彰化縣教育網路中心

「資通安全管理系統」
資訊安全政策

機密等級：一般

編　　號：IS-01-001

版本編號：2.0

制訂日期：113.02.01

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	110.12.06	資安保護執行小組	初版發行	召集人
2.0	113.02.01	資安保護執行小組	因應 ISO/IEC 27001:2022 年版進行升級改版	召集人

本程序書由資安保護執行小組負責維護。

目錄：

1 目的

1.1 彰化縣教育網路中心（以下簡稱本中心）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，以提供本中心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 本政策適用於本中心各項資訊資產及其使用者，使用者係包含同仁、委外服務供應商及其他經授權使用資訊資產之人員。

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，對本中心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 願景與目標

4.1 資訊安全政策願景：

強化人員認知、避免資料外洩

落實日常維運、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，推廣同仁資訊安全之意識與強化其對相關責任之認知。

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

4.2.3 定期進行稽核作業，確保相關作業皆能確實落實。

4.2.4 確保本中心關鍵核心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，應遵循本中心「監督與量測管理程序書」辦理。

4.4 資安保護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，向資訊安全保護推動委員會召集人進行報告。

5 責任

5.1 本中心的管理階層建立及審查此政策。

5.2 資安保護執行小組透過標準和程序以實施此政策。

5.3 所有人員和委外服務供應商均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中心之相關規定進行懲處。

6 審查

6.1 本政策應至少每年審查 1 次，以反映政府法令、技術及業務等最新發展現況，以確保本中心永續運作及資訊安全實務作業能力。

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 任何機關單位因業務需求取得本中心機敏性資訊或個人資料時，應負起資料保密責任，並做妥善運用，且須遵守國家相關之法令及本中心

之相關資訊安全規定。

7.2 若因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 資訊安全政策配合管理審查會議進行審核。

7.4 本政策經「資訊安全保護推動委員會」進行會審後，由召集人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中心所屬員工及與各校、委外廠商...等利害關係者，修訂時亦同。