BCCS 漢昕科技

離你最近的資安專家

國立臺南大學

委外廠商自評與委外系統管理注意事項教育訓練

一站式資安防護

講師：漢昕科技 顧問 郭家瑋

日期：2026/07/02

近期委外資安事件：廠商維護遭駭歷程

01. 憑證遭竊取

攻擊者透過社交工程或惡意軟體，成功竊取委外維護廠商的 **VPN 登入帳號與密碼**。

02. 合法登入系統

駭客利用取自廠商之 **VPN 帳密**，冒充維護人員，合法遠端登入機關內部網域與伺服器。

03. 個資外洩爆發

駭客進一步控制機關內部人員帳號，查詢並竊取敏感個資，導致 **3 級資安事件**。

建議防範措施與遠端存取控制

1. **落實原則禁止**：內部系統遠端維護應「原則禁止、例外允許」；若有需求必須取得正式授權。
2. **強化身分鑑別**：針對外部 VPN 遠端登入，應全面啟用 **MFA 多因子認證機制**，避免單一密碼遭破壞即遭入侵。

BCCS 漢昕科技
- 離你最近的資安專家 -

委外資安事件案例：永擎電子帳密外流事件

公司名稱

永擎電子股份有限公司

發布時間

115 年 1 月 22 日

事件說明

⚠ 起因：外包廠商帳密外流

經確認外流之帳密權限，僅限於官網資料、已公開資訊或須搭配特定硬體產品始能運作之產測程式。

◐ 排查：排除內伺服器遭入侵

受影響範圍不含機密文件、重大財務資訊或任何客戶與員工之個人敏感資料。

▦ 評估與後續：營運無重大影響

目前評估無重大影響，後續將持續密集監控，以確保整體資訊安全。

資安院 案號 S111004「委外要當心！電視台新聞片庫慘遭協力廠商刪除」

【 焦點話題 】

電視台新聞片庫遭刪除

- **起因**：內部缺乏資安人才，委請外部廠商建置全新儲存系統。
- **疏失**：廠商擅自安裝遠端軟體，且未經同意執行風險指令。
- **損失**：刪除近42萬份影片，僅救回部分，共**淨損失8.4萬份**。
- **處置**：進行專案報告，並委請律師研議後續求償。

【 重點摘要 】

履約義務與民事賠償

- **監督義務**：機關對於受託業務仍負有妥適監督之責。
- **給付不能**：履約過程中因可歸責於廠商之事由，導致契約無法履行。
- **加害給付**：不僅契約無法履行，更導致資料滅失之額外損害。
- **損害賠償**：依**民法第227條第2項**，廠商依法負有賠償責任。

【 法律分析 】

強化委外監管及稽核

- **資安漏洞**：機關常因預算與編制缺乏人才，因而高度仰賴委外。
- **嚴格管控**：不能因委外而降低安全標準，應落實日常監管與權限審查。
- **防範措施**：遠端存取應落實「原則禁止、例外允許」，並應啟用多因子驗證（MFA）。

資訊服務供應商遭駭後影響機關業務

供應鏈安全漏洞分析與遠端維護防禦對策

⚠ 供應鏈安全威脅與案例

常見攻擊模式

駭客常以委外資訊服務商為「跳板」入侵機關。委外人員若資安意識不足或未落實安全控制，極易成為防護最脆弱的一環。

機關遭駭案例

- **通道入侵**：利用廠商維護系統的遠端連線通道進行滲透。
- **加密勒索**：植入勒索軟體加密資通系統，導致業務運作停頓。
- **緊急應變**：立即中斷網路連線阻止擴散，並透過備份重建系統。

遠端維護安全管制指引

核心辦理原則

依據院臺護字第1100165761號函，遠端維護必須以**「原則禁止、例外允許」**方式嚴格控管。

具體加強防護措施

- **限時開放**：要求事先申請，且僅開放短天期之維護時間。
- **來源限制**：設定防護措施，嚴格限制特定存取來源位址。
- **雙重驗證**：強制要求登入時採用多因子驗證 (MFA) 等方式。
- **監控審計**：監控連線活動，要求廠商依防護基準保存與管理日誌。

