軍網目錄服務系統發展指導要點

中華民國 109 年 07 月 14 日國通資安字第 1090149722 號令頒
中華民國 112 年 10 月 13 日國通軟資字第 1120280772 號令頒

一、為發展軍網目錄服務系統之準據，以因應未來發展趨勢，並作為後續全軍導入雲端通用服務之整合平台，特訂定本要點。

二、適用範圍

（一）人員：國防部及所屬機關(構)、部隊、學校所屬官、士、兵及聘僱人員、友軍（同駐營區、任務編組）、合約廠商（長期進駐、駐廠、技代）等，運用軍網公務電腦執行公務者。

（二）伺服主機與電腦：各單位建置連接軍網之伺服主機、行政公務電腦、資訊教室多人共用訓練電腦等。

三、名詞定義

（一）網域（Domain）：網域是一個由網路系統管理員所定義的電腦集合，包含人員帳號、個人電腦、工作站、伺服器、儲存設備、印表機等資訊設備，並共用一個通用目錄資料庫，以簡化管理工作，統一集中管控，強化網路資訊安全。

（二）網域樹狀目錄（Domain Tree）：指一或多個網域組成的階層結構，具有父系與子系、上下階層之關係，形成一個連續的名稱空間，網域間彼此信任。

（三）樹系（Forest）：由一或數個網域樹狀目錄組成，共用一般架構、設定及通用類別目錄，網域間為雙向遞移信任關係。

（四）群組（Group）：為使用者、電腦、連絡人及其他組集合；群組用於資源存取授予，同時可發布電子郵件發布清單。

（五）組織單元（Organization Unit,OU）：為使用者、群組、電腦及其他組織單元邏輯容器；OU 為最小領域或單位，可對指派群組原則設定或委派系統管理授。

四、權責劃分

（一）國防部參謀本部通信電子資訊參謀次長室（以下簡稱通次室）

1.負責國軍目錄服務發展整體規劃。

2.負責國軍目錄服務根網域（mil.tw）管理。

3.負責軍網使用單位目錄服務系統部署與管理。

4.指導國軍各級單位目錄服務系統整合規劃與部署。

5.負責訂頒全軍目錄服務整合介面標準規範。

6.稽核各軍種目錄服務系統。

7.各司令部及國防部直屬機關（構）或幕僚單位網路磁碟區部署之核定。

（二）國防部各幕僚單位

1.配合國防部目錄服務系統架構，負責所屬目錄服務人員帳號、權限管理。

2.負責單位所屬公務電腦導入目錄服務系統。

3.負責排除所屬目錄服務系統使用問題。

（三）各司令部、國防部直屬機關（構）

1.依據國軍目錄服務系統整合發展指導、標準，規劃

部署所屬目錄服務系統。

2.配合國軍資訊（安）政策指導，執行目錄服務系統精進、整合、測試與運用。

3.督導、管制所屬目錄服務系統部署與管理。

4.所屬單位網路磁碟區部署之核定。

五、系統發展原則

（一）軍網目錄服務系統為單一樹系架構，頂層網域為mil.tw，各司令部（指揮部）現行網域樹狀目錄，管理所屬目錄服務系統，與國防部網域建立信任關係，俾整合人員授權及資源存取。

（二）目錄服務系統之人員帳號及電腦帳號，建置於不同組織單元（示意圖如附件一）。

（三）軍網公務電腦名稱及使用者帳號等命名原則(如附件二)，由各司令部(指揮部)、國防部直屬機關(構)或幕僚單位、部隊及學校統一律定。

（四）目錄服務系統之組織單元及使用者群組，為便於管理應適當命名，並委派所屬單位執行存取授權及管理作業。

（五）目錄服務系統人員基本資料，應與國軍人事資料庫整合，確保人員帳號最新動態。

（六）目錄服務系統之組織單元架構依據組織編制，採階層式（如司令部、軍團、指揮部單位）管理模式向下發展。

（七）各單位建置之目錄服務系統，均應與國軍智慧卡整合，

通次室提供整合介面標準。

（八）各單位部署網路磁碟區、即時通訊系統及單一登入架構等資訊服務，優先考量與國防部網域帳號資源結合。

（九）單位若因任務特性，自行建置目錄服務機制者（區域內網），部署計畫呈報國防部核備。

六、系統管理原則

（一）各級目錄服務系統管理人員，應統一管控所屬公務電腦管理權限，公務電腦使用人員僅核配一般使用權，避免人員任意更改設定、安裝軟體，杜絕惡意程式入侵風險。

（二）各單位業管目錄服務系統，建立高可用性備援機制，確保資訊服務不中斷。

（三）目錄服務系統建立帳號及資源權限管理機制，避免不當及未經授權存取行為。

（四）軍網目錄服務系統使用者帳號建立，配合國軍智慧卡運用，以人員身分為主，結合國軍人事資料同步即時異動，避免採用職稱為帳號；演習、值班輪值席位分以席位、使用者帳號為主。

（五）共駐營區友軍、非編制內使用人員（其他約聘、廠商駐點人員）等，須使用軍網公務電腦者，由僱用、契約業主單位配賦目錄服務系統使用者帳號，納入收容範圍，全程管制使用權限，另共駐營區友軍單位，仍應依編制隸屬納入軍種目錄服務系統管控及帳號使

