文件編號	NCHU-ISMS-B-009	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	4.0	發行日期	111.04.21

資訊安全存取管理辦法

機密等級:**一般**
文件編號:**NCHU- ISMS-B-009**
版　次:**4.0**
初版日期:**96.12.13**

文件制修訂紀錄			
修訂日期	修訂人員	修訂內容摘要	版次
96.12.13	陳建平	初版	1.0
98.8.18	陳建平	文件版型調整	2.0

文件編號	NCHU-ISMS-B-009	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	4.0	發行日期	111.04.21

文件制修訂紀錄			
修訂日期	修訂人員	修訂內容摘要	版次
105.11.08	葉宏	修訂文件編號 文件名稱刪除「計算機及資訊網路中心」 修訂1.目的 改為本校 修訂2. 適用範圍 改為全校 修訂4. 權責 新增 3.1. 秘密鑑別資訊 修訂5.1. 存取控制政策5.2. 使用者註冊與註銷5.3. 使用者存取權限之配置5.4. 具特殊存取權限之管理5.5. 使用者之秘密鑑別資訊的管理5.6. 使用者存取權限的定期審查5.7. 存取權限之移除或調整5.8. 秘密鑑別資訊之使用責任5.9. 資訊存取限制5.10. 系統保全登入程序5.11. 通行碼管理系統5.12. 具特殊權限公用程式之使用5.13. 程式原始的存取控制5.14. 密碼式控制措施(加密控制措施) 5.15. 金鑰管理5.16. 密碼式控制措施(加密控制措施)的法規遵循5.17. 遠距工作5.18. 存取事件紀錄的管理	3.0
111.04.21	賴怡君	配合教育體系資安規範進行, 修改整本程序條文規範。	4.0

文件編號	NCHU-ISMS-B-009	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	4.0	發行日期	111.04.21

文件編號	NCHU-ISMS-B-009	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	4.0	發行日期	111.04.21

1. 目的

確保國立中興大學(以下簡稱本校)對資訊系統的存取權限均經適當的授權及維護, 以防止不當存取。

2. 適用範圍

本辦法適用本校提供資訊服務存取所需之作業相關資訊系統與網路, 包括作業平台、資料庫、應用系統、校園網路、遠距存取服務及各種網路設備等。

3. 名詞定義

3.1. 秘密鑑別資訊

係指用於確認使用者身分的機制, 密碼/通行碼(password)為常見資訊, 其他包含加密金鑰資訊(cryptographic keys), 或存放在智慧卡(Smart card)等硬體符記(Hardware tokens)上的鑑別資訊等。

3.2. 靜態密碼

系統登入時所使用, 以文字、數字或特殊字元組成由系統自動產生或人工設定之密碼。

3.3. 一次性密碼

密碼僅供一次登入或認證使用, 由系統自動產生或人工設定下一次登入之密碼, 密碼不能重複。

4. 權責

4.1. 主機/資料庫/應用系統管理者

4.1.1. 負責主機群組、帳號管理作業。

4.1.2. 定期審查主機使用者存取權限。

4.1.3. 執行主機密碼管理作業。

4.2. 網路管理者

4.2.1. 負責網路設備帳號及密碼管理作業。

4.2.2. 定期審查網路設備使用者存取權限。

4.3. 資料擁有者(單位)

4.3.1. 審查使用者存取權限。

4.3.2. 公務資料之蒐集或利用, 應尊重當事人之權益, 依誠實及信用方法為之, 不得逾越公務目的之必要範圍。

4.4. 應用系統使用者。

4.4.1. 應用系統規劃、上線與管理。

4.4.2. 應用系統主機管理與保管。

5. 要求事項

5.1. 存取控制政策

5.1.1. 存取控制政策宜考量下列事項:

(1) **營運應用系統的安全要求與風險**。

(2) **資訊傳播和授權政策, 以及資訊的安全等級與分級**。

(3) **不同系統與網路間存取控制與資訊分級政策的一致性**。

(4) 有關保護資料或服務存取的適當法規及所有的契約責任與義務。
(5) 存取控制角色的區隔與特權存取管理，資訊存取權限之設定以工作所需之最小權限與最少資訊為原則。
(6) 存取權限申請與授權程序。
(7) 存取控制措施定期（宜每半年）審查的要求。
(8) 存取權限的移除。
(9) 關於使用者身分和安全鑑別資訊之使用和管理的重要事件歸檔。