課程大綱：四大核心模組

- 模組一：委外作業型態與常見風險
- 模組二：資安法規要求與開發防護基準
- 模組三：採購合約擬定與驗收管理
- 模組四：維運應變、測驗與交流

委外管理

Outsourcing Management

組織將部分業務、資訊系統或服務委託外部廠商執行時，所實施之全生命週期管理措施。

核心管理目標

- 確保資訊安全：防止敏感資料外洩
- 個人資料保護：加強個資隱私防護
- 法規遵循：符合主管機關合規要求

01
受託者選任
評估廠商資質、技術能力及安控水準。

02
契約簽訂
明定雙方權責、服務水準與罰則規範。

03
資安要求
訂定安全防護標準與機密資訊規範。

04
履約監督
執行日常作業監控、定期稽核與追蹤。

05
績效評估
定期考核服務指標，作為續約衡量基礎。

06
結案管理
妥善處理資產回收、資料銷毀與交接。

委外作業的定義與範圍

只要涉及外部廠商處理校內資料或維護設施，皆屬委外範疇。

01 主機系統與網路硬體維護

02 應用系統開發與軟體客製化

03 雲端 / 資料服務

04 專業資安顧問服務

委外範圍說明：主機系統與網路硬體維護

01 HOST & NET

針對校內核心主機作業系統與網路骨幹硬體之定期巡檢、故障排除、安全設定與弱點修補，確保基礎設施不間斷營運。

A. 主機系統營運維護

伺服器作業系統（OS）更新與優化、硬體資源監控、系統備份與還原機制驗證，確保核心主機高可用性。

B. 網路硬體與骨幹維運

防火牆（Firewall）、路由器、交換器配置與規則檢視，異常流量監控與即時阻斷，確保校內網路通訊暢通安全。

安全管理基準要求

外部維護廠商必須遵循「最小權限原則」登入，且所有遠端維護行為皆須留存完整軌跡（Log）以備稽核。

委外範圍說明：應用系統開發與軟體客製化

02 DEV & APPS

涵蓋新系統之「委外開發」與既有系統之「軟體功能客製化」，必須落實安全程式設計並融入資安要求，從源頭降低資安風險。

A. 安全軟體開發生命週期 (SSDLC)

於系統規劃與分析階段，即將資安要求納入規格，落實程式碼漏洞預防與安全架構設計。

B. 源碼檢測與弱點修補

交付前必須通過第三方弱點掃描、滲透測試與源碼檢測，修補中高風險漏洞，並出具無漏洞證明。

開發安全基準要求

廠商交付軟體前需依機關之安全規範完成壓力測試及系統漏洞掃描檢測，確認系統無重大安全危害。

委外範圍說明：雲端 / 資料服務

03 CLOUD & DATA

涵蓋校內「雲端服務」與「資料委外處理」，須確保基礎設施安全並防範敏感資料外洩。

- **SaaS** (軟體即服務)：免安裝、透過瀏覽器直接使用的應用軟體。
- **PaaS** (平台即服務)：提供開發、測試與部署應用程式的託管環境。
- **IaaS** (基礎設施即服務)：租用運算、儲存與網路等底層硬體資源。

