「臺北市政府目錄服務管理要點」逐點說明

規定	說明
名稱：臺北市政府目錄服務管理要點	訂定法規名稱。
壹、總則	一般性總則規範。
一、臺北市政府(以下簡稱本府)為規範本府所屬公務機關及受監督之行政法人目錄服務之建置、維運及資通安全防護，依資通安全責任等級分級辦法第十一條第二項規定，特訂定本要點。	本要點之訂定目的為規範本府所屬公務機關及受監督之行政法人目錄服務之建置、維運及資通安全防護作為。
二、本要點主管機關為本府資訊局（以下簡稱資訊局）。	說明本要點之主管機關。
三、名詞定義 (一)公務機關：指依本府組織自治條例第六條至第八條設置之局、處、委員會、區公所，及依上開機關組織規程、組織自治條例設置之次級機關、學校及臺北市立大學。 (二)行政法人：指依行政法人法及本府自治條例設置之行政法人。 (三)資訊單位：指依臺北市政府各機關資訊組織及人力管理作業要點，各機關資訊業務專責一級單位、資訊業務專責二級單位、資訊推動任務編組或資訊業務主辦單位；行政法人準用上開規定，指定主辦資訊業務權責單位。 (四)目錄服務(Directory Service)：指遵循 LDAP(Lightweight Directory Access Protocol)和 X.500協定，儲存、組織和提供使用者、電腦和其他共享資源存取服務之軟體系統，包括但不限於微軟 Microsoft Active Directory、Linux LDAP Server。	重要名詞定義。

規定	說明
(五)TPEAD 目錄服務：指由資訊局整合建置、管理及維運之目錄服務。 (六)個人電腦（PC, Personal Computer)：指由終端使用者直接操控之資通設備，包括桌上型電腦、筆記型電腦及平板電腦。 (七)自攜設備（BYOD,Bring Your Own Device)：指各機關員工或廠商人員，為連接本府網路，處理資訊與使用應用程式而使用之非屬各機關資產之資通設備。 (八)核心資通系統：指各機關依資通安全管理法施行細則第七條第二項定義支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。 (九)政府組態基準(GCB, Government Configuration Baseline)：指由數位發展部所制定，規範資通訊設備(如個人電腦、伺服器主機及網通設備等）的一致性安全設定(如密碼長度、更新期限等)。 (十)共通性軟體：指由資訊局提供各機關，執行資訊作業或資通安全維護所必要之軟體或軟體元件。	
貳、目錄服務設置	目錄服務設置規範。
四、本府目錄服務採向上集中原則。除依本要點規定專案報准者外，各機關不得建置其他目錄服務。	說明目錄服務採向上集中為原則，各機關未經專案報准不得自設。
五、各機關有設置目錄服務，資通安全責任等級應為 C 級以上；如屬跨機關(含所屬機關)使用，資通安全責任等級應為 B 級。各機關資通安全等級如不符前開規定時，應依資通安全責任等級分級辦法第三條第六項規定	說明設置目錄服務之各機關，資通安全責任等級應為 C 級以上；若提供跨機關(含所屬機關)使用，則資通安全責任等級應為 B 級。

規定	說明
辦理等級變更。	
六、目錄服務如提供各機關任一核心資通系統進行使用者認證或應用服務，則應連帶列為核心資通系統。	說明目錄服務列為各機關核心資通系統之認定方式。
七、具目錄服務之機關應至少辦理工作事項如附表。	說明目錄服務之機關應參照附表辦理工作事項。
八、各機關新增目錄服務，應事前提送目錄服務建置計畫，經資訊局審查同意，始得辦理採購及其他建置程序，目錄服務建置計畫書應包括目錄服務設置原因、管理能力及人力、實體結構、目錄結構、資通安全防護措施等說明。第六點至第七點所列相關措施，於目錄服務啟用時同時完成。	說明自建目錄服務之各機關應送審建置計畫及完成相關應辦事項。
九、各機關測試環境之目錄服務，相關實體設備及其連接之所有裝置(包括但不限於個人電腦、伺服器主機)如均位於封閉性網路內，並與公務網路系統作實體隔離，經資訊局審查同意，得不適用前第五點至第八點規定	說明目錄服務測試環境與正式環境區隔方式。
參、網域設定	網域設定規範。
十、TPEAD 目錄服務採單一網域架構，網域名稱為 TPEAD，根網域為 TPEAD.GOV.TW。各機關個人電腦應加入 TPEAD 網域，自攜設備或因其他事由無法加入 TPEAD 網域或須加入其他網域之個人電腦，應造冊提交資訊局列管備查。	說明未加入 TPEAD 網域之各機關電腦應造冊列管。
十一、TPEAD 目錄服務為提升資通安全防護能力，減少資通安全漏洞及風險，不得與其他目錄服務建立信任關係（Trust Relationship）。	說明 TPEAD 目錄服務不與其他目錄服務建立信任關係。
十二、加入 TPEAD 網域之個人電腦於每次使用時，均應登入網域，惟因工作	說明加入 TPEAD 網域之個人電腦，每周至少一次登入

規定	說明
區域、網路環境或作業性質無法常態登入時，得採周期登入方式辦理。登入次數每周以不少於一次為原則，並應配合資訊局之政府組態基準設定或共通性軟體遠端部署作業登入更新。	網域以確保部署共通性軟體及政府組態基準設定。
十三、資通安全責任等級 B、C 及 D 級機關，應指定 TPEAD 網域機關管理者及其代理人，負責各機關個人電腦加入至 TPEAD 網域或自 TPEAD 網域移除作業；資通安全責任等級 E 級機關，該移除作業由其上級機關、監督機關或上級機關指定之機關兼辦或代辦。	說明各機關之 TPEAD 網域機關管理者及其代理人之指定。
十四、個人電腦加入 TPEAD 網域前，其主機名稱應依照本府資訊設備命名規則，並依資訊局規定及要求安裝資通安全防護及管理軟體。	說明加入 TPEAD 網域之電腦名稱、安裝資通安全防護及管理軟體。
肆、政府組態基準及共通性軟體部署	政府組態基準及共通性軟體部署規範。
十五、加入 TPEAD 網域之個人電腦，政府組態基準設定及共通性軟體之安裝及更新由資訊局使用 TPEAD 目錄服務進行遠端部署。	說明加入 TPEAD 網域之個人電腦，其政府組態基準設定及共通性軟體之安裝及更新由資訊局遠端部署。
十六、未加入 TPEAD 網域或無法使用 TPEAD 目錄服務進行遠端部署之個人電腦，政府組態基準設定及共通性軟體如有安裝及更新需求，由資訊局提供相關資料或檔案，各機關應自行完成部署或安裝，若未涉及資通安全風險者，應於次一工作天起二周內完成，若涉及資通安全風險者，應於次一工作天內完成，並回報資訊局。 政府組態基準設定及共通性軟體安裝及更新是否涉及資通安全風險及其緊急程度，由資訊局依個案認定及通知。	說明未加入 TPEAD 網域之個人電腦，其政府組態基準設定及共通性軟體之安裝及更新由資訊局提供資料或檔案予各機關自行部署。