附件一

高雄市橋頭區仕隆國小
資通安全推動小組成員及分工表

編號：

製表日期：　　年　　月　　日

單位職級	職別	業務事項	分機	備註（代理人）
校長	資通安全長	綜理資通安全核定與督導	10	
資訊執秘	資安策略規劃與管理組	資通安全事務協調、資通安全維護計畫、資通安全事件通報	90	
教務處主任	資安策略規劃與管理組	學生學習歷程系統成績資料安全與維護	20	
學務處主任	資安通報防護組	校務行政系統學生出缺勤、獎懲紀錄資料安全與維護	30	
總務處主任	資安通報防護組	資通安全設備招標採購	40	
人事室主任	資安通報防護組	差勤系統安全與維護、協助資通安全人員獎勵事宜	21	
會計室主任	資安策略規劃與管理組	協助資通安全預算編列與核銷	60	
各學年導師	資安策略規劃與管理組	進行學生資通安全宣導		

承辦人：　　單位主管：　　機關首長：

附件二

高雄市橋頭區仕隆國小
資通安全保密同意書

編號：

立同意書人＿＿＿＿＿＿於民國＿＿＿年＿＿＿月＿＿＿日起於＿＿＿＿任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。

二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：＿＿＿＿＿＿(簽章)

身份證字號：＿＿＿＿＿＿(後五碼)

單位主管(資通安全長)：＿＿＿＿＿＿

機關首長：＿＿＿＿＿＿

中　　華　　民　　國　　年　　月　　日

高雄市橋頭區仕隆國小
資通安全需求申請單

附件三

編號：

申請單位		**申請日期**	
申請項目	□軟體 □硬體 □服務 □其他	**項目名稱**	
申請數量		**需用日期**	
申請類別	□新增 □升級 □刪除	**使用設備**	□電腦（位置）____ □系統_____ □其他_____
用途說明			
申請人		**申請人 單位主管**	
審查結果		**審查說明**	
承辦人		**資通安全長**	

仕隆國小資訊及資通系統資產清冊

附件四

編號：

製表日期：　　年　月　日

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	防護需求等級	核心系統	備註
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

承辦人：　　主任：　　校長：

仕隆國小風險評估表

附件五

編號：

製表日期：　　年　　月　　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										
2										
3										
4										
5										
6										
7										
8										
9										
10										

資通系統防護需求分級原則

防護需求等級 構面	高=3	中=2	普=1
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

附件六

高雄市橋頭區仕隆國小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。

高雄市橋頭區仕隆國小管制區域人員進出登記表

文件編號：　　　　　　　　　　　　　　承辦人：　　　　　　　　　　　　附件七

製表日期：　　　　　　　　年　　　　月　　　　日

日期(民國年月日) 進入機房時間	事由	進出人員 簽名	陪同人員 簽名	請勾選	
				設備 新增/下架	攜入媒體
年　月　日 進入時間： 離開時間：		單位： 姓名：		□新增 □下架	□ 可攜式電腦 □ 可攜式儲存媒體，如磁片、光碟、隨身碟、外接式硬碟
年　月　日 進入時間： 離開時間：		單位： 姓名：		□新增 □下架	□ 可攜式電腦 □ 可攜式儲存媒體，如磁片、光碟、隨身碟、外接式硬碟
年　月　日 進入時間： 離開時間：		單位： 姓名：		□新增 □下架	□ 可攜式電腦 □ 可攜式儲存媒體，如磁片、光碟、隨身碟、外接式硬碟
年　月　日 進入時間： 離開時間：		單位： 姓名：		□新增 □下架	□ 可攜式電腦 □ 可攜式儲存媒體，如磁片、光碟、隨身碟、外接式硬碟

附件八

高雄市橋頭區仕隆國小委外廠商執行人員保密切結書

立切結書人_____（簽署人姓名）等，受_____（廠商名稱）委派至_____（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。

二、 未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、 經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、 廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。

五、 機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、 本保密切結書不因立切結書人離職而失效。

七、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章	身分證字號(後 5 碼)	聯絡電話及戶籍地址

立切結書人所屬廠商：

廠商名稱及蓋章	廠商負責人姓名及簽章	廠商聯絡電話及地址

填表說明：

一、　廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。

二、　廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

附件九

高雄市橋頭區仕隆國小委外廠商查核項目表

填表日期：　　年　　月　　日

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	□	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	□	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	□	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	□	□	□	指派副首長擔任資安長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	□	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	機關內部訂有資安責任分工組織。
3.配置適當之資通安全專業人員及適當之資	3.1 是否訂定人員之安全評估措施？	□	□	□	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	機關依規定配置資安人員2人。
	3.3 是否具備相關專業資安證照或認證？	□	□	□	專業人員具備ISO27001之證照