A. 雲端平台安全管理

定期評估雲端服務商（CSP）資安認證與防護基準，針對虛擬網路、身分識別與存取權限進行安全配置與持續性合規監控。

B. 資料委外處理與加密防護

落實敏感資料傳輸與儲存加密，建立委外處理之資料存取軌跡追蹤，並於合約終止時確實執行資料返還、移轉或徹底銷毀驗證。

雲端安全基準要求

涉及核心業務或敏感個人資料委外處理時，應優先選用通過國際資安標準（如 ISO 27001 / ISO 27017）認證之雲端服務，並落實資料在地化規範。

委外範圍說明：專業資安顧問服務

04 SECURITY CONSULTING

引進外部專家資源，針對校內資訊安全管理系統（ISMS）進行規劃、建置與持續改善，並協助落實資安法合規與稽核準備，提升整體防護韌性。

A. 資安管理與合規顧問服務

協助評估資安法規符合度（如資通安全責任等級要求），規置ISMS管理體系（ISO 27001），提供定期成熟度評估、差異分析與持續合規之改善建議。

B. 威脅防禦與緊急應變諮詢

提供資安事件模擬演練（含社交工程、藍隊防禦演練）、緊急應變計畫（IRP）編修諮詢，並在發生重大資安威脅時提供關鍵決策與鑑識調查支援。

顧問服務執行基準

執行顧問諮詢服務之外部機構，其委派之主導顧問應具備相關專業資安證照（如 CISSP, CISA, ISO 27001 LA），以確保規劃與評估之專業性與合規品質。

委外常見風險與駭客手法分析

01 策略面風險

02 治理面風險

03 需求面風險

04 合約面風險

05 廠商面風險

駭客利用廠商合法的 VPN 帳號登入機關系統，進而查詢內部資料導致個資外洩。

只要個資外洩即屬「3 級資安事件」

資訊作業委外常見風險

Key Risk Domains in IT Outsourcing

lightbulb01 策略面

- 委外策略評估
- 核心業務識別

gavel02 治理面

- 管理制度建立
- 明確權責與稽核

assignment03 需求面

- 規格完整分析
- 資安與個資要求

history_edu04 合約面

- SLA品質水準
- 資安條款與NDA

business05 廠商面

- 能量評選與監督
- 防範單一依賴

ISO 27001:2022 對照

insights策略面

A.5.19 供應商關係資訊安全

description合約面

A.5.19、A.5.20、A.5.21 供應商安全要求

gavel治理面

A.5.20 供應商合約中的資訊安全

groups廠商面

A.5.22 供應商服務監控、審查與變更管理

assignment需求面

A.5.8 專案管理資訊安全

verified_user對照指引

落實委外生命週期各階段的資安防護與合規

策略面 · ISO控制項說明

策略面概述

資訊作業委外服務之型態、範圍及管理方式等整體策略之評估與規劃，旨在事前識別組織的核心能力與關鍵業務，避免盲目將不適合的系統委派外部維運。

A.5.19 供應商關係資訊安全

組織應與供應商協商並記錄資訊安全要求，以減輕與供應商存取組織資產相關的風險：

- **委外可行性評估**：明確定義哪些核心資產與營運流程不可委外。
- **供應商關係原則**：建立健全的供應商准入評估與全生命周期策略。

控制項落實建議 (A.5.19)

在策略規畫階段，應由高階主管與資安團隊共同落實以下措施以符合合規要求：

- **核心業務識別**：鑑別不適合委外之核心技術，降低單一廠商依賴度。
- **制定退場機制**：於合約前規劃替代方案，防止因廠商倒閉陷入僵局。

案例分析：委外評估不足之風險

因人力不足而草率委外，未考量業務重要性與系統自主權，將面臨巨大的營運中斷風險。

真實案例

學校校務系統委外維護

學校將核心校務行政系統完全交由A公司維護，五年後該廠商不幸倒閉，導致：

- **無法取得程式碼**：系統無法進行任何後續維護。
- **系統文件不完整**：交接困難，新團隊難以接手。
- **無法更換廠商**：技術綁定嚴重，陷入維護僵局。
- **全校行政受阻**：日常行政作業遭受重大影響。

可能影響

忽視風險評估，將對組織內部運作產生連鎖性的致命打擊：

關鍵業務中斷

- 核心行政與業務系統停擺，導致服務癱瘓。

技術受制於廠商

- 喪失資訊主導權，完全依賴單一廠商的配合度。

系統移轉成本高

- 在無程式碼與文件的狀況下，重建系統需耗費鉅資。

建議控制措施

應建立以下防護網，落實委外生命週期的風險控管：

委外可行性評估

- 事前評估業務重要性與潛在風險。

建立委外策略

- 明定委外權責劃分，不盲目因人力不足委外。

保留系統文件及原始碼

- 合約中載明應交付完整文件與託管原始碼。

避免單一廠商依賴

- 分散服務供應商，確保具備替代方案與移轉彈性。

ISO 27001:2022 CONTROL DETAILS

治理面 · ISO控制項說明

治理面概述

資訊作業委外服務之管理制度建立，旨在明確劃分組織與供應商之間的資訊安全權責。透過合約條款落實稽核機制，以確保委外維運過程中的控制有效性及作業透明度，防範管理失控之風險。

