新北市政府地政局及
各地政事務所

F0-1-01

資通安全管理原則

機密等級：一般

文件版次：5.0

版本修訂紀錄表

文件版本	修訂日期	內容說明
5.0	113.07	因應 ISMS 制度轉版 27001:2022 版標準修正本原則，並依據新北市政府地政局 113 年 7 月 10 日第 1131355338 號簽奉核准。

資通安全管理原則

一、目的

新北市政府地政局（以下簡稱本局）及各地政事務所（以下簡稱各地所）為強化資通安全管理，依據資通安全管理法及其子法及新北市政府資訊安全政策，訂定本原則。以確保資訊資產安全，免於因內部或外部之蓄意或意外之各種威脅與破壞，導致業務資訊遭受竄改、揭露、破壞或遺失等風險，並符合國家法令法規及國際制度標準要求，作為資通安全管理系統作業程序之規範。

二、適用範圍

（一）本原則適用於本局及各地所各項資訊資產及其資訊使用者（含本局及各地所所屬員工、各應用系統建置維護廠商及其他經授權使用資訊資產之人員）。

（二）資通安全管理涵蓋組織、人員、實體及技術等四大控制主題，依本局及各地所業務特性，檢視各項資通安全控制措施適用情形，詳列於「適用性聲明書」落實管理。

三、資通安全定義

確保本局及各地所業務持續營運，落實資通訊相關人、事、物安全之保護措施，符合法令法規要求。依本質大致可歸類為：

（一）機密性－Confidentiality：使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

（二）完整性－Integrity：保護資產的準確度（accuracy）和完全性（completeness）的性質。

（三）可用性－Availability：經授權個體因應需求之可存取及可使用的性質。

（四）遵循性－Compliance：確保資通訊作業及資產保護，符合法律法規規範性質。

四、資通安全責任

（一）應由本局及各地所資通安全首長授權組織資通安全推動小組，並適時修訂本原則，以確保本原則符合現行需求。

（二）本局及各地所高階主管應積極參與資通安全管理活動，提供對

資通安全之支持及承諾。

（三）應每年定期召開資通安全會報會議，審核本原則之擬定，以確保本原則符合現行需求

（四）資通安全推動小組應提供本局及各地所全體同仁資通安全訓練課程相關資訊，提升人員資通安全認知。

（五）本局及各地所同仁應使用標準程序，以達成本原則對安全之各項要求並記錄之。

（六）本局及各地所同仁皆須遵守資通安全事件通報機制，通報所發現之資通安全事件或資通安全弱點。

（七）本局及各地所所有資訊往來廠商皆須簽署保密與責任條款，並遵守本原則以及相關程序之規定，不得未經授權使用或濫用各類資通訊資產。

（八）本局同仁、各地所同仁、本局及各地所資訊往來廠商都有責任遵循本原則。

（九）任何蓄意違反資通安全的行為將依相關規範處理或採取法律行動。

五、資通安全要求之政策及控制措施

（一）組織控制面

為明確規範組織與權責依業務特性制定「資通安全組織程序書」；為確保文件化資訊之控制，制定「文件管理程序書」；為落實資產風險管理與評鑑，制定「資訊資產管理程序書」及「風險評鑑與管理程序書」；為有效營運持續與事件通報，制定「營運持續與資通安全事件管理程序書」；為完善專案與委外安全管理，制定「專案與委外安全管理程序書」；為確保作業持續改善，制定「資通安全內部稽核管理程序書」。

（二）人員控制面

為確保所有人員任用符合資訊安全政策，制定「資通安全人事管理作業程序書」。

（三）實體控制面

為確保資訊資產免受威脅，避免人為破壞，防止資訊資產之遺失、破損、危害、失效及中斷影響運作，制定「實體及環境安

全管理程序書」。

（四）技術控制面

為落實資訊存取控制及資料保護作業，制定「資訊存取控制作業程序書」；為維持系統運維與網路安全管理，制定「系統維運與網路安全管理程序書」；為確保於軟體及系統開發安全，制定「系統開發程序書」。

六、為落實資通安全政策目的，應建立資通安全目標包含機密性、完整性、可用性及遵循性等要項，並確保資通安全管理指標之有效性，符合本局及各地所資通安全政策目的。

七、本原則應由資通安全推動小組每年定期或因業務、法令或環境等因素之變更，予以適當修訂，陳資通安全長核准後公告實施，並通知相關往來廠商。

八、本原則之相關表單由本局及各地所另訂之。