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
源	3.4 是否配置適當之資源？	□	□	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	□	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	□	□	□	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	□	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	□	□	□	機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	離職人員之權限未刪除。
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	□	□	對於進出人員並未監督其活動。
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	□	□	□	按時檢測機房物理面之情況。
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	□	□	□	依規定定期檢查並按時提供同仁安全設備之使用運練。
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	□	□	並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？	□	□	□	對於核心系統主機並未設置特別保護機制。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	□	□	□	定期檢查物理面之風險。
	5.9 電源之供應及備援電源是否作安全上考量？	□	□	□	有設置備用電源。
	5.10 通訊線路及電纜線是否作安全保護措施？	□	□	□	電纜線老舊，並未設有安全保護措施。
	5.11 設備是否定期維護,以確保其可用性及完整性？	□	□	□	設備按期維護。
	5.12 設備送場外維修,對於儲存資訊是否訂有安全保護措施？	□	□	□	訂有相關之保護措施。
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	□	□	□	攜帶式設備訂有保護措施。
	5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	□	□	□	設備報廢前均有進行資料清除程序。
	5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	□	□	人員下班後並未將機敏性公文妥善存放。
	5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	□	□	□	系統開發測試與正式作業區隔。
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	按時更新病毒碼。
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	定期進行相關系統之病毒掃瞄。
	5.19 是否定期執行各項系統漏洞修補程式？	□	□	□	定期進行漏洞修補。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	□	□	□	系統設有檢查之機制。
	5.21 重要的資料及軟體是否定期作備份處理？	□	□	□	有定期做備份處理。
	5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	備份資料均有測試。
	5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	□	□	□	均有設加密之保護措施。
	5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	□	□	□	訂有可攜式媒體之管理程序。
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	□	□	□	訂有使用者存取權限註冊及註銷之作業程序。
	5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	□	□	□	未定期檢視使用者存取權限。
	5.27 通行碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	□	□	□	通行碼符合規定。
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	通行碼符合規定。
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	□	□	□	依規定訂定適當之存取權限。
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	□	□	□	對於特定網路有訂定相關之控制措施。
	5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	□	□	□	有針對行動式電腦訂定管理政策。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.32 重要系統是否使用憑證作為身份認證？	□	□	□	針對重要系統設有身份認證。
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	□	□	□	系統更新後相關措施仍有效。
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	□	□	□	可即時取得系統弱點並採取應變措施。
6.訂定資通安全事件通報及應變程序及機制	5.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	有訂定通報應變程序。
	5.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	□	□	□	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	5.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	□	□	□	有留存相關紀錄。
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	□	□	□	有定期辦理宣導。
	7.2 是否對同仁進行資安評量？	□	□	□	按期進行資安評量。
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	□	□	□	有定期辦理教育訓練。
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	□	□	□	同仁均瞭解單位之資通安全政策及目標。
8.資通安全維護計畫實形進施之精善機制	8.1 是否設有稽核機制？	□	□	□	訂有稽核機制。
	8.2 是否定有年度稽核計畫？	□	□	□	有訂定年度稽核計畫。
	8.3 是否定期執行稽核？	□	□	□	有按期執行稽核。
	8.4 是否改正稽核之缺失？	□	□	□	訂有稽核後之缺失改正措施。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
9.資通安全維護計畫及實施情形之績效管考機制	10.1 是否訂定安全維護計畫持續改善機制？	□	□	□	有訂定持續改善措施。
	10.2 是否追蹤過去缺失之改善情形？	□	□	□	有追蹤缺失改善之情形。
	10.3 是否定期召開持續改善之管理審查會議？	□	□	□	定期召開管理審查會議。

查核人員：　　單位主管：　　資通安全長：

附件十

高雄市橋頭區仕隆國小資通安全教育訓練計畫

壹、 依據

高雄市橋頭區仕隆國小之資通安全維護計畫辦理。

貳、 目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行本校之資通安全維護計畫，以強化本校之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

