<table>
<tr><td>項目</td><td colspan="3">(七) 資通安全防護及控制措施</td></tr>
<tr><td>7.7</td><td colspan="3">是否針對電子郵件進行過濾，且定期檢討及更新郵件過濾規則？是否針對電子郵件進行分析，主動發現異常行為且進行改善（如針對大量異常電子郵件來源之 IP 位址，於防火牆進行阻擋等）？是否有電子郵件之使用管控措施，且落實執行？是否依郵件內容之機密性、敏感性規範傳送限制？</td></tr>
<tr><td rowspan="3">稽核依據</td><td>資通安全責任等級分級辦法應辦事項：技術面之資通安全防護之具有郵件伺服器者，應備電子郵件過濾機制</td><td colspan="2">N20703</td></tr>
<tr><td>資通安全責任等級分級辦法附表十資通系統防護基準：存取控制之帳號管理</td><td colspan="2">C0101</td></tr>
<tr><td colspan="3">1. 資通安全管理法施行細則
2. 第 6 條第 1 項第 8 款：資通安全防護及控制措施
3. 第 6 條第 1 項第 13 款：資通安全維護計畫與實施情形之持續精進及績效管理機制
4. 資通安全責任等級分級辦法第 11 條第 1 項：應辦事項之資通安全防護-具有郵件伺服器者，應備電子郵件過濾機制
5. 資通安全責任等級分級辦法第 11 條第 2 項：附表十資通系統防護基準：存取控制之帳號管理
6. 範本_玖、資通安全防護及控制措施_三、作業與通訊安全管理_(三)電子郵件安全管理
7. CNS27002：2023
(1) 5.14 資訊傳送：©以安全之方式(例：透過經鑑別及受保護的通道)，將鑑別資訊(包括暫時鑑別資訊)，傳送予使用者，且避免使用未受保護(明文)電子郵件訊息
(2) 8.2 特殊存取權限：(l)僅使用具特殊存取權限之身分，執行管理任務而非用於一般日常任務 [亦即檢查電子郵件、存取網頁(使用者宜具不同之正常網路身分進行此等活動)]</td></tr>
<tr><td>稽核重點</td><td>電子郵件資安防護措施</td><td>佐證資料</td><td>電子郵件資安管理措施及管理檢視情形</td></tr>
</table>

稽核參考	1. 了解機關電子郵件安全管理規範。 2. 電子郵件帳號宜定期清查，離職或不在職人員應即停用或刪除帳號。 3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。 4. 電子郵件過濾原則、發現異常行為之因應。 5. 最近 1 次電子郵件管理檢視情形。 6. 機關對於以電子郵件傳送機密性、敏感性資料之規範。 7. 下列安全控制措施參考： （1）傳遞機郵件，須以郵件加密傳送，且密碼應以電郵以外方式提供。 （2）電子郵件加簽。 （3）不應使用公務帳號加入網路社群、消費性雲端服務、網路會員購物網站。 （4）建議封鎖圖片自動下載等設定。 （5）預設開啟信件行為建議預設以純文字模式開啟郵件。 （6）可將收信軟體的郵件預覽功能關閉。
FQA	