<table>
<tr><td>項目</td><td colspan="4">(七)資通安全防護及控制措施</td></tr>
<tr><td>7.15</td><td colspan="4">是否建立帳號管理機制，並定期盤點?使用預設密碼登入資通系統時，是否於登入後要求立即變更密碼，並規定密碼強度、更換週期（限制使用弱密碼）？是否是最小權限？是否有使用角色型存取控制？有管理者權限之帳號是否有只用於管理活動？</td></tr>
<tr><td rowspan="5">稽核依據</td><td colspan="2">資通安全責任等級分級辦法附表十資通系統防護基準：識別與鑑別</td><td colspan="2">C0401、C0402C0403、C0404C0405</td></tr>
<tr><td colspan="2">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及最小原則</td><td colspan="2">C0101、C0102</td></tr>
<tr><td colspan="2">行政院資通安全處 105 年 11 月 30 日院臺護字第 1050185463 號函</td><td colspan="2">O01</td></tr>
<tr><td colspan="2">110 年 12 月 7 日行政院國家資通安全會報第 38 次委員會議擴大會議紀錄</td><td colspan="2">O01</td></tr>
<tr><td colspan="4">1. 資通安全責任等級分級辦法第 11 條第 2 項：資通系統防護基準之識別與鑑別-身分驗證管理</td></tr>
<tr><td>稽核重點</td><td>密碼（應不得使用預設密碼，且強度）應符合政府組態基準（GCB）</td><td>佐證資料</td><td colspan="2">存取控制文件、機關 GCB 套用情形、機關 GCB 例外管理清單、機關訂定之系統發展維護辦法、資通系統功能規格書、資通系統身分驗證功能測試紀錄、帳號權限清單</td></tr>
<tr><td>稽核參考</td><td colspan="4">1. 了解機關對於密碼之管理機制。
2. 新建帳號第一次或以預設密碼登入資通系統時，應有強制變更密碼機制。
3. 帳號不得為身份證字號。
4. 不得配置相同之預設密碼，建議不得為容易取得資料或其排列組合，如統編、身分證字號、機關代碼或身分證後 4 碼+生日年月日等。
5. 了解使用者權限是否最小化，權限應與職務符合。
6. 管理者帳號應只用於管理活動。
7. 資料查詢有涉及非公開資料者，其驗證方式是否易遭推論（如統編、流水</td></tr>
</table>

	號等)。 8. 系統帳號盤點與管理(含離職人員之異動交接)： (1) 不共用帳號、啟用多因子認證、內容發佈建立審核和授權機制、避免分享機密或敏感資訊，並應定期檢查帳號登入紀錄。 (2) （建議事項）宜包含社群媒體平臺，如政府機關對外政策溝通應用之管道 Facebook、Instagram 等，並適用於社群媒體平臺經營者(包含所有管理者、編輯、版主等)。
FQA	