用，惟系統連線所需網路通訊協定，應以公文協調開通。

（六）軍網目錄服務系統應負責人員身分認證及服務存取授權，各單位開發各類新資訊系統時，應將目錄服務系統納入規劃，以達系統帳號、密碼及權限一致性。

七、網路磁碟區運用原則

（一）網路磁碟存取控制應依國軍資訊安全政策存取控制規範，建立完善帳號權責管控規範及檔案傳輸稽核機制，確保資料安全。

（二）檔案均應運用國軍加解密軟體加密，始得上傳網路磁碟區。

（三）網路磁碟交換區應區分單位建置，各單位資料僅供內部交換使用，不得全面開放，並落實定期清整。

八、軍網即時通訊系統運用原則

（一）全面禁止檔案傳輸，僅得實施文字訊息傳遞。

（二）禁止傳送密級以上訊息。

九、稽核及其他

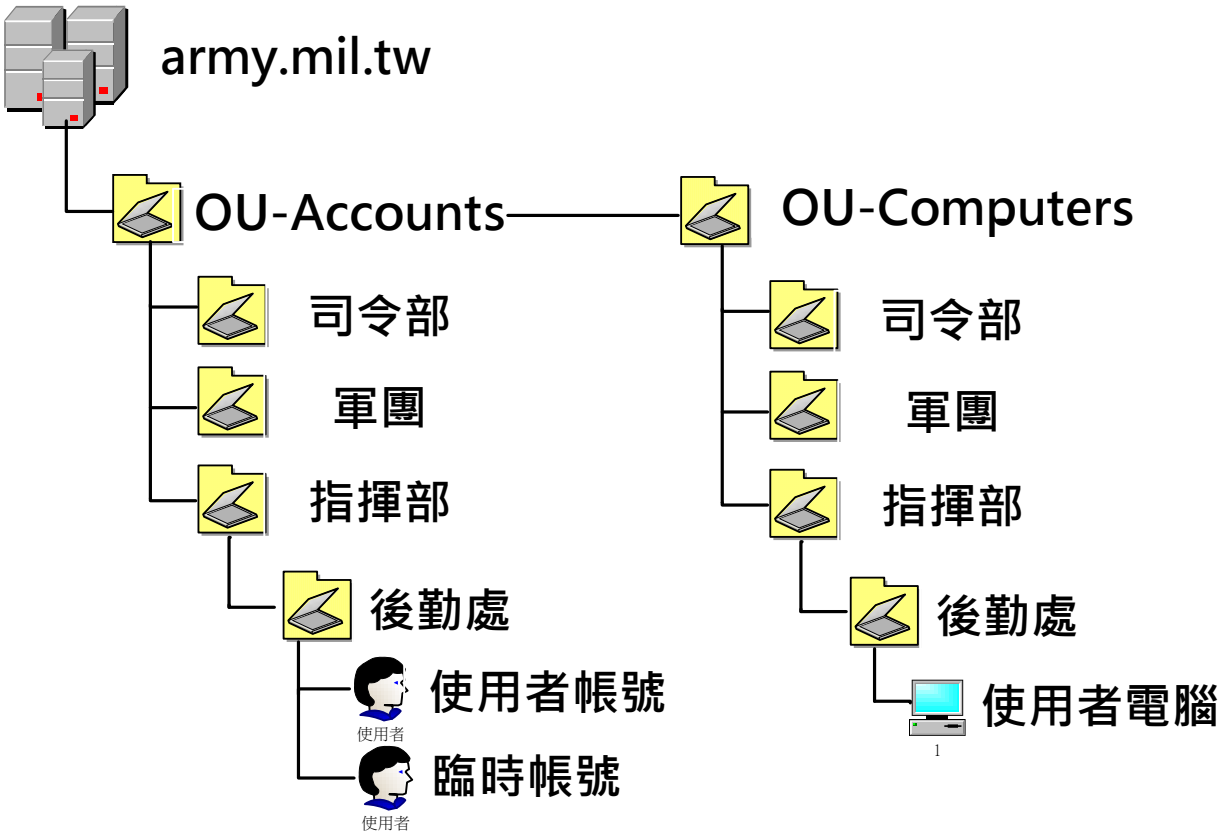
（一）違反本要點規範事項者，依國軍資通安全獎懲規定相關規定檢討懲處。

（二）國防部配合年度通電資系統整備等各類督導時機，稽核各單位目錄服務系統、網路磁碟區及軍網即時通訊系統部署與管理情形。

（三）各司令部、國防部直屬機關（構）針對所屬目錄服務系統、網路磁碟區、軍網即時通等發展、管理或運用

得配合資訊（安）政策訂定管理作業規定。

附件一 人員及電腦帳號建置示意圖



附件二 使用者帳號及電腦名稱命名原則

類別	命名原則規範
使用者帳號	1. 軍網行政用帳號統一以身分證字號為主，演習、值班區域之帳號以席位名稱訂定。 2. 不同之使用者帳號應配賦不同之普通名稱（CN, Common Name），普通名稱統一以 9 碼訂定。 a. 第 1~3 碼：網域名稱。 b. 第 4~6 碼：流水編號，並以 0~Z 表示。 c. 第 7~9 碼：流水編號，並以 0~9 表示。
電腦名稱	1. 一般電腦名稱格式分為三段，長度 12~14 碼。 a. 第一段：軍種、單位英文簡稱，長度 2~4 碼。 b. 第二段：IP 位址後 class B、C，以 0 補足 6 碼。 c. 第三段：網路卡位置末 4 碼，字母大寫。 d. 範例：通次室電腦 IP：10.22.144.248 網卡位址：60-A4-4C-E7-A8-E3，電腦名稱應為 CEI022144A8E2。 2. 伺服器電腦名稱區分三段以「-」符號區分。 a. 單位代碼:軍種或單位。 b. 網域名稱:伺服器提供服務網域名稱(FQDN)。 c. 單位管制編號:長度 0-3 碼英數。 d. 範例：國防部即時通伺服器叢集，伺服器電腦名稱分別為：MND-SFB-01、MND-SFB-02、MND-SFB-03。