資料外洩案例–檔案未限制存取權限

一、案情提要

（一）機關 C 內部系統提供所屬機關人員列印包含個資資訊功能，系統會自行產出列印報表檔案連結存放於伺服器。

（二）內部系統未提供公開連結下載報表，但檔案未限制存取權限，有心人士可透過搜尋引擎查找取得，造成機關 C 員工個人資料資訊外洩。

二、應變與改善作為

（一）機關C清查搜尋引擎可取得報表清單，釐清受影響對象與範圍，除透過存取紀錄，掌握資料流向，亦依個人資料保護法規範，通知相關受影響員工。

（二）協請廠商移除已產生報表檔，同時以白名單方式限制報表檔案存取權限。

（三）新系統於規劃設計階段已納入資安考量，將導入安全系統發展生命週期**(SSDLC)**。

（四）機關應依資訊系統服務對象設置存取來源，內部使用資訊系統建議以白名單設置存取來源。

（五）除定期檢視資訊系統帳號權限設置外，亦應檢視檔案**/**資料夾內容，確認存取權限設置適切性。

（六）存取機敏資料的資訊設備，應避免安裝非必要之應用軟體。