雲林縣政府

Yunlin County Government

資訊安全管理制度

政策

文件編號： YLHG-01-001

版　　次： 1.6

文件日期： 112 年 10 月 24 日

機密等級： 普通

文件版本制(修)訂紀錄

制(修)訂版次	制(修)訂核准日期/文號	文件制(修)訂說明	制(修)訂單位	制(修)訂者	文件管制員
V1.0	980202	初版發行	ISMS 執行小組		
V1.1	990401	「資訊安全管理系統執行小組」更名為「資訊安全管理系統執行分組」	ISMS 執行分組		
V1.2	106	配合「文件與紀錄管理程序」文件編碼原則修改	ISMS 執行分組		
V1.3	1071205	配合 ISO27001:2013 外部驗證稽核，修訂目標、原則、實施方式	ISMS 執行小組		
V1.4	1100813	「資安事故」更名為「資通安全事件」; 配合「文件與紀錄管理程序」將「資訊安全管理系統執行小組審議」修改為「資訊安全管理委員會審查」	ISMS 執行小組		
V1.5	111 年 7 月 28 日府計資一字第 1113009652 號書函	修訂文件框架及部分內容	ISMS 執行小組	莊齊珉	莊齊珉
V1.6	112 年 10 月 24 日府計資二字第 1123011863 號函	修正本府資通安全目標	ISMS 執行小組	莊齊珉	莊齊珉

目　　錄

壹、 目的

資訊安全政策（以下簡稱本政策）之目的為強化雲林縣政府（以下簡稱本府）資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，保障民眾權益。依據「資通安全管理法」及其子法、「ISO/CNS 27001：2013 資訊技術－安全技術－資訊安全管理系統－要求事項」、「個人資料保護法」及其子法及「著作權法」之相關規定，特訂定本政策，以茲各單位及全體人員遵循。

貳、 依據

一、 資通安全管理法

二、 資通安全管理法施行細則

三、 資通安全責任等級分級辦法

四、 資通安全事件通報及應變辦法

五、 資通安全情資分享辦法

六、 公務機關所屬人員資通安全事項獎懲辦法

七、 個人資料保護法

八、 個人資料保護法施行細則

九、 著作權法

十、 ISO/IEC 27001:2013 (Information technology — Security techniques — Information security management systems — Requirements)

十一、CNS 27001:2013 (資訊技術 — 安全技術 — 資訊安全管理系統 — 要求事項)

參、 適用範圍

本政策適用於本府所有單位及人員（含約聘僱人員、技工工友、臨時人員、替代役、各連線使用單位、協力廠商之駐府人員）及資訊資產。

肆、 政策原則

一、 目標

推動各單位強化資訊安全管理，建立「資訊安全，人人有責」之觀念，降低資通安全事件發生之機率及管理事件造成之影響至可接受的程度，以確保本府業務之正常運作及保障民眾權益，本府 ISMS 目標如下：

(一)確保本府提供之網路服務，於正常上班時間內因意外或操作錯誤造成無法使用持續達 4 小時以上之次數，每年不得高於 3 次。

(二)確保本府所提供之資訊服務，如發生資通安全事件時，不得有未依照法令規定通報之情形。

(三)確保本府之系統與資訊資產作業處理過程與結果符合機密性、完整性、可用性要求。

(四)確保本府之系統與資訊資產作業處理過程與結果符合法遵性要求。

二、 原則

(一)本府將配合上級主管機關及民眾等內外部關注方之需求，適時回應並持續改善本府所提供之相關資訊服務。

(二)確保資訊資產的機密性、完整性及可用性，防止敏感性資料與民眾個人資料外洩與遺失。

(三)各項資訊安全防護及管理規定，應符合政府資訊安全相關政策、規定及法令要求。

(四)以制定、演練、稽核及維護的方式，維持本府業務及資訊持續運作。

(五)提供本府同仁資訊安全訓練的機會，並應充分了解本政策及相關規範並克盡保護本府資訊資產安全之責。

(六)宣導民眾正確使用本府資訊。

(七)違反本政策與資訊安全相關規範，依相關法規議處。

(八)資訊資產（包括軟體、硬體、網路通訊設施及資料庫等）應

予適當保護，採行合宜之備援回復措施及作業，防止未經授權或因作業疏忽對資產所造成之損害，並定期演練前項備援回復作業。

(九)所有資通安全事件或可疑之安全弱點，應即時依程序通報反映，並予以適當調查及處理。

(十)往來廠商及民眾，由本府計畫處資訊管理科提供必要資訊安全技術之協助。

(十一) 接觸本府業務資料之外機關人員、委外服務提供廠商人員及訪客，亦應適當保護本府資訊資產之安全性。

(十二) 本政策應每年定期評估檢討，以反映政府法令、技術發展及業務需求等，以落實資訊安全作業。

(十三) 本政策須經資訊安全管理委員會審查通過，奉資安長核定後實施，修正時亦同。

三、 實施方式

(一)本府各單位主管對本政策及相關規範應負督導執行之職責。

(二)本府員工應充分了解本政策及相關規範，並克盡保護本府資訊安全之責。

(三)接觸本府業務資料之外機關人員、委外服務提供廠商人員及訪客，亦應配合本府所訂定之資訊安全相關要求，並適當保護本府資訊資產之安全性。

(四)往來廠商及民眾，由本府計畫處資訊管理科提供必要資訊安全技術之協助。

伍、 政策之評估及檢討

本政策內容應定期由資訊安全管理委員會轄下資通安全處理小組每年定期或因本府業務、法令或環境等因素之更迭，予以適當修訂，確保本府資訊暨個資安全實務作業的可行性及有效性，本政策經核定後於本府對外網站公告實施，修正時亦同。