、存取和傳輸，並及時檢測和應對異常活動或安全事件。確保不再需要時，個資能夠被安全且永久地刪除。

5 資通安全管理目標

本地政處及各地所執行 ISMS 需達成之資通安全目標，應依據「IS-N0-02-015 監督與量測管理程序書」之相關規定辦理。

6 資通安全責任

6.1 本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本地政處與各地所永續運作及資通安全實務作業能

力。

6.2 資通安全管理者透過適當的標準和程序以實施本政策。

6.3 所有人員與契約委外廠商均須依照程序以維護資通安全管理政策。

6.4 所有人員有責任通報安全事件和任何已鑑別出的弱點。

6.5 任何蓄意違反資通安全的行為將受到相關規範或法律行動。

6.6 資通安全執行小組應於管理審查會議中，針對資通安全目標有效性量測結果，向資通安全委員會召集人(資通安全長)進行報告。

7 實施

7.1 機關單位因業務需求取得本地政處與各地所機敏性資訊或個人資料時，應負起資料保密責任及妥善運用，並遵守國家相關之法令及本地政處與各地所之相關資通安全規定。

7.2 若因資料取得機關單位疏失造成資料外洩或資安事件，應負相關法律責任。

7.3 資通安全政策配合管理審查會議進行審核。

7.4 本政策經「資通安全委員會」進行會審後，由召集人（資通安全長）核定後實施，並以書面、電子郵件、網站公告或其他方式告知本地政處與各地所所屬員工及與本地政處或各地所有關之機關（構）、委外廠商...等利害關係者，修訂時亦同。