

苗栗縣政府

資訊安全管理政策

機密等級：	<input checked="" type="checkbox"/> 公開 <input type="checkbox"/> 內部 <input type="checkbox"/> 機敏
文件編號：	MLG-ISMS-G-01-01
制(修)訂日期：	115年03月01日
版次：	5.0

文件制(修)訂紀錄表

文件版本	制(修)訂日期	制(修)訂摘要說明	制(修)訂者	核准者
1.0	107年9月1日	發行文件	管理師	資安長
1.1	107年12月1日	修訂資安政策貳、一、(一)法律遵循；(九)可用性要求	管理師	資安長
1.2	108年12月18日	修訂參考文件為資通安全管理法相關子法	管理師	資安長
1.3	109年11月13日	增訂參考文件，納入「公務機關所屬人員資通安全事項獎懲辦法」及「苗栗縣政府及所屬各機關學校公務人員平時獎懲標準表」	管理師	資安長
1.4	112年6月30日	因「行政院及所屬各機關資訊安全管理要點」已停止適用，從參考文件刪除。	管理師	資安長
2.0	113年04月01日	1. 因本府 113 年組織調整，將權責單位：計畫處資訊科調整為行政處資訊及為民服務科。 2. 新增名詞定義－權責單位。	管理師	資安長
3.0	113年09月01日	因應 ISO 27001 改版為 2022 版，調整參考文件(一)為 ISO/IEC 27001:2022，並新增(十)個人資料保護法及(十一)個人資料保護法施行細則。	管理師	資安長
4.0	114年05月01日	因本府 114 年組織調整，將權責單位：行政處資訊及為民服務科調整為行政處資訊科。	約聘人員	資安長
5.0	115年03月01日	因本府 115 年組織調整，將權責單位：行政處資訊科調整為資訊安全推動委員會。	約聘人員	資安長

目 錄

壹、總則	3
貳、政策內容	3
參、附則	4

壹、總則

一、制訂目的

- (一) 苗栗縣政府(以下簡稱本府)為維護民眾及自身權益，組織成員有責任和義務共同建立及維護一個安全的資訊與通訊作業環境，使資訊安全成為組織文化的一環，特訂定本資訊安全政策以「資訊安全，人人有責」為口號，並明確定義資訊安全目標與要求，以資遵循。
- (二) 本政策制訂之目的，在提供可依循之組織資訊安全指導大綱及方向，明確定義資訊安全管理之目標，並作為安全責任之指導原則。強化資訊安全管理，確保資料、資訊系統、資訊設備及網路通訊之安全，以有效降低因人為疏失、蓄意破壞、設備故障或天然災害等因素導致資訊資產遭竊、不當使用、洩漏、竄改、毀損或服務中斷之風險，符合資訊安全管理制度(ISMS)要求，確保資訊資產之機密性、完整性與可用性。

二、適用範圍

本府同仁。

三、權責單位

本府資訊安全推動委員會。

四、名詞定義

- (一) 機密性：確保資訊資產不受未經授權的存取、使用或揭露。
- (二) 完整性：確保資訊資產為真，並有能力證明其未經竄改或偽造。
- (三) 可用性：確保資訊資產於授權時間內，可以不受中斷的存取或使用。
- (四) 權責單位：協助制/修訂本政策，並送陳本府副首長核定並公告等行政流程。

貳、政策內容

一、資訊安全之要求事項承諾

- (一) 法規遵循：本府執行業務時應遵守資通安全管理法、個人資料保護相關法規及內部資訊安全管理相關規範。本府人員違反相關法規規範致生損害者，依相關規定究責。
- (二) 組織設置：設置資訊安全推動委員會，負責本府資訊安全管理之建立及推動。
- (三) 安全教育：定期實施資訊安全教育訓練，宣導資訊安全管理政策及實施規

定。

- (四) 規劃資源：建立資訊資產管理機制，統籌分配並有效應用資源，解決安全問題。
- (五) 事先防範：新資訊系統或服務建置或推出前，應納入資訊安全因素，以防範危害安全情況之發生。
- (六) 安全監控：建立資訊安全監控與防護措施，並定期進行檢視。
- (七) 授權管理：明確規範資訊系統、網路服務、敏感資訊之使用權限，防止未經授權存取之行為。
- (八) 檢討改善：訂定及執行內外部稽核活動，以落實資訊安全管理制度，並針對未盡事項執行改善。
- (九) 業務持續：訂定資訊安全之營運持續計畫並實際演練，確保突發事故發生時得以應變，以符合關注方對系統可用性之要求。
- (十) 資安文化：所有人員皆負有資訊安全之責任，且應了解及遵守相關之資訊安全規定，並於工作職責中落實。
- (十一) 領導承諾：本府管理階層應積極參與資訊安全管理活動，並提供推展資訊安全管理系統所需之支持及承諾。

二、持續改善資訊安全管理系統之承諾

本府應以「規劃－執行－確認－改善行動」之精神持續改善資訊安全管理系統。

三、目標及範圍

本府資訊安全管理系統應達成之目標詳如「資訊安全實施程序書」。

四、政策傳達

本政策於組織內傳達，於適用時提供給關注方，傳達方式詳如「資訊安全要求溝通說明與執行」。

參、附則

一、參考文件

- (一) ISO/IEC 27001：2022。
- (二) 資通安全責任等級分級辦法
- (三) 資通安全事件通報及應變辦法

- (四) 行政院所屬各機關資訊業務委外服務作業參考原則。
- (五) 資通安全管理法
- (六) 資通安全管理法施行細則
- (七) 資通安全情資分享辦法
- (八) 公務機關所屬人員資通安全事項獎懲辦法
- (九) 苗栗縣政府及所屬各機關學校公務人員平時獎懲標準表
- (十) 個人資料保護法
- (十一) 個人資料保護法施行細則

二、 相關表單

無。

三、 修訂與公告

- (一) 本政策應依組織、業務、法令或實體環境等因素更迭予以適當修訂。
- (二) 本政策由單位副首長(資訊安全推動委員會召集人或資安長)核定後公布施行，修正時亦同。