

資訊安全宣導 2 則

第一則

資訊安全的重要性

隨著電腦運用的普及與網際網路的蓬勃發展，已帶給人類急速而巨大的衝擊，也改變了人類生活模式。然而隨著資訊便利而來的則是令人擔憂的資訊安全問題，因此，我們必須做好資訊安全防護措施，唯有在確保資訊安全之前提下享受資訊便利，才是面對資訊世紀來臨的正確態度，進而迎接未來更大的挑戰與衝擊。

資訊安全防護的種類

- a. 實體安全：包含硬體環境控制、火災、地震、風災、水災及盜竊人為破壞管理控制...等。
- b. 軟體安全：包含程式及系統安全防護防止駭客、入侵、病毒及人為破壞管理控制...等。
- c. 資料安全防護：包含防止重要資料受損遺失或外洩，讓資料安全防護做到滴水不漏。

影響資訊安全的因素

- a. 未經授權者（駭客）侵入電腦系統，竊取或更改資料甚至更動原系統設定。
- b. 合法使用電腦人員有意或無心，造成資料的毀損、竊取或系統破壞。
- c. 資料在傳輸中途被截取、竊窺或變更。
- d. 電腦感染病毒與傳遞病毒。

資訊安全的應用層面

資訊安全相關工作又可概分為資料安全、電腦系統安全、網路安全與電腦病毒防治等應用層面。

第二則

資訊安全的防護措施

一、資訊資產目錄之建立及保護

- (一) 應該建立一份與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。
- (二) 資訊資產參考項目如下：
 - 1、資訊資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、業務永續運作計畫、預備作業計畫等。
 - 2、軟體資產：應用軟體、系統軟體、發展工具及公用程式等。
 - 3、實體資產：電腦及通訊設備、磁性媒體資料及其他技術設備。
 - 4、技術服務資產：電腦及通信服務、其他技術性服務（電源及空調）。

二、資訊安全之等級分類

- (一) 資訊安全分類原則
 - 1、應依據需要，建立資訊安全等級之分類標準，以及相對應的保護措施。
 - 2、資訊安全分類標準，應考量資訊分享及限制的影響、未經授權的系統存取或是系統損害對機關業務的衝擊，尤其要考量資料的機密性、資料真確性及可用性。
 - 3、資訊安全分類，可依據需要，區分機密性、敏感性及一般性等三類。
 - 4、界定資訊安全等級之責任，應由資料的原始產生者，或是由指定的系統所有者負責。
 - 5、當須執行或參考其他機關訂定之資訊安全等級分類時，應特別注意其與工作職務的資訊安全等級分類，在定義及標準上是否相同。
- (二) 資訊安全等級標示
 - 1、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。
 - 2、應納入安全等級分類的項目，包括書面報告、螢幕顯示、磁性媒體、電子訊息及檔案資料等。