A.5.20 供應商合約中的資訊安全

組織應與供應商協商、明定並正式記錄相關資訊安全要求：

- **確立權責邊界：**於合約中詳細列出雙方需共同遵守的資安規範與維運責任。
- **資安合規保證：**要求供應商承諾合規義務，並明定資安事件通報及處理時效。

控制項落實建議 (A.5.20)

在治理與合約規劃階段，應由管理團隊及法務協同落實以下防護：

- **落實定期稽核：**合約應明定稽核權利，允許機關定期或於事件發生時進行稽核。
- **違約罰則與終止：**訂定明確的資安違約罰則，以及服務終止時的敏感資料銷毀與點交機制。

案例分析：委外管理不足之風險

委外後認為全部交給廠商即可，校方未指定管理窗口，也未追蹤服務品質。

真實案例

校務系統異常事件

在缺乏明確窗口與追蹤機制下，系統發生異常時面臨推諉：

- **系統異常**：校務系統異常兩天，無人主動對接。
- **資訊組**：認為廠商已在處理中。
- **廠商**：認為學校尚未正式報修。
- **延宕結果：最後兩天均無人真正開始處理。**

可能影響

管理真空與追蹤缺失，將直接導致服務品質崩潰：

事件嚴重延誤

- 系統故障無法及時排除，中斷日常行政。

責任歸屬不清

- 雙方認知落差，責任互相推諉難以釐清。

SLA承諾未達成

- 服務水準協定流於形式，無法保障學校權益。

建議控制措施

建立專責管理與定期檢討機制，確保委外品質：

指定專責管理窗口

- 學校與廠商皆須明定專責對接負責人。

定期召開服務檢討會

- 建立溝通機制，定期審視履約狀況與問題。

KPI與SLA持續追蹤

- 量化指標控管，依合約執行績效追蹤。

定期資安稽核

- 確保廠商配合安全規範，保障系統與資料安全。

ISO 27001:2022 CONTROL DETAILS

需求面 · ISO控制項說明

需求面概述

資訊作業委外服務之規格分析、資安與個資要求之評估，旨在專案規畫初期，即將資安需求納入專案管理生命週期中，以確保專案產出具備完備的防護能力。

A.5.8 專案管理資訊安全

組織應在專案管理中確定並落實資訊安全要求，以確保在整個專案生命週期中妥善考量資安風險：

- **專案規劃資安需求：**於委外專案發起時，即應鑑別並納入必要的資訊安全與合規條款。
- **風險評估與控管：**將資訊安全作為專案里程碑的審查指標，落實持續性監控。

控制項落實建議 (A.5.8)

在專案與需求規畫階段，應由專案經理與資安代表共同落實以下措施：

- **資安規格完整分析：**明確定義委外產出的功能規格，並將資安檢測機制寫入驗收標準。
- **落實個資保護要求：**若專案涉及敏感個資，須於專案範疇中制定去識別化與存取授權規範。

