文件編號	ISMS-207-01	存取控制管理要點	版本	2.0

1.依據.....1

2.目的 1

3.範圍.....1

4.權責.....1

5.定義.....1

6.作業規範.....1

7.相關資料.....5

8.附件暨使用表單.....6

9.角色權責分配表.....6

文件編號	ISMS-207-01	存取控制管理要點	版本	2.0

1. **依據**

1.1 行政院頒定之『行政院及所屬各機關資訊安全管理規範』

1.2 財政部頒定之『財政部暨所屬機關(構)資訊安全管理準則』

2. **目的**

為確保財政部財政資訊中心暨各地區國稅局(以下簡稱各機關)資訊作業其所運用之系統與資料的存取權限經適當的授權及控管，以防止不當存取。

3. **範圍**

各機關資訊作業須經授權存取之系統與資料。

4. **權責**

依據『資訊安全組織管理要點』附件1、資訊安全工作執行執掌表。

5. **定義**

5.1 系統

泛指作業系統、系統軟體、應用系統、套裝軟體、資訊安全軟體。

5.2 使用者

泛指各機關內部人員與外部人員(內部人員與外部人員之定義參照『人力資源安全管理要點』)。

5.3 密碼(Password)

係指『ISO 27001』與『CNS 27001』標準所提之「通行碼(Password)」。

6. **作業規範**

6.1 存取控制管理原則

6.1.1 系統與資料之使用須經授權，且其存取權限之設定應以作業所需之最小權限為原則。

6.1.2 對於使用者應建立適當之角色或群組，並對該角色或群組設定存取權限。

6.2 使用者存取管理

6.2.1 帳號管理

6.2.1.1 各系統之使用者帳號與管理者帳號(或較高作業權限之帳號)應視業務與資訊作業需求，運用相關管理程序申請適當角色或相關系統權限，並經權責主管審核通過後(各機關得視需求建立相關角色或系統權限設定參考資訊，例如依照其單位性質來規劃角色與群組、群組與系統(程式)間的預設關係)，得由系統自動設定其角色與權限或交由各系統(程式)管理者建置相關資料，職務異動之權限調整亦同。帳號異

動(含申請及註銷)應保留紀錄。

6.2.1.2 若因作業需求，須由委外廠商持有系統管理者帳號，系統負責人應考量操作系統之安全需求，由系統負責人代為申請或註銷帳號，對委外廠商執行之作業採取適當審核與確認。

6.2.1.3 人員調、離職之帳號異動作業應依據『人力資源安全管理要點』辦理。

6.2.1.4 如需保留帳號之系統資訊，供相關稽核作業運用，無使用需求之人員(含離職人員)帳號應採鎖定或其他安全管制措施。

6.2.1.5 應避免使用共用帳號，如有特殊控管限制或考量需使用共用帳號，須經相關權責主管同意。

6.2.2 密碼管理

6.2.2.1 密碼設定時系統應主動辨識，其長度應為 8 碼(含)以上，且須為數字與英文字母混合，如系統允許應再與特殊字元組合。

6.2.2.2 密碼如係由系統或相關承辦人員預設，應告知使用者於首次使用系統時進行變更，或由系統強制執行。

6.2.2.3 密碼更改時，新密碼不得與前 5 次重複，至少每 90 天更換 1 次，系統可設置一定期間的緩衝期，以防止使用者長時間未登入系統，未及變更密碼而導致帳號被鎖定；稅務資料庫密碼至少每 180 天變更一次；如不涉及稅務資料之工具軟體所使用的帳號，得不執行定期變更密碼。

