

# 宜蘭縣員山鄉公所網路儲存裝置使用管理稽核作業規定

中華民國 112 年 4 月 10 日員鄉政字第 1120005420 號  
函訂定

## 壹、依據

- 一、個人資料保護法。
- 二、資通安全管理法。
- 三、資通安全管理法施行細則。
- 四、資通安全責任等級分級辦法。
- 五、無限網路安全參考指引。
- 六、政風機構人員設置條例第四條第七款。
- 七、政風機構維護公務機密作業要點。

## 貳、適用範圍

本作業規定適用範圍涵蓋本所及附屬單位(含幼兒園及圖書館)。

## 參、網路儲存裝置之管理

### 一、網路儲存裝置之保管

- (一)網路儲存裝置管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。

### 二、網路儲存裝置之使用

- (一)本所同仁使用資訊、資通系統及網路儲存裝置時，應留意其資通安全要求事項，並負對應之責任。
- (二)非本機關同仁使用本機關之資訊、資通系統及網路儲存裝置，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。

### 三、網路儲存裝置存取控制與加密管理

#### (一)網路安全控管

1. 使用者及管理應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
2. 使用者應經授權後在授權之範圍內存取本機關內部網路之網路資源。
3. 無線網路防護
  - (1)機密資料原則不得透過無線網路及設備存取、處理或傳送。
  - (2)行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

(3)用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二)網路儲存裝置使用者應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准，不得共用 ID。

#### 肆、網路儲存裝置安全管理

- 一、本所之主機、個人電腦及網路儲存裝置應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
- 二、使用者不得私自使用已知或有嫌疑惡意之網站。
- 三、應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞。攻擊網路儲存裝置。

#### 伍、網路儲存裝置使用安全

- 一、禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
- 二、儲存裝置連網應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- 三、筆記型電腦、實體隔離電腦等儲存裝置應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- 四、機密資料不得由未經許可之行動設備存取、處理或傳送。

陸、本所應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

#### 柒、網路儲存裝置稽核

- 一、由政風室協調權管課(室)提供稽核所需資料抽檢之，稽核結果如有異常情事，提列主管會報檢討，並保存相關紀錄備查。
- 二、稽核結果發現異常，再行調閱該帳號使用者使用紀錄，加以清查過濾，早期發現不法使用資料情事，以妥適處理。

柒、如有其他未盡事宜，參酌個人資料保護法、資通安全管理法暨其施行細則、資通安全責任等級分級辦法及無限網路安全參考指引等相關規定辦理。

捌、本作業規定簽奉鄉長核定後實施，修正時亦同。