作　業　項　目	資通安全管理辦法	編　號	H10

作　　業　　程　　序	控　制　重　點
一、網路及其週邊設備安全管理 1.網路設備(例如：電腦主機、伺服器、Switch、Hub…等) 應安裝穩壓及不斷電電力系統裝置(UPS)，以避免電壓不穩及不預期之斷電時，造成資料之流失。 2.須建立「網路設備配置圖」、「網路設備配置圖」及「網路使用者端配置圖」必隨時更新，以供維護人員查閱，並定期對於各線路檢測，以保持網路之暢通。 3.啟動設備時應注意運轉是否正常。 4.網路設備如發生故障時，應將其處理情況記錄於「網路設備故障表」內，以供查閱。 **二、人員安全與管理** 1.人員之進用及調派應作適當安全之評估。 2.對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工應有妥適分工、分散權責。 3.有網路作業需求或須調整使用權限者，須向資訊單位提出「網路帳號使用權限申請單」，經資訊單位主管審核同意後，交由資訊工程師完成使用者權限設定。 4.使用者密碼關係到資訊安全與防護，嚴禁張貼於電腦或電腦營幕上。 **三、通訊與操作管理** 1.發生資訊安全事件時，應立即填寫「資通安全事件通報單」給資訊組，並記錄其處理過程。 2.遵守軟體授權規定，禁止使用未取得授權之軟體。 3.定期對電腦系統及資料儲存煤體進行防毒掃瞄。 4.伺服器及個人電腦採必要的事前預防及保護措施。 5.委外時，與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，及對於機密性，敏感性資料之雙方權責及作業程序，納入契約條款。 6.對於外來及內容不確定的資訊檔案在使用前，應先作電腦病毒掃瞄，對重要的資料及軟體定期作	一、是否定期對單位人員及資訊設備進行安全評估，以確定其是否遵守資訊安全政策及相關規定。 二、發生資訊安全事件通報時，是否立即通報給危機處理小組，並記錄其處理過程。 三、與外單位簽訂資料存取之契約中是否包含資料保護、服務水準、智慧財產權、事故發生處理方式條款。 四、委外契約中有關安全需求內容是否包含法律需求(如電腦處理個人資料保護法)，界定雙方有關人員權責，使用何種實體與邏輯安全控管措施、得依實際需要隨時修改安全控管措施及作業程序等。

備份處理。 四、存取控制 1.資訊存取控制政策依工作性質與職務分別訂定，且需符合資料保護等相關法令與契約規定。 2.對於多人使用之資訊系統，應建立使用者註冊管理程序及記錄。 3.網路型態(Internet、Intranet、Extranet)訂定適當的存取權管理方式，且資訊系統與服務系統盡量避免使用共同帳號。 五、系統開發與維護 1.應用系統在規畫分析時，應將安全需求納入考量，安全控管方式則採用系統自動控管及人工控管兩種方式處理。 2.對高敏性的資料在傳輸或儲存過程中使用加密技術；對應用程式執行碼更新作業，限定只能由授權的管理人員才可執行，版本更新應係留舊版軟體及系統文件。 3.系統變更後，資訊組應主動公告異動的範圍、時間可能的影響，定期對使用軟體實施病毒偵測。 六、委外契約之管理作業 1.請購、採購及付款程序比照採購及付款循環辦理。 2.應簽訂委外契約，內容應合如下： A.對外單位簽訂資料存取之契約應合資料保護，服務水準、智慧財產權、事故發生處理方式等條款。 B.委外契約中有關安全需求內容應包含法律需求(如電腦處理個人資料保護法)，界定雙方有關人員權責，使用何種實體與邏輯安全控管措施，得依實際需要隨時修改安全控管措施及作業程序。 C.委外開發合約中應明訂對著作權之歸屬，並簽訂履行條約與相關罰則。	