6.2.2.4 如為特定系統因功能限制，密碼設定與更改作業無法完全符合前項要求，得經相關權責主管核准，調整該系統之密碼設定要求或密碼變更頻率。

6.2.2.5 使用者忘記密碼時，應先確認使用者身分後，再重設密碼。

6.2.2.6 針對可存取敏感等級以上資料之系統，得依業務需求考量採取帳號與密碼認證以外之身分認證機制(如：數位憑證等)。

6.2.3 權限審查

6.2.3.1 各機關權責主管應管制管理者帳號數量，僅授予合法管理者及其代理人，並每半年至少審查 1 次，註銷不適切之權限。

6.2.3.2 使用者帳號應建立適當稽核機制，每年至少檢視 1 次存取權限適當性。

6.2.4 使用者(含管理者)存取管理相關控管措施依『存取管理作業規範』辦理。

6.3 使用者責任

6.3.1 使用者之密碼應妥善保管，避免他人知悉。

6.3.2 避免使用與個人有關資料（如：英文名字、生日、身分證字號、單位簡稱、電話號碼、車牌等）作為密碼。

6.3.3 應取消系統或瀏覽器之密碼自動記憶功能，避免密碼遭擷取或竊用。

6.3.4 放置於辦公區域之無人看管設備，應考量辦公區域特性，採取適當的實體安全保護措施，如：妥善安置、上鎖、設置適當系統存取控制或適當標示等。

6.3.5 使用者離開電腦設備時，應關閉電腦螢幕電源或啟動電腦鎖定功能，以確保資料之安全。若超過 15 分鐘未使用電腦，須設定螢幕密碼保護或強制登出措施。

6.3.6 使用者離開辦公區域時，其辦公區域存放之資料，應依據『資訊資產暨風險管理要點』辦理。

6.4 網路存取控制

6.4.1 網路服務申請及規範

6.4.1.1 為確保資訊傳輸的安全，禁止使用未經授權之網路設備及線路，若有違反規定之行為，則依各機關相關規定進行懲處。

6.4.1.2 因業務與資訊作業需求而有網路服務(含內部網路與網際網路相關服務，如：申請 IP、SSL VPN 帳號、遠距工作 防火牆規則開通等)使用需求者，應依據相關管理程序申請，經權責主管核准後交承辦單位辦理。另入侵偵測與防禦機制之調整異動應參照『網路防禦設備管理作業規範』辦理。

6.4.1.3 使用期限超過 1 年之防火牆規則、委外廠商使用 IP、SSL VPN 帳號等網路服務申請，應每年定期覆核。

6.4.2 網路區隔

6.4.2.1 內部網路與網際網路採實體隔離，任何連線設備均不得同時連通內部網路與網際網路。

6.4.2.2 為便於管理，防止不當網路存取行為與流量散佈，應區分伺服器主機與一般使用者工作之電腦，賦予適當網路區段，以協助網路存取控制管理。

6.4.2.3 應依據各機關資訊作業之網路服務需要，區隔出獨立的邏輯網段，確保核心主機與重要資料(例如敏感等級以上資料)之安全。

6.4.2.4 應將對外網際網路連線服務予以適當存取控制，防止重要資料(例如敏感等級以上資料)外洩、避免不當網路資源運用或降低遭惡意攻擊之機會。

6.4.2.5 處理敏感等級以上資料(例如：稅務資料或個人資料)之電腦，應落實網路隔離或採用適當控管機制(例如限制對外網際網

路連線或建立適當監控機制)。

6.4.2.6 禁止同仁使用私有設備與各機關網路介接。委外駐點廠商如因業務上需要申請對外網路，須經各機關管理單位許可，使用時嚴禁同時連結稅務網路。

6.4.3 網路選路(Routing)與頻寬管理

6.4.3.1 內部網路存取行為應透過各機關網路設備與專屬線路，對外網路存取行為須經由對外專屬線路，並受到相關網路安全管控機制監控與管理。

6.4.3.2 應建立網際網路內容瀏覽限制，定期審議並建立網站過濾規則性。

6.4.3.3 外部網路禁止使用即時通訊相關軟體及點對點(Peer-to-Peer，P2P)分享軟體。

6.4.3.4 應進行網路流量之監控，保障網路頻寬之正常使用。

6.4.3.5 如發現流量異常，應立即採取適當措施後，分析網路異常原因。如為使用者非法使用或發生電腦病毒感染事件，應依據『資訊安全事故管理要點』進行通報，並通知相關人員進行後續處理。