DOMAIN 03 / 案例探討

採購安全規格不足之風險與因應

採購需求僅要求「系統能用」，未納入資安及個資法規要求，導致重大安全漏洞。

t真實案例

新建招生系統時：

× 完全未要求安全性規格

- HTTPS 傳輸加密
- MFA 雙重驗證
- 完整的 Log 軌跡紀錄
- 安全密碼複雜度

⚠ 系統上線後才發現漏洞百出

可能影響

缺乏前期規劃，將造成無法彌補的重大損失：

敏感個資外洩
- 學生或校務機敏資料遭駭客竊取。

系統面臨重工
- 架構不符法規，需重寫核心模組。

增加維護費用
- 後續修補漏洞耗費龐大額外預算。

建議控制措施

未來於採購需求書中加入：

27001 標準要求

個資法及隱私合規

教育部資通安全規範

OWASP 安全開發指引

ISO 27001:2022 CONTROL DETAILS

合約面 · ISO控制項說明

合約面概述

委外契約簽署前、中、後之權責劃分與資安要求制定。核心任務為將資安防護與個資保護義務以合約條款具體化，確保委外開發、維運均有法規與責任約束，減輕供應鏈資安風險。

A.5.20 供應商合約中的資訊安全

組織應與各家供應商正式簽署協議，明定資訊安全與個資防護之合規責任：

- **明訂罰則與責任歸屬**：合約應載明若因廠商疏失導致個資外洩之賠償與法律責任。
- **保密協定與合規要求**：強制要求簽署保密協定 (NDA) 與配合定期資安合規審查。

A.5.21 資訊與通訊技術供應鏈安全

組織應與供應商協商協定，以管理ICT產品與服務供應鏈相關之資訊安全風險：

- **要求服務品質水準 (SLA)**：明訂系統可用性、回應時間及備援機制等資安與營運指標。
- **分包限制與資安傳遞**：嚴格控管廠商轉包或分包行為，要求分包商須承擔同等資安標準。

DOMAIN 04 / 案例探討

契約只有功能需求，沒有資安要求

委外契約缺乏資安及法規要求，容易導致權責不清、求償困難之重大安全漏洞。

真實案例

委外廠商誤刪學生資料：

× 契約完全未約定：

- 通報時間
- 資料復原責任
- 違約賠償與稽核權

⚠ 最後雙方互相推卸責任

可能影響

求償困難

• 缺乏條款保障，難以向委外廠商要求合理賠償與資料修復責任。

法律責任不明

• 事故發生時無合約義務軌跡，容易陷入漫長的民事訴訟與糾紛。

個資法裁罰

• 因監督不週違反個資法安全維護義務，將面臨主管機關鉅額罰鍰。

建議控制措施

契約應強制納入：

NDA 保密協定

SLA 服務層級協定

資安事件通報機制

個資保護與稽核權權益

終止資料返還與銷毀證明

ISO 27001:2022 CONTROL DETAILS

廠商面 · ISO控制項說明

廠商面概述

資訊作業委外生命週期之廠商監督與稽核機制。旨在建立持續性的服務監控、定期安全性審查，以及嚴格的變更管理程序，防範廠商因資安疏漏或非預期變更而危害機關系統環境。

A.5.22 供應商服務監控、審查與變更管理

組織應定期監控、審查及評估供應商服務之交付，並管理供應商服務的變更，以確保資安合規：

- **服務監督與稽核：**定期審查供應商的服務報告，並針對敏感系統落實資安實地稽核。
- **變更程序管控：**供應商服務或系統之任何重大變更，均須經過嚴格的資安衝擊分析。

控制項落實建議 (A.5.22)

於委外維運階段，應由專案管理與稽核團隊共同落實以下措施以符合合規要求：

- **落實變更申請：**廠商進行系統維護或權限變更前，必須提出書面申請並留存簽核與操作軌跡。
- **定期弱點掃描：**對廠商交付之系統或服務，定期進行獨立的安全漏洞檢測與滲透測試。

