題號	評量項目	佔分	自評項目	準備資料或客觀證據
六、資通安全風險評估				
	08.依據資通安全維護計畫，學校應完成資通訊(產)相關之風險分析評估及處理；並評估結果擬定因應控制措施。(2 分)	2 分	已完成 未逾限	準備資料或客觀證據： 相關文件或風險評估表
學校	1.依據「風險類型暨風險對策參考表」填寫資通風險評估表，並核章。			

南投縣仁愛鄉仁愛國民小學—資通安全風險評估表

編號：

製表日期：109 年 11 月 16 日

項次	資產名稱	類別	擁有者/職稱	機密性(C)	完整性(I)	可用性(A)	資訊資產價值(C, I, A 取最大值)	發生可能性/威脅等級(T)	脆弱等級(V)	風險值 資訊資產價值*(T*V)
1.	學校防火牆 NA361R	實體資產	蔡永瑩/網管	3	2	2	3	3	2	18
2.	UniFi Switch 48	實體資產	蔡永瑩/網管	1	1	1	1	1	2	2
3.	UniFi Switch 24	實體資產	蔡永瑩/網管	1	1	1	1	1	2	2
4.	UniFi Switch 24	實體資產	蔡永瑩/網管	1	1	1	1	1	2	2
5.	UniFi Switch 24	實體資產	蔡永瑩/網管	1	1	1	1	1	2	2
6.	UniFi Switch 24	實體資產	蔡永瑩/網管	1	1	1	1	1	2	2
7.	D-Link DGS-1210-	實體資產	蔡永瑩/網管	1	1	1	1	1	2	2
8.	D-Link DGS-3210-	實體資產	蔡永瑩/網管	1	1	1	1	1	2	2
9.	群暉 Synology	實體資產	蔡永瑩/網管	3	2	2	3	2	2	12
10.	午餐食材盤點系統	軟體資產	林雪苓/午秘	2	2	2	2	2	2	8
11.	出納支票系統	軟體資產	曾意珊/出納	2	2	2	2	2	2	8

承辦人員：教師蔡永瑩　單位主管：教師兼教導主任高裕明　資安長：南投縣仁愛國小校長沈慧美

風險類型暨風險對策參考表

南投縣仁愛鄉仁愛國民小學風險類型暨風險對策參考表

風險類型暨風險對策參考表		
作業內容	具體風險類型	風險處理對策（建議，例示非列舉）
網際網路探尋	網頁搜尋	強化網頁伺服器，避免存放 index.html、default.asp 的檔案資料夾，並禁用相關的目錄索引。使用 robots.txt 指示搜尋引擎不要為其內容編制索引。
	WHOIS 查詢	在 WHOIS 資料庫及 TLS 憑證中，使用平常、單一的網路管理人聯絡資訊，以降低社交工程與撥號攻擊的成功率。
	DNS 查詢	設定 DNS 伺服器，禁止其對不可信任的主機執行區域轉送，並主動從網際網路掃描 TCP 和 UDP 的端口 53，以便發現是否有偽冒的名稱伺服器。刪減 DNS 區域檔案內容，以防洩漏不必要的訊息，例如非公開的 IP 位址和主機名稱，並且於必要時才使用 PTR 紀錄。
	SMTP 探尋	設定 SMTP 伺服器在遇到問題時，例如寄件人不存在時，不要發送 NDN，以防攻擊者藉機列舉內部郵件系統及組態內容。
區域網路攻擊	MITM 和偽冒伺服器攻擊	強制採用傳輸層安全加秘與透過具有憑證檢驗功能的身份驗證機制
	802.1X 攻擊	●檢測 X.509 憑證是否有效。 ●指定合法驗證者（RADIUS 伺服器）之一般名稱值。 ●在安全功能發生問題時，禁止提供詳細資訊給終端使用者，以提高故障安全性。
	資料連結層攻擊	●將交換連接埠設為 access 模式，並關閉動態建立主幹網路的功能。 ●關閉未用到的乙太網路連接埠，並歸類在隔離的 VLAN 外。
	網路層與應用層的攻擊	●如果沒有明確要求，應關閉 IPv6。 ●取消對 ICMP 重導向的支援。 ●停用群播名稱解析及 Windows 的 NetBIOS over TCP/IP 通訊。
網路服務漏洞	網路攻擊表面	將不必要的功能關閉。
	伺服器套件包與程式庫攻擊	隨時修補存在攻擊表面的已知攻擊。
	透過傳輸與遠端維護操作之服務進行攻擊	●停用無加密傳輸安全性的 Telnet、FTP、SNMP、VNC 等。 ●遠端操作維護須透過安全的身份驗證連接。 ●建構封閉的管理網路。
	SSH 伺服器攻擊	●強制使用 2.0 版本的協定，禁止向下相容特性。 ●停用使用者的密碼驗證機制，強制使用者採取一次性密碼（OTP）、公鑰或多因子驗證，例如可透過 Google Authenticator、Duo Security 或其他平台取得。

	DNS 伺服器攻擊	●停止支援來自不受信任來源的遞回查詢。 ●確保區域檔案不含多餘或敏感資訊。
	Kerberos 伺服器攻擊	●停止支援較弱的 HMAC 演算法。 ●在微軟環境中，可考慮強制使用最高的網域功能等級。
郵件服務	SMTP 攻擊	不要將多功能的 SMTP 伺服器公開到網際網路或不受信任的網路。
	不受信任郵件的攻擊	●使用 SPF、DKIM 和 DMARC 防止伺服器傳輸或接收未經授權的內容。 ●將對外的 SMTP 介面設定成不接受偽冒的內部網路郵件。 ●配置外部內容過濾機制。
	防毒軟體弱點攻擊	應及時更新病毒碼與維持版本最新。
	電子郵件帳戶攻擊	●建議在用戶端增加一層憑證式的驗證機制。 ●強制郵件伺服器使用強密碼政策。 ●紀錄郵件服務身份驗證失效的日誌，應制定帳號鎖定原則。
VPN 服務	VPN 攻擊	●確認 VPN 伺服器的維護作業，並修補到最新版本。 ●強制使用 AH 和 ESP 功能身份驗證及機密性服務。 ●使用數位憑證取代預置共享金鑰，並要求對設備進行身份驗證。 ●過濾內連的 VPN 流量，以便在發生入侵事件時限制網路存取。 ●定期稽核已授權的 VPN 使用者，以防有偽冒的帳號。
網頁應用程式框架	Web 應用伺服器攻擊	●確保應用程式框架組件都已修補至最新版本，包括相依與間接使用的組件。 ●禁止將管理介面或特權功能公開在不受信任的網路上。 ●在可行的情況下，將開放網頁應用程式和管理功能隔離。
資料儲存機制	資料庫攻擊	●限制資料服務只與經授權的對象往來，特別是雲端環境中。 ●避免使用不支援身份驗證的儲存系統和協定。 ●禁止在可公開讀取的儲存裝置，例如 NFS、iSCSI、SMB 和 AFP 等，以未加密狀態儲存機敏資料，包括系統和資料庫的備份檔案通常存有機敏資料，例如密碼、身份憑證。 ●確保密碼強度。 ●限制只有受信任的網路才能存取管理服務。 ●稽查和監控身份驗證事件，識別濫用身份憑據和暴力拆解密碼的情形。

參考來源：資安風險評估指南，第三版，Chris McNab，江湖海譯。