# 教育部國民及學前教育署所轄高級中等以下學校

# 資通系統及資料庫主機資通安全及資料備份提醒事項

**112.01.31**

## 壹、系統備份、資料備份及檔案備份(應立即落實辦理)

一、教育部國民及學前教育署所轄高級中等以下學校(以下簡稱學校)資通系統及資料庫主機因蒐集多項師生個人資料,且多涉及學生權益(如:校務行政系統、學習歷程檔案),學校應落實資訊安全防護措施,並應定期備份資料,資料庫及學生上傳檔案務請落實備份作業,為避免硬體故障毀損,備份資料不可與原始資料放在同一個磁碟上,另外為了避免勒索病毒攻擊時將原始資料與備份資料一同被加密,備份資料(**包含資料庫及上傳檔案**)需要離線保存,以下就自動化、人工作業分別提供備份建議做法:

(一)自動化作業:備份至其他電腦或 NAS 時,應至少備份 3 代以上,每日確認備份作業是否成功。

(二)人工作業(**備份檔案離線存放**):可準備兩個 USB 隨身碟或行動硬碟等,先檢視主機需備份資料是否正常,備份檔案拷貝及加密後,拔出電腦妥善保管。建議至少每週一次,輪流進行以上步驟。

(三)應定期規劃備份還原演練作業,以確認備份資料有效性。

二、NAS 的安全防護

(一)現行 NAS 都有管理系統,以方便使用,因此系統也要定期更新,以避免系統漏洞未及時修補,讓駭客有可趁之機。

(二)應該停用系統內建的最高權限管理員帳號(如 admin),以自建的帳號代替。最高權限管理員帳號的密碼應有一定複雜度,並定期更換,例如:至少 8 碼以上,英數字均有。

(三)通常 NAS 內建有防火牆,建議設定開啟;並檢查 NAS 預設提供的網路服務,請關閉不必要的服務。

(四)定期檢查 NAS 的磁碟狀態,避免硬碟損壞數量超過磁碟陣列容錯能力而未更換,進而造成資料損失。

(五)目前許多 NAS 支援直接備份到雲端空間 (Google Drive、Microsoft

OneDrive、Dropbox、其他外部儲存空間)，但請特別注意資料安全性。由於雲端儲存空間常有被攻擊而洩露資料之事件發生，因此未加密之資料，不應備份到雲端；如果要備份到雲端，就應先進行檔案加密，加解密金鑰請勿一併置於雲端空間，應妥善保管於學校端。

三、系統安全

(一) 學校資通系統(例如：學習歷程、校務行政系統)及資料庫主機之作業系統應定期升級及更新。Windows Server 至少應為 Windows Server 2012 r2 (2023 年 10 月終止支援)，建議 Windows Server 2019 或 2022；MS SQL Server 至少應為 MS SQL 2014 (2024 年 7 月終止支援)，建議 MS SQL 2017 或 2019 的版本；Linux 依其分散版本，建議使用長期維護版本，且應在維護期間內。

(二) 學校資通系統(例如：學習歷程、校務行政系統)及資料庫主機之作業系統內建防火牆應完整啟用，並只開放有使用到之服務埠，且安裝有防毒軟體(Windows 可用 Defender 或其他防毒軟體，Linux 可以使用之 Anti-Virus Software)。伺服主機上軟體安裝以最小化為原則，即除所提供服務必須要用到的軟體外，不應隨便安裝應用軟體，更不應當成工作站或個人電腦使用。

(三) 學校資通系統(例如：學習歷程、校務行政系統)及資料庫主機之服務連線，包括 WEB 服務、FTP 服務(不應使用無加密之 FTP 服務)、資料庫連線等均應啟用 TLS 1.2 以上之協定(Protocol)，並應關閉 SSL 所有版本(1.0、2.0、3.0)，及 TLS 1.0、1.1。

(四)教學行政用個人電腦應與伺服主機分置於不同網段，並經過防火牆過濾，如果可以，建議資料庫主機與伺服主機也區分為不同網段，作適當的隔離；伺服主機及資料庫網段應僅開放特定電腦可以連線維護。

(五)學校防火牆規則設定，建議採取預設封鎖(拒絕)規則，並以最小化設定服務開放，有關防火牆建置參考指引請參考行政院國家資通安全會報技術服務中心共同規範 (https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh)；由於 SMB 協定有多種已知高風險漏洞，若有需要要使用，應僅提供校園內部網路使用，並僅啟用 SMBv3，關閉 SMBv2 及 SMBv1 協定。學校防火牆對外及各網段間均不應開啟 SMB 協定相關服務埠(服務埠：137、138、

139 及 445)。

(六)學校資通系統及資料庫主機建議放置於學校機房，機房進出應有嚴格管制及紀錄，並配有不斷電系統。如果條件許可，建議採用虛擬化技術，將校務系統、學習歷程及資料庫主機改為虛擬機器(Hyper-V 或 VMware)；國立高級中等以下學校五大核心資通系統(學校官方網站、網域名稱服務（DNS）、電子郵件伺服器、校務行政系統、學生學習歷程系統)及資料庫主機則應配合政策以向上集中至指定機房為原則。

貳、常見備份機制與週期之錯誤樣態及具體建議作法

| | 備份機制與週期之錯誤樣態 | 具體建議作法 |
|---|---|---|
| 一 | 作業系統、資料庫系統版本過舊 | 主機/伺服器之作業系統應定期升級及更新，以符資安需求。 |
| 二 | 備份方式為「無備份」 | 學校應立即啟動備份機制並執行備份，建議先行調配校內可用之電腦(若已無主機/伺服器可先以一般桌上型電腦)，或善用國教署前於109年補助學校購置之NAS儲存裝置進行異機備份，且應指派專人每日檢核及確認備份作業皆落實執行。 |
| 三 | 備份資料之儲存硬碟非磁碟陣列組(RAID 1、RAID 5 或以上) | 若備份主機無磁碟陣列，建議至少要有2至3份之備份於不同實體磁碟。 |
| 四 | 資料備份模式項目學校只勾選「差異備份」或「增量備份」，而未勾選「完整備份」 | 備份機制應包含完整備份及差異(增量)備份，請學校確認備份設定(第1次差異(增量)等於是完整備份）。 |
| 五 | 資料備份方式為「同機同碟」 | 建議至少應有異機備份。 |
| 六 | 備份週期(頻率)為「每月」 | 建議資料庫每週1次完整備份，附件檔每日1次差異或增量備份。 |
| 七 | 備份資料保存期程過短 | 若設備容量許可，建議保留至少3代完整備份，備份檔案可保留約30-45天(每週1次完整備份至少需保留21天、每2週1次完整備份則須保留約45天)，各 |

| | | |
|---|---|---|
| | | 校請依學生人數及設備容量彈性調整。 |

參、異地備份其他注意事項

一、現採用 NAS 儲存設備之備份方案，資料上傳時需要先使用帳號進行登入方可傳輸，並於資料傳輸完成後登出；請學校及廠商準備具有帳號登入及登出之資料備份排程程式或腳本，以達到接近離線備份之運作機制。

二、如將登入之帳號密碼寫在排程程式或腳本內，帳號密碼資訊勿以明文存放。

三、備份資料須於傳輸前進行加密，如備份後須透過程式進行解密，解密資訊勿以明碼存放於程式內。