DOMAIN 05 / 案例探討

廠商本身資安能力不足

委外廠商若缺乏帳號管理與權限回收機制，將對內部系統防護造成重大潛在威脅。

真實案例

維護人員離職管理疏漏：

× **帳號未及時停權：**

- 維護工程師離職
- 原 VPN 帳號未停用
- 半年後仍可登入學校防火牆

⚠ **離職帳號未清理成潛在後門**

可能影響

未授權存取

- 離職員工或外部人員可任意連線內部網路，窺探機敏系統資訊。

個資外洩

- 防火牆失守導致內部資料庫暴露，引發大規模個資外洩風險。

惡意入侵與破壞

- 駭客可輕易劫持該離職帳號進行跳板攻擊，植入勒索軟體。

建議控制措施

強化帳號與連線控管：

check_circle **定期帳號清查**

check_circle **人員異動立即停權**

check_circle **遠端連線申請制度**

check_circle **導入 MFA 多因素驗證**

check_circle **定期資安查核**

06 / OUTSOURCING RISKS

資訊作業委外 十大常見風險

- 未簽保密協議(NDA)
- 權限過大
- 共用帳號
- 更新未測試
- 離職帳號未停用
- 個資未加密
- 遠端維護未申請
- 未約定通報時限
- 遠端連線未留紀錄
- 契約終止未確認資料銷毀

01 / OUTSOURCING RISKS

1. 未簽署保密協議 (NDA)