參、 實施範圍

本校所屬人員：

人員類別	人數
一般使用者	
主管	
共計	

肆、 訓練項目

人員類別	訓練課程	時數
一般使用者		
主管		

伍、 訓練期程

由各校自行排定教育訓練期程。

陸、 訓練方式

由各校自行決定教育訓練方式(實體課程、線上課程...)。

附件十一

高雄市橋頭區仕隆國小資通安全認知宣導及教育訓練簽到表

課程名稱：

時　　間：

地　　點：

單　位	職　稱	姓　名	簽　名

附件十二

高雄市橋頭區仕隆國小資通安全維護計畫實施情形

依據教育部臺教資(四)字第 1080063464 號函文，本校為公立高級中等以下學校，且配合資訊資源向上集中計畫，資訊系統均由上級或監督機關兼辦或代管，其資通安全責任等級為 D 級第一類。依資通安全管理法第 12 條之規定，提出本（108）年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明 （下列內容為範例，請各校依自身情形填寫對應的說明，並提供證明，如計畫、程序、記錄或相關公文等）
1. 核心業務及其重要性	1.1 核心業務及重要性盤點	本校核心業務及重要性詳參資通安全維護計畫（詳附件）。
	1.2 非核心業務及說明	本校非核心業務及說明詳參資通安全維護計畫（詳附件）。
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本校已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定(詳公文附件)。
	2.2 資通安全目標之訂定	本校已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本校為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4 資通安全政策及目標定期檢視	本校已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性 (詳會議記錄) 。
3. 設置資通安全推動組織	3.1 設定資通安全長	本校已指定校長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本校已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。
4. 專責人力及經費之配置	4.1 專職(責)人員配置	本校依資通安全責任等級分級辦法之規定，屬資通安全責任

		等級 D 級第一類，設置一名正式人員兼辦資通安全業務。
	4.2 經費之配置	本校今年視需求已合理分配資安經費，資安經費佔資訊經費之○○%。
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本校已於今年 1 月盤點本校之資訊、資通系統，建立資產目錄。
	5.2 機關資通安全責任等級分級	本校依資通安全責任等級分級辦法，為資通安全責任等級 D 級第一類機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本校已於今年 1 月完成本校之資訊、資通系統及相關資產之風險分析評估及處理。 本校應每年針對資訊及資通系統資產進行風險評估，若配合資訊資源向上集中計畫，資訊系統均由上級或監督機關兼辦或代管，則不需進行。
	6.2 資通安全風險之因應	本校已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 資訊及通系統之保管	本校已依依安全維護計畫辦理，詳附件資料。(以下為未導入 CNS27001 機關之範例)
	7.2 存取控制與加密機制管理	本校已依安全維護計畫辦理。
	7.3 作業及通訊安全管理	本校已依安全維護計畫辦理。
	7.4 系統獲取、開發及維護	本校已依安全維護計畫辦理。
	7.5 執行資通安全健診	本校已依安全維護計畫辦理。
	7.6 資通安全防護設備	本校已依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本校已依規定訂定資通安全事件通報應變程序。(詳附件)
	8.2 資通安全事件通報、	本校已依規定進行資通安全事

	應變及演練	件通報。 本校已依規定於今年○月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	本校接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本校已接受情資之分類，採取對應之因應措施。
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	本校已依安全維護計畫辦理。
	10.2 監督受託者資通安全維護情形應注意事項	本校已依安全維護計畫辦理。
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本校人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本校已於今年○月辦理資通安全教育訓練。
12. 公務機關所屬人員辦理業務涉及資通安全事項之考核機制	12.1 訂定考核機制並進行考核	本校已建立考核機制，並已依規定進行平時及年終考核。
13. 資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1 資通安全維護計畫之實施	本校已依安全維護計畫辦理。
	13.2 資通安全維護計畫實施情形之稽核機制	本校已依安全維護計畫辦理。
	13.3 資通安全維護計畫之持續精進及績效管理	本校已依規定召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
其他說明		

單位主管：　　資通安全長：

附件十三

高雄市橋頭區仕隆國小稽核結果及改善報告

稽核範圍	
稽核日期	
審查日期	

改善措施				
編號	稽核缺失或待改善稽核項目	改善措施	改善期程規劃	相關證明資料
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

附件十四

高雄市橋頭區仕隆國小改善績效追蹤報告

製表日期：

稽核發現			
稽核日期	108 年 10 月 20 日 08 時	受稽核單位	○○○
稽核區域	■ 電腦機房 委外業務之監督措施 _ 自動備份系統之安全措施		
缺失或待改善項目與內容	待改善項目：電腦機房所設置之預備電源設備老舊。 缺失項目：委外廠商未定期為保養相關設備。		
影響範圍評估	將影響電腦機房之運作及相關非核心系統之線上服務之提供。		
發生原因分析	未落實監督委外廠商管理之責任。		

改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面	定期進行委外廠商承辦人員之教育訓練，已落實對委外廠商之監督責任。	要求委外廠商每季進行保養，並提供相關保養紀錄。	已與委外廠商接洽。
技術面			
人力面			

資源面	更新相關電腦機房設備，並確保備份設備及機制運作效果。	電腦機房電源設備更新，並採用不斷電系統，於停電時可維持 12 小時運作。	已進行採購作業。
作業程序			
其他			

績效管考			
改善措施確認	■合格／完成 □待追蹤(追蹤期限：_____年_____月_____日) □不合格(說明：_____)		
經費需求或編列執行金額	○○○萬元。	經費執行情形	已進行相關電腦機房設備更新採購，共執行○○萬元。
預定完成日期	108 年 11 月 20 日	實際完成日期	108 年 11 月 20 日
完成進度或情形說明	定期檢視委外廠商之監督維護責任。		
改善成效考核			
後續成效追蹤			
資通安全推動小組	○○○	資通安全長	○○○