附表：具目錄服務之機關應辦事項

構面	應辦事項
存取控制	1. 建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 2. 閒置帳號、已逾期之臨時或緊急帳號應刪除或禁用。 3. 定期審核帳號之申請、建立、修改、啟用、停用及刪除。 4. 採最小權限原則，僅允許使用者依機關任務及業務功能，完成指派任務所需之授權存取。 5. 目錄服務維運廠商帳號需經該目錄服務之機關資訊主管核准始可登入使用，並按作業內容採一次性有效、單次作業效期不得超過一天為原則。屬常態性維運作業或特殊事由，若經該目錄服務之機關資訊主管核准，則不受前述限制，惟效期最長不得超過一年。 6. 目錄服務網域管理者帳號、特權帳號及維運廠商帳號應每月定期盤點，盤點結果需提交資訊單位主管確認。 7. 目錄服務主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取 8. 目錄服務應禁止與網際網路進行連線，並不得自網際網路(含虛擬私有網路，VPN)遠端連線方式管理，如有特殊情形，需經機關資訊單位完成資通安全風險評估並完成必要防護措施，經由資通安全長簽署同意後始得辦理，且每年應至少重新評估及簽署一次，上開評估、簽署之過程及結果，應保留書面或電子紀錄備查。
識別與鑑別	1. 使用者應具備識別及鑑別之唯一性，禁止使用共用帳號，並應識別及鑑別非機關使用者。 2. 使用預設密碼登入系統時，應於登入後要求立即變更。 3. 身分驗證相關資訊不以明文傳輸。 4. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 5. 目錄服務網域管理者帳號、特權帳號及維運廠商帳號之密碼強度，密碼長度應十二個字元以上，包含英文大小寫、數字及特殊字元；目錄服務網域使用者帳號

	之密碼強度，密碼長度應八個字元以上，包含英文大小寫、數字及特殊字元。 6. 密碼最短效期為一日，最長效期為九十日。 7. 密碼變更時，不得與前三次使用過之密碼相同。
事件日誌與可歸責性	1. 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 2. 確保目錄服務有記錄特定事件之功能，並決定應記錄之特定系統事件。 3. 應記錄目錄服務管理者帳號所執行之各項功能。 4. 應定期審查機關所保留資通系統產生之日誌。 5. 日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一之日誌紀錄機制，確保輸出格式一致性。 6. 目錄服務於日誌處理失效時，應對機關特定之人員或角色提出告警。 7. 對日誌之存取管理，僅限於有權限之使用者。 8. 應運用雜湊或其他適當方式之完整性確保機制。 9. 應至少每日備份日誌至原系統外之其他實體系統(如日誌伺服器)、儲存媒體或資通安全威脅偵測管理中心(SOC)。
營運持續計畫	1. 應訂定系統最大可容忍中斷時間(MTPD)、復原時間目標(RTO)及資料復原時間目標(RPO)，以及原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。 2. 應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性，並將備份還原作為營運持續計畫測試之一部分。
系統與資訊完整性	1. 目錄服務主機(含跳板機) 應每月執行修補更新，如有重大安全性更新且有資通安全疑慮時，應配合即時完成更新。 2. 每年執行一次主機弱點掃描及每二年執行一次滲透測試，如經檢測有發現安全性漏洞，應立即修補，且漏洞修復應測試有效性及潛在影響。 3. 目錄服務應監測攻擊與未經授權之連線或使用者，如發現有被入侵跡象時，應立即完成日誌及相關跡證保全，採取必要阻絕防護措施，並依資通安全事件通報及應變辦法進行通報。