新竹縣政府資訊安全政策

一、 新竹縣政府 (以下簡稱本府) 為配合行政院推動各機關強化資訊安全管理，建立安全及可信賴之電子化政府，特訂定本政策。

二、 本政策係依據資通安全管理法、行政院及所屬各機關資訊安全管理要點等有關法令，考量本府業務需求，參考行政院及所屬各機關資訊安全管理規範訂定。

三、 為確實掌握本縣所屬各機關之資訊通訊及網路系統遭受破壞、不當使用等危安或重大災害事件，設置本府資通安全管理委員會及其資通安全推動中心 (以下簡稱推動中心)，處理執行本縣所轄各機關及公民營事業機構之資通安全預防及危機通報、緊急應變處理相關措施。

四、 本政策目的為確保資訊業務之永續經營，建立資料處理、傳送及儲存之安全環境，確保本縣資料、系統、設備及網路安全，以保障民眾權益。

五、 依下列分工原則，配賦有關單位及人員權責：
(一) 資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由推動中心安全預防組負責辦理。
(二) 資料及資訊系統之安全需求研議、管理及保護等事項，由各業務單位負責辦理。
(三) 資訊機密維護及安全稽核等事項，由推動中心稽核小組會同相關單位負責辦理。

六、 本政策之範圍如下，有關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效：
(一) 人員管理及資訊安全教育訓練。
(二) 電腦系統安全管理。
(三) 網路安全管理。
(四) 系統存取控制。
(五) 系統發展及維護安全管理。
(六) 資訊資產安全管理。
(七) 實體及環境安全管理。
(八) 營運持續管理計畫之規劃與管理。

七、 人員應適當施予資訊安全教育訓練，提升資安觀念，人員調職或離職應終止其作業權限。

八、 委外辦理資通系統之建置、維運或資通服務之提供應依據法規或契約實施廠商安全管理，防止機敏資料或個人資料被竊取、竄改、毀損、滅失或洩漏。資訊系統應依相關法規或契約規定，完成資通系統分級，並依防護基準執行控制措施。

九、 對外網路連線應採取加密通道作業，建立網路流量監控機制，確保網路之持續可用；未經當事人授權之個人資訊不得於網路上公開，訂定電子郵件使用規定，機密性資料及文件之傳送應採取資料加密等保護措施。與外界網路連接之網點，應以防火牆及其他必要安全設備，禁止私設無線網路連接本府公務用網路，防止未經授權的網路存取。

十、 因公務需求申請電腦系統存取控制授權，應以最小授權為原則並留下紀錄。廠商遠端連線，應課其相關安全保密責任，作業期間應留下日誌紀錄。

十一、 系統發展應在系統生命週期之初始階段，即將資訊安全及個人資料管理需求納入考量，系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

十二、 資訊資產應依據安全等級分類，訂定資產項目及擁有者。資料保護或公開應符合相關法律規定辦理。

十三、 明訂有關實體及環境安全管理之設備安置、周邊環境、人員管制及其他安全管理措施，以確保系統及資料之安全。

十四、 應訂定營運持續管理計畫和資訊安全事件緊急處理機制，並依不同安全等級，採取適當及充足之資訊安全措施。

十五、 建立資訊安全稽核制度，定期及不定期進行資訊安全稽核作業，包含資訊業務委外廠商稽核。

十六、 本政策應至少每年評估一次，必要時得依最新法令、技術及業務或其他發展現況隨時評估，確保資訊安全實務作業之有效性。