彰化縣福興鄉公所資訊安全政策

中華民國 104 年 1 月 9 日

福鄉行字第 1040000238 號

彰化縣福興鄉公所（以下簡稱本機關）為強化資訊安全管理，確保資料、系統、設備及網路安全，特訂定本政策。

*本政策係依據行政院及所屬各機關資訊安全管理要點等有關法令，考量本機關業務需求，參考行政院及所屬各機關資訊安全管理規範訂定，並以書面、電子或其他方式通知員工及與本機關連線作業之有關機關（構）、廠商有所規範及遵循。

*為統籌資訊安全管理等事項之協調、推動及監督，成立跨部門之資訊安全處理小組，幕僚作業由資訊單位負責。

*分工原則：對安全作業程序及權責規範如下

1.資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。

2.資料及資訊系統之安全需求研議、管理及保護等事項，由業務單位負責辦理。

3.資訊機密維護及安全稽核等事項，由政風單位會同相關單位負責辦理。

4.資訊安全制度計畫擬訂、執行及定期、不定期進行稽核，撰寫報告、陳核、改進事項追蹤等，由資訊稽核小組辦理。

*執行政策之範圍：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。

1.人員管理及資訊安全教育訓練（人事室、資訊單位）。

2.電腦系統安全管理（資訊單位）。

3.網路安全管理（資訊單位）。

4.系統存取控制（資訊單位、政風室）。

5.系統發展及維護安全管理（資訊單位）。

6.資訊資產安全管理（資訊單位）。

7.資訊資產安全管理（資訊單位）。

8.業務永續運作計畫之規劃與管理（行政課（庶務）、政風室、資訊單位）。

*本政策之實施範圍如說明：

1.人員管理及資訊安全教育訓練

(1).對資訊相關職務及工作，應進行安全評估，於人員進用前嚴格篩選，於工作任務指派時，審慎評估其適任性，簽署保密協定，並進行必要之考核。訂定資訊

作業內部之代理制度，以確保系統之安全、順利運作。
(2).針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知及法律責任與遵循，正確使用資訊處理設備，以提升資訊安全水準。
2.電腦系統安全管理
(1).辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。
(2).依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。
(3).採行必要的事前預防及保護措施，偵測、錄影監控及防制電腦病毒及其他惡意軟體，確保系統正常運作。
3.網路安全管理
(1).開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
(2).與外界網路連接之網點，應以防火牆及其他必要安全設施作實體隔離，控管外界與內部網路之資料傳輸與資源存取。
(3).利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。
(4).訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。
4.系統存取控制
(1). 訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。
(2).離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
(3).建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過三個月為原則。
(4).對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，賦予相關安全保密責 任。
(5).對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，賦予相關安全保密責任。
5.系統發展及維護安全管理
(1).自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；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。
(2).對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。
(3).委託廠商建置及維護重要之軟硬體設施，應在本機關相關人員監督及陪同下始得為之。
6.資訊資產安全管理
(1).建立與資訊系統有關之資訊資產目錄，訂定資訊資產之項目、擁有者及安全等級分類等，且由專人負責並規範其權責。
(2).依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應之保護措施。
(3).已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。
7.實體及環境安全管理
就設備安置、周邊環境之保全及資訊室人員進出管制、重要媒體異地存放及報廢等，訂定實體及環境安全管理措施。
8. 業務永續運作計畫之規劃與管理
(1).訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。
(2).建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或資通安全處理小組通報，採取反應措施，必要時並聯繫檢警調單位協助偵查。
(3).依相關法規訂定及區分資料安全等級，並依不同安全等級採取適當及充足之資訊安全措施。
*本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。
*本政策自鄉長核定後發布施行，修訂時亦同。