

## 宜蘭縣政府及所屬各機關辦理資訊使用管理稽核作業規定

中華民國 98 年 04 月 17 府政行字第 0980055456 號函頒施行

中華民國 105 年 10 月 6 日府政行字第 1050164186 號函修正

第 8 點、刪除第 11 點。

一、宜蘭縣政府（以下簡稱本府）及所屬各機關（以下簡稱各機關）為維護資訊設備、網路、系統及資料使用安全，建立安全及可信賴之電子化政府，減少外在、人為因素破壞資訊使用安全，落實執行資訊機密維護及稽核使用管理工作，特訂定本作業規定。

前項稽核事項依本作業規定之規定；本作業規定未規定者，準用【行政院及所屬各機關資訊安全管理要點之規定。】

二、本府政風處及各機關政風單位應會同資訊等相關單位實施資訊使用管理稽核作業。必要時，得成立稽核小組，由政風單位辦理秘書作業，資訊單位負責技術支援。

三、實施稽核作業，得調閱有關資料、實地測試及檢查資訊軟、硬體設備使用情形。必要時，應由資訊等相關作業人員或本府計畫處資訊安全稽核師（主導稽核員 Lead Auditor）提供說明及專業諮詢意見。

四、資訊使用管理稽核實施範圍，應以系統存取控制管理為主，參酌機關資訊現況，針對下列事項，稽核其系統存取有無異狀及實施情形是否符合相關法令之規定：

- （一）網路存取安全管理。
- （二）使用者存取控制。
- （三）資訊系統存取控制及使用管理規定。
- （四）電腦系統存取控制。
- （五）應用系統存取控制。
- （六）機關外部人員存取資訊系統之安全管理。
- （七）系統存取權責及應用監督機制。
- （八）資訊資產安全管理。
- （九）實體及環境安全管理。

(十) 其他資訊安全管理事項。

五、資訊使用管理稽核作業程序如下：

- (一) 綜合分析本機關資訊系統特性、系統存取政策、系統異常存取狀況及授權規定或其他使用管理規定，據以研（修）訂稽核項目，擬訂稽核計畫陳報機關首長核可後實施。
- (二) 計畫內容包括：稽核目的、時間、項目、稽核人員編組、受稽核單位與人員、稽核方法、進程序及行政支援事項等。
- (三) 依據稽核結果就優缺點及改進措施提出書面報告，陳報機關首長及上級政風單位，並協調缺失單位確實檢討改進，必要時實施複查。
- (四) 前款報告內容包括：依據、稽核目的、時間、項目、稽核人員編組、受稽核單位及人員、稽核方法、稽核結果處理及建議事項等。

六、資訊使用管理稽核區分如下：

- (一) 外部稽核：指由上級機關對所屬機關或邀集專家、學者及相關機關共同組成跨機關稽核小組規劃辦理之稽核作業。
- (二) 內部稽核：指由本機關對內部單位自行規劃辦理之稽核作業。

七、本府每年實施資訊使用管理「外部稽核」作業一至二次，由政風處會同資訊等相關單位辦理。

八、本府列為資安等級 B 級機關，每年至少執行資訊使用管理「內部稽核」作業一次。

C 級以下機關，請自行檢視資訊使用管理「內部稽核」作業。

前二項各機關資安等級，依據行政院國家資訊安全會報訂定之資訊安全責任等級分級結果辦理。

九、各機關並得視業務實際需要實施不定期稽核。

十、各機關得依據本作業規定，審酌本機關主管業務性質、預算額度及實際需要，會同資訊及業務等相關單位訂定本機關資訊使用管理稽核作業規定。