

# NDDS系統因應資安法 使用者有感之相關功能調整說明

吳宏德 STPI副技術師

2019/11/27



# 依據

- 資通安全管理法(以下簡稱資安法)
  - 為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。
  - 107年5月11日 立法院完成三讀
  - 107年6月6日 由總統公布
  - 107年11月21日 公告「資通安全責任等級分級辦法」
  - 108年1月1日 正式施行，並應於一年內完成「應做項目」
- NDDS 被評定  
資通系統安全等級➡中級



# 安全控制措施

依「資訊系統分級與資安防護基準作業規定」  
中級系統需包含：6個構面、58項控制措施

構面	控制措施類別	NDDS實作措施(普+中)	使用者有感項目
存取控制	帳號管理 / 最小權限 / 遠端存取	10(2+8)	4
稽核與可歸責性	稽核事件 / 稽核紀錄內容 / 稽核儲存容量 / 稽核處理失效之回應 / 時戳及校時 / 稽核資訊之保護	12(8+4)	-
營運持續計畫	系統備份 / 系統備援	5(2+3)	-
識別與鑑別	內部使用者之識別與鑑別 / 身分驗證管理 / 鑑別資訊回饋 / 加密模組鑑別 / 非內部使用者之識別與鑑別	11(8+3)	9
系統與服務獲得	系統發展生命週期需求階段 / 系統發展生命週期設計階段 / 系統發展生命週期開發階段 / 系統發展生命週期測試階段 / 系統發展生命週期部署與維運階段 / 系統發展生命週期委外階段 / 獲得程序 / 系統文件	13(9+4)	-
系統與通訊保護	傳輸之機密性與完整性 / 資料儲存之安全	-	-
系統與資訊完整性	漏洞修復 / 資通系統監控 / 軟體及資訊完整性	7(2+5)	-



# 識別與鑑別

~密碼複雜度

## ■ 控制措施

- 基於密碼之鑑別，資通系統應  
強制最低密碼複雜度

## ■ NDDS因應方式

- 密碼複雜度  
自設密碼應強制最低密碼長度及複雜度原則
  - 新讀者/館員
    - 密碼長度8~20個字元
    - 至少須包含英文字母大寫+小寫+數字
    - 但 < > " ' % ; ( ) + 等特殊字元與空格不可使用
  - 既有讀者/館員
    - 密碼未符合長度及複雜度原則之使用者，  
於登入後要求立即變更密碼



# 識別與鑑別

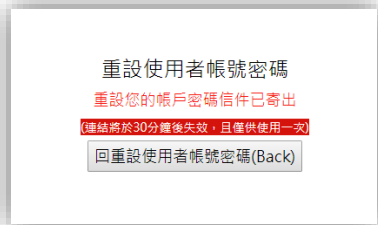
~密碼重設機制

## ■ 控制措施

- 使用**預設密碼**登入系統，應於登入後要求**立即變更**
- 身分驗證相關資訊，不以明文傳輸
- 密碼重設機制對使用者重新身分確認後，發送**一次性**及具有**時效性**符記

## ■ NDDS因應方式

- 密碼重設機制
  - 系統寄送重設密碼通知信至註冊 email
  - 點選 email 中之重設密碼連結(時效性 $\leq 30$ 分鐘)
  - 連結驗證成功
    - 依照網頁提示輸入新密碼，並需符合密碼原則
  - 連結失效
- 超過30分鐘操作
- 已執行成功過重設密碼



# 存取控制

~閒置帳號&逾期連線

## ■ 控制措施

- 已**逾期**之臨時或緊急**帳號**應刪除或**禁用**
- 資通系統**閒置帳號**應禁用
- **逾越**機關所定**預期間置時間**或可使用期限時，系統應自動將使用者登出

## ■ NDDS因應方式

- 逾期使用
  - **30分鐘未活動**之連線，自動登出
- 閒置帳號
  - 2年未登入之使用者
  - 閒置帳號登入後，需**重設密碼再登入**後方能使用

NDDS使用者您好，因應資安需求，館員首次啟用帳號、使用者密碼設定不符原則或2年內未登入本系統者，請按確定並依畫面提示重新設定您的密碼，造成不便，敬請見諒。

確定



NDDS 全國文獻傳遞服務系統

STPI 科技政策研究與資訊中心

重設密碼

密碼 Password

(密碼長度8~20個字元，至少須包含英文大小寫字母及數字，但 < > " ' % ; ( ) + 等特殊字元與空格不可使用)

密碼確認 Password confirm

(密碼長度8~20個字元，至少須包含英文大小寫字母及數字，但 < > " ' % ; ( ) + 等特殊字元與空格不可使用)

送出(Submit)



# 識別與鑑別

~身分驗證管理

## ■ 控制措施

- 帳號登入進行身分驗證**失敗達3次**後，至少**15分鐘**內不允許該帳號繼續嘗試登入
- 身分驗證機制應**防範自動化程式**之登入或密碼更換嘗試

## ■ NDDS因應方式

- 具備**帳戶鎖定**機制
  - **失敗達3次** ➔ **鎖15分鐘**
- **防範自動化程式**登入

 [文獻查詢 / 申請](#) Search / Order

期刊聯合目錄 Union List of Serials

CONCERT電子期刊聯合目錄 Union List of Electronic Journals

全國圖書目資訊網 NBINet (National Bibliographic Information Network)

METACAT+即時跨館整合查詢

臺灣期刊論文索引系統 PerioPath Index to Taiwan Periodical Literature System

臺灣博碩士論文系統 National Digital Library of Theses and Dissertations in Taiwan

博碩士論文(STPI館藏 1994~2004) Dissertations & Theses

學術會議論文(1988~2009) Conference Papers

國科會研究報告(1971~2001) NSC Research Reports

政府研究資訊系統(GRB) Government Research Bulletin

 使用者登入

請輸入讀者或館員帳號

密碼

請輸入圖片中的文字

4436

您連續輸入三次錯誤密碼，帳號已鎖定，請15分鐘後再試

登入 Log in

申請帳號  
Create an  
Account

忘記密碼  
Forgot  
Password

新單位註冊 New Library Register

新合作聯盟註冊 New Union Register

# 識別與鑑別

~加密模組鑑別

## ■ 控制措施

- 資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存

## ■ NDDS因應方式

- 加密時以SALT機制添加亂數
  - 相同的內容加密結果卻不相同，以防堵加密結果回推破解
  - 加密項目：  
使用者密碼、姓名、身分證字號



簡報結束

敬請指教

