

# 白河區白河國中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、單一的網路管理人員聯絡資訊，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密與透過具有憑證檢驗功能的身份驗證機制
	802.1X 攻擊	<ul style="list-style-type: none"> <li>● 檢測 X.509 憑證是否有效。</li> <li>● 指定合法驗證者（RADIUS 伺服器）之一般名稱值。</li> <li>● 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。</li> </ul>
	資料連結層攻擊	<ul style="list-style-type: none"> <li>● 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。</li> <li>● 關閉未用到的乙太網路連接埠，並歸類在隔離的 VLAN 外。</li> </ul>
	網路層與應用層的攻擊	<ul style="list-style-type: none"> <li>● 如果沒有明確要求，應關閉 IPv6。</li> <li>● 取消對 ICMP 重導向的支援。</li> <li>● 停用群播名稱解析及 Windows 的 NetBIOS over TCP/IP 通訊。</li> </ul>
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	隨時修補存在攻擊表面的已知攻擊。

	與程式庫攻擊	
	透過傳輸與遠端維護操作之服務進行攻擊	<ul style="list-style-type: none"> <li>● 停用無加密傳輸安全性的 Telnet、FTP、SNMP、VNC 等。</li> <li>● 遠端操作維護須透過安全的身份驗證連接。</li> <li>● 建構封閉的管理網路。</li> </ul>
	SSH 伺服器攻擊	<ul style="list-style-type: none"> <li>● 強制使用 2.0 版本的協定，禁止向下相容特性。</li> <li>● 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。</li> </ul>
	DNS 伺服器攻擊	<ul style="list-style-type: none"> <li>● 停止支援來自不受信任來源的遞回查詢。</li> <li>● 確保區域檔案不含多餘或敏感資訊。</li> </ul>
	Kerberos 伺服器攻擊	<ul style="list-style-type: none"> <li>● 停止支援較弱的 HMAC 演算法。</li> <li>● 在微軟環境中，可考慮強制使用最高的網域功能等級。</li> </ul>
VPN 服務	VPN 攻擊	<ul style="list-style-type: none"> <li>● 確認 VPN 伺服器的維護作業，並修補到最新版本。</li> <li>● 強制使用 AH 和 ESP 功能身份驗證及機密性服務。</li> <li>● 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。</li> <li>● 過濾內連的 VPN 流量，以便在發生入侵事件時限制網路存取。</li> <li>● 定期稽核已授權的 VPN 使用者，以防有偽冒的帳號。</li> </ul>
網頁應用程式框架	Web 應用伺服器攻擊	<ul style="list-style-type: none"> <li>● 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。</li> <li>● 禁止將管理介面或特權功能公開在不受信任的網路上。</li> <li>● 在可行的情況下，將開放網頁應用程式和管理功能隔離。</li> </ul>
資料儲存機制	資料庫攻擊	<ul style="list-style-type: none"> <li>● 限制資料服務只與經授權的對象往來，特別是雲端環境中。</li> <li>● 避免使用不支援身份驗證的儲存系統和協定。</li> <li>● 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。</li> <li>● 確保密碼強度。</li> <li>● 限制只有受信任的網路才能存取管理服務。</li> <li>● 稽查和監控身份驗證事件，識別濫用身份憑據和暴力破解密碼的情形。</li> </ul>
<p>參考來源：資安風險評估指南，第三版，Chris McNab，江湖海譯。</p>		

## 白河區白河國中 資通安全風險評估表

製表日期：109 年 02 月 14 日

項次	資產名稱	類別	擁有人/ 職稱	機密性 ◎	完整性 (I)	可用性 (A)	資訊資產 價值(T) (C,I,A 取 最大值)	潛在風險 事件	風險發生 可能性 (V)	風險值 資訊資產價 值*(V)
1.	個人電腦	實體 資產	全體教職 員	1	1	2	2	2.3.3	2	4
2.	行動裝置	實體 資產	全體教職 員	1	1	1	1	2.4.3	2	2
3.	可攜式媒體	實體 資產	全體教職 員	1	1	1	1	2.5.2	2	2
4.	學校網站	軟體 資產	資訊組	1	1	1	1	1.2.2	1	1
5.	網路交換器	實體 資產	資訊組	2	1	2	2	2.2.1	1	2
6.	教學組業務 相關檔案	資料 資產	教學組長	3	1	1	3	3.1.4	2	6
7.	設備組業務 相關檔案	資料 資產	設備組長	2	1	1	2	3.1.2	1	2
8.	資訊組業務 相關檔案	資料 資產	資訊組長	2	1	1	2	3.1.2	1	2
9.	生教組業務 相關檔案	資料 資產	生教組長	2	1	1	2	3.1.2	1	2
10.	體衛組業務 相關檔案	資料 資產	體育組長	2	1	1	2	3.1.2	1	2
11.	活動組業務 相關檔案	資料 資產	活動組長	3	1	1	3	3.1.4	2	6
12.	健康中心業 務相關檔案	資料 資產	護理師	3	1	1	3	3.1.4	2	6
13.	輔導組業務 相關檔案	軟體	輔導組長	2	1	1	2	3.1.2	1	2

項次	資產名稱	類別	擁有者/ 職稱	機密性 ◎	完整性 (I)	可用性 (A)	資訊資產 價值(T) (C,I,A 取 最大值)	潛在風險 事件	風險發生 可能性 (V)	風險值 資訊資產價 值*(V)
		資產								
14.	資料組業務 相關檔案	資料 資產	資料組長	2	1	1	2	3.1.2	1	2
15.	出納組業務 相關檔案	資料 資產	出納組長	2	1	1	2	3.1.2	1	2
16.	文書組業務 相關檔案	資料 資產	文書組長	2	1	1	2	3.1.2	1	2
17.	事務組業務 相關檔案	資料 資產	事務組長	2	1	1	2	3.1.2	1	2
18.	人事室業務 相關檔案	資料 資產	人事主任	3	1	1	3	3.1.4	1	3
19.	會計室業務 相關檔案	資料 資產	會計主任	2	1	1	2	3.1.2	1	2