風險與案例

- **風險說明**

委外廠商接觸校內機敏資料，但未簽署保密協議，缺乏法律約束。

- **實際案例**

某校委託廠商維護招生系統，工程師將學生名單下載至個人電腦分析，離職後仍保留資料。

可能影響

- 學生個人資料外洩
- 違反個人資料保護法
- 校譽受損

建議控制措施

簽署 NDA

合約納入保密條款

定期宣導保密義務

2. 委外人員使用共用帳號

風險與案例

- **風險說明**

多人共用同一管理帳號，無法辨識實際操作人員。

- **實際案例**

三位工程師共用 Administrator 帳號登入校務系統，系統設定遭修改後，無法追查責任歸屬。

可能影響

- 無法追蹤操作紀錄
- 難以調查資安事件
- 違反帳號唯一性原則

建議控制措施

每人使用專屬帳號

啟用 **MFA**

保留完整稽核日誌

03 / OUTSOURCING RISKS

3. 離職帳號未停用

風險與案例

- **風險說明**

委外人員離職後，系統帳號或 VPN 權限仍持續有效。

- **實際案例**

委外工程師離職三個月後，仍可透過 VPN 登入校園網路，形成重大資安風險。

可能影響

- 未授權存取資料
- 校內個人資料外洩
- 系統遭惡意存取利用

建議控制措施

離職立即停權

定期帳號盤點

每季權限審查

04 / OUTSOURCING RISKS

4. 遠端維護未經申請

風險與案例

- **風險說明**

廠商可直接遠端登入系統，未經校方核准。

- **實際案例**

廠商於深夜直接登入防火牆更新設定，資訊單位事後才發現網路異常。

可能影響

- 未授權變更
- 系統中斷
- 無法追蹤責任

建議控制措施

建立遠端維護申請流程

經主管核准後執行

指定人員陪同或監看

05 / OUTSOURCING RISKS

5. 遠端連線未留存紀錄

風險與案例

- **風險說明**

缺乏登入、操作及維護紀錄。

- **實際案例**

廠商更新校務系統後發生異常，但因未保留操作紀錄，無法確認問題原因。

可能影響

- 無法事件追查
- 稽核缺失
- 改善困難

建議控制措施

保留 VPN Log

保存操作紀錄

定期檢視日誌

06 / OUTSOURCING RISKS

6. 未限制系統管理權限

風險與案例

- **風險說明**

委外人員取得超出工作需求的權限。

- **實際案例**

維護網站的工程師同時擁有資料庫與 AD 管理權限，可存取全校教職員資料。

可能影響

- 權限濫用
- 個資外洩
- 違反最小權限原則

建議控制措施

採 RBAC（角色型存取控制）

落實最小權限原則

定期權限複核

7. 系統更新未經測試

風險與案例

- **風險說明**

直接於正式環境更新系統，未完成測試。

- **實際案例**

校務系統更新後，選課功能異常，造成學生無法正常選課。

可能影響

- 業務中斷
- 資料錯誤
- 學生權益受影響

建議控制措施

check_circle 建立測試環境

check_circle 完成驗證後再正式上線

check_circle 建立回復（Rollback）機制

08 / OUTSOURCING RISKS

8. 個人資料未加密傳輸

風險與案例

- **風險說明**

透過電子郵件或雲端分享未加密的個資檔案。

- **實際案例**

委外廠商以電子郵件傳送學生名冊 Excel 檔，未設定密碼，寄錯收件人。

可能影響

- 個資外洩
- 違反個資法
- 信譽受損

建議控制措施

檔案加密

密碼分開傳送

採用安全傳輸機制

09 / OUTSOURCING RISKS

9. 契約未約定資安事件通報時限

風險與案例

- **風險說明**

發生事件後，廠商無明確通報義務。

- **實際案例**

廠商發現系統遭入侵，但三天後才通知學校，錯失最佳應變時機。

可能影響

- 擴大損害
- 延誤通報
- 增加法律風險

建議控制措施

契約明訂通報時限

建立聯絡窗口

定期演練通報流程

10. 契約終止未確認資料返還或銷毀

風險與案例

- **風險說明**

委外契約結束後，廠商仍保留學校資料。

- **實際案例**

校務系統維護契約終止一年後，廠商測試主機仍保存學生個人資料。

可能影響

- 個資外洩
- 法規違反
- 後續責任不明

建議控制措施

契約明訂資料返還及銷毀要求

要求提供資料銷毀證明

驗證備份資料同步清除

資通安全管理法之要求與機關義務

[法規依據]資通安全管理法第 10條：機關委託他人建置或維運資通系統，應考量受託者之專業能力與資安需求。

01_能力考量

確認受託廠商專業能力

- 相關資安證照 (ISO 27001)
- 同類型系統建置實績
- 團隊成員背景查核

02_需求明訂

於合約中載明資安需求

- 服務水準協議 (SLA)
- 安全性開發規範
- 資料加密與保護要求

03_監督維護

落實對廠商之監督

- 定期或不定期資安稽核
- 系統存取日誌檢查
- 弱點掃描與修補追蹤

BCCS 漢昕科技
- 離你最近的資安專家 -

委外資安評估：能力考量指標說明

[補充說明] 針對受託廠商之「專業能力」進行多維度實質審查，降低專案建置與維運階段之潛在資安風險。

01_資安證照審查

確認相關資安認證與資格

- **ISO 27001**：檢視廠商是否取得國際資訊安全管理系統認證，且仍在有效期限內。
- **認證範疇**：確認該認證之適用邊界與業務範疇是否涵蓋本次委外開發或維運之技術與人員。

02_實績經驗檢核

同類型系統建置與營運經驗

- **歷史專案**：評估廠商過去承接公部門或同等規模機構之資通系統建置實績。
- **穩定維運**：檢視其是否具備處理大規模流量或高安全防護等級系統之長期維運能力與口碑。

03_團隊背景查核

團隊成員素行與技術考核

- **資格審查**：確認主要開發與維運人員具備資安專業技術證照（如 CISSP、CEH 等）。
- **背景查核**：落實人員背景調查，簽署保密切結書，且嚴禁危害國家資安之特定籍別人士參與。

委外資安評估：需求明訂指標說明

[補充說明] 於合約書與規範中明確定義資安義務，建立標準化之服務水準、安全開發與資料保護條款。

01_服務水準協議

明確定義服務水準 (SLA)

指標量化：設定系統可用性指標、資安事件通報時效與應變修復時間之最低標準。

違約罰則：於合約中訂定未達服務水準之罰則與補償機制，確保運作穩定性。

02_安全性開發規範

規範安全軟體開發流程

程序遵循：規範廠商需遵循安全程式碼撰寫指引，防範 OWASP Top 10 等常見漏洞。

檢測交付：要求交付原始碼檢測報告與弱點掃描報告，確保軟體本質安全。

03_資料保護要求

落實資料加密與保護

加密傳輸：敏感資料無論於儲存（At-Rest）或傳輸（In-Transit）狀態皆須落實強加密。

存取控制：訂定明確的資料存取權限，落實個人資料與機敏資訊去識別化。

委外資安評估：監督維護指標說明

[補充說明] 落實對受託廠商之日常與定期監督機制，確保資安防護維持有效性，並建立持續追蹤與改善程序。

01_資安稽核機制

定期與不定期資安稽核

- **稽核規劃**：明訂年度稽核計畫，針對廠商之管理實體、技術執行層面進行實地或書面合規審查。
- **動態抽查**：保留因應重大資安事件或情資時，對受託廠商進行不定期、無預警資安稽核之權利。