5.1.2. 存取控制若以角色為基準(Role-based Access Control)，對於權限之申請以加入各種角色為原則，避免對個別使用者或帳號進行授權。

5.2. 秘密鑑別資訊之使用

5.2.1. 施行單位於使用秘密鑑別資訊(如通行碼、加密金鑰或憑證資訊等)時，應要求使用者遵循單位之規定。使用者宜：
(1) 維持秘密鑑別資訊的機密性，確保不洩露給包括授權人員的任何一方。
(2) 避免保留秘密鑑別資訊的紀錄（例如：在紙張、軟體檔案或手持裝置），除非其能被安全地存放，且該存放經過核准（例如：密碼庫）。
(3) 只要秘密鑑別資訊有可能遭受破解的跡象，宜立即更改。
(4) 不要與他人共用個人的秘密鑑別資訊。
(5) 自動登入程序中內含秘密鑑別資訊做為機密鑑別資訊並儲存時，宜確保適當地保護通行碼。
(6) 公務與非公務使用目的勿使用相同秘密鑑別資訊。

5.3. 使用者註冊與註銷

5.3.1. 對於多人使用的資訊系統，建立正式的使用者註冊程序。

5.3.2. 使用者註冊管理程序，宜考量：
(1) 查核使用者是否已經取得使用該資訊系統的正式授權。
(2) 查核使用者被授權的程度是否與業務目的相稱，以及符合資訊安全政策與規定。
(3) 以書面或其他方式告知使用者系統存取權利。
(4) 要求使用者簽訂約定，使其確實了解系統存取的各項條件及要求。
(5) 在系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。
(6) 宜建立及維持系統使用者之註冊資料記錄，以備日後查考。

(7) 使用者調整職務及離(休)職時，宜盡速註銷其系統存取權利。
(8) 宜定期(宜每半年)檢查及取消閒置不用的識別碼及帳號。
(9) 閒置不用的識別碼不宜重新配予其他的使用者。

5.4. 使用者存取權限之配置

5.4.1. 使用資訊系統或服務的授權流程，應實作正式之使用者存取權限配置程序。

5.4.2. 查證存取等級授與的適當性，且符合存取政策及職務區隔等要求。

5.4.3. 確保授權程序完成後才開啟存取權限。

5.4.4. 維護資訊系統與服務之使用者存取權限紀錄。

5.4.5. 變更角色或工作的使用者須立即調整其存取權限；已離開施行單位的使用者宜立即移除或封鎖其存取權限。

5.4.6. 資訊系統或服務的擁有者宜定期(宜每半年)審查存取權限，並依規定進行帳號清查，系統管理者將查核結果紀錄呈各權責主管審查。

5.5. 具特殊存取權限之管理

5.5.1. 嚴格管制系統存取特別權限。

5.5.2. 針對有必要特別保護的系統，賦予使用者系統存取特別權限，並依下列的授權程序管理：

(1) 宜確認系統存取特別權限之事項，例如作業系統、資料庫管理系統、應用系統、需賦予系統存取特別權限的人員名單，並由權責主管應審查其合適性。
(2) 宜依執行業務的需求，視個案逐項考量賦予使用者系統存取特別權限；系統存取特別權限之配予，宜以執行業務及職務所必要者為限。
(3) 宜建立申請系統存取特別權限之授權程序，並只能在完成正式授權程序後，才能配予使用者；另外，宜將系統存取特別權限之授權資料建檔。

5.6. 管理者及操作者日誌

5.6.1. 宜忠實記錄系統啟動及結束作業時間、系統錯誤、更正作業及建立日誌條目的人員或程序等事項，限定僅由系統管理者或具讀取權限者存取。

5.6.2. 作業人員的系統作業紀錄，宜定期交由客觀的第三者檢查。

5.7. 遠距工作

5.7.1. 本機關資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有需求，應填寫「遠端連線申請單」，經相關權責主管核准後，執行權限開放。

5.7.2. 針對遠距工作之連線應採適當之防護措施，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。

5.7.3. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

5.8. 具特殊權限公用程式之使用

5.8.1. 應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。關於具有特殊權限之系統公用程式的管理宜:

5.8.1.1. 嚴格限制及控管電腦公用程式之使用。

5.8.1.2. 制訂公用程式之安控措施，如:

(1) 設定使用者密碼以保護系統公用程式。

(2) 將系統公用程式與宜用系統分離。

(3) 將有權使用系統公用程式的人數限制到最少的數目。

(4) 建立臨時使用公用程式的授權制度。

(5) 限制系統公用程式的可用性，例如變更公用程式的使用時間授權規定。

(6) 記錄系統公用程式的使用情形，備日後考察。

(7) 訂定系統公用程式的授權規定。

6. 參考文件

6.1. 網路安全管理辦法。

6.2. 資訊應用系統安全防護設計及管理辦法。

6.3. 資訊安全文件暨紀錄管理辦法。

6.4. 教職員工電子郵件帳號申請表。

6.5. 遠端連線申請單。

6.6. 帳號清查紀錄表。

6.7. 帳號清查結果報告。