6.4.4 網路連線管理

6.4.4.1 依照各網路介面用途及通訊協定，設定存取控制清單，以便進行存取控制。

6.4.4.2 關閉網路設備(例如路由器、交換器、集線器及防火牆等)不必要之服務與通訊協定。

6.4.4.3 網路線路異動須經權責主管核可後始可施工，並須同步更新網路佈線圖。

6.5 作業系統存取控制

6.5.1 調整系統安全設定，以滿足使用者存取管理要求。

6.5.2 使用者帳號應具唯一識別性與鑑別性，並避免共用帳號。

6.5.3 取消、停用匿名帳號。

6.5.4 定期審查並刪除多餘不用之帳號與群組。

6.5.5 依各資料夾(目錄)之用途，設定適當使用權限。

6.5.6 應關閉所有網路資源分享與服務，如有特殊控管限制或需求，需使用網路資源分享服務，須經權責主管同意。

6.5.7 啟用稽核原則(如：登入失敗之稽核)，保留相關稽核紀錄。

6.5.8 依據系統特性設定會談期逾時(Session Time Out)時間。

6.5.9 登入處理敏感等級以上資料之系統後，若超過時限無任何動作時，系統須設定將其帳號鎖定或登出。

6.5.10 各機關系統主機與個人電腦之公用程式由資訊單位統一控管，軟體之安裝管理依據『遵循性管理要點』辦理。

6.6 應用系統存取控制

6.6.1 應依據『應用系統獲取、開發及維護管理要點』辦理，於限制存取的應用系統(程式)，應採取身分認證(例如帳號、密碼)或其他身分鑑別機制，並對處理敏感等級以上資料之系統採用適當隔離措施或其他控管措施。

6.6.2 重要應用系統可限制連線或使用時間。

6.7 可攜式設備與通信

6.7.1 可攜式設備之安全管控措施參照『通訊與作業管理要點』辦理。

6.8 遠端連線存取控制

6.8.1 使用遠端桌面遙控(如： PC Anywhere、SmartIT、TeamViewer 等)或遠端登入軟體(如：ssh)管理主機、伺服器或 PC，應經權責主管核准後方可使用，使用過程中應啟動加密功能或採取其他適當管控措施。

6.9 遠距工作

6.9.1 經各機關評估業務需求得予以開放運用，惟其相關安全控管措施規劃應考量到遠距工作環境／設備之實體安全、遠距工作之通信安全(例如網路通訊應採用適當加密機制)及遠距工作所需系統與相關運用資料之存取安全等。

7. 相關資料

7.1『資訊安全組織管理要點』
7.2『資訊資產暨風險管理要點』
7.3『人力資源安全管理要點』
7.4『通訊與作業管理要點』
7.5『應用系統獲取、開發及維護管理要點』
7.6『遵循性管理要點』
7.7『存取管理作業規範』
7.8『網路防禦設備管理作業規範』

8. 附件暨使用表單

無。

9. 角色權責分配表

存取控制管理作業主要活動角色權責分配表(A- Accountable 負責角色、R- Responsible 執行角色、C- Consulted 受諮詢角色、I- Informed 被告知角色)：

負責單位 資安工作事項	申請單位承辦人員(含使用者)	申請單位主管	資訊單位承辦人員(含系統負責人、網路安全管理員與網路管理員)	資訊單位主管
使用者帳號管理	R	A	I	I
管理者帳號管理	R	R	R	A
權限審查	R	R/A	C	C
使用者密碼保管	R/A	I	I	I
網路存取控制	R/I	R/I	R	A
作業系統存取控制	R/I	R/I	R	A
應用系統存取控制	R	A	I	I
行動計算安全管控	R/I	R/I	R	A
遠端連線存取控制	R/I	R/I	R	A