02_日誌安全檢查

落實系統存取日誌檢查

- **稽留完整**：確保受託廠商依約完整記錄系統維運、特權帳號登入及資料變更等關鍵行為軌跡。
- **定期送審**：要求廠商定期彙整並提交異常存取日誌報告，由機關管理人員進行合規性審查。

03_漏洞追蹤修補

弱點掃描與修補追蹤

- **定期檢測**：要求廠商定期針對系統執行網路及主機弱點掃描、系統滲透測試，以發掘潛在資安盲點。
- **限期改善**：依據風險分級（高、中、低）明訂修補時效，對未能按時修補之弱點進行警示與追蹤。

資通系統籌獲各階段資安強化措施

REGULATORY BASIS

資通安全管理法 第十條規定

公務機關或特定非公務機關於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供。

本措施旨在建立標準化流程，協助委託機關落實受託者之選任與監督管理。

管理與監督三大強化重點

01 專業選任與評估

應綜合考量受託者之專業能力、經驗、委外項目性質及實際資通安全需求，選任最適當之受託者。

02 落實資安監督

委託機關應建立有效之監督機制，持續監督並掌握受託廠商之資通安全維護與執行情形。

03 補強行政程序

依本法施行細則第七條規定，補充說明選任或監督受託者之相關行政流程與應注意事項。

委外資安評估：資通系統籌獲範疇

[籌獲定義] 指委託機關辦理本法第十條所定委外建置、維運或資通服務提供，執行方式包含以下三類：

01_採購方式

採購取得與執行

- 包含工程定作、財物買受、定製、承租及勞務委派/僱傭。
- 不論是否依據政府採購法，凡執行時使用資通系統者。

02_委任方式

下級機關執行

- 依行政程序法第十五條第一項規定辦理。
- 委任所屬下級機關執行業務，且其執行時使用資通系統。

03_委託方式

外部與民間委託

- 依行政程序法第十五條第二項或第十六條規定辦理。
- 委託不相隸屬之行政機關、民間團體或個人辦理業務，且使用資通系統。

*** 排除與特別規定：**

「無客製化之套裝軟體」、「網路及資安等資通訊設備購買」不適用本措施。惟「例行性或不定期之系統維護案」仍應視契約要求適用維運階段規定。

委外資安評估：(一)需求階段作業規範

[階段核心] 於籌獲需求與規劃初期，落實安全等級評估、估算資安預算，並確立專業選任與評選委員資格。

01_等級與預算

防護等級與經費估算

- **等級評估**：取得前應評估防護需求等級，並經資安長確認。
- **經費估算**：應至少以資訊經費 5% 估算資安經費；未達者需送核。

02_招標與評選

招標規範與評選設計

- **最有利標**：以最有利標、不訂底價為原則選任受託者。
- **配分權重**：資安配分占 10% 為原則；系統占比低者至少占 5%。

03_專業人員

專業人員與團隊配置

- **委員資格**：評選委員需含至少一位資安專家（具證照、實務或教學經驗）。
- **團隊配置**：不採評選者，籌獲團隊亦應包含至少一位資安專業人員。

委外資安評估：(二) 建置階段作業規範

[階段核心] 於系統開發與籌獲建置期間，落實安全軟體開發生命週期(SSDLC)及核心系統獨立驗證(IV&V)。

安全軟體開發 SSDLC

委託機關之資通安全專責人員應以適當方式協助籌獲需求單位，監督並確認開發團隊於系統開發時遵循安全軟體開發生命週期(SSDLC)。

重點里程碑確認

資通系統籌獲案之重點里程碑，應有委託機關之資通安全專責人員協助資通系統籌獲需求單位進行確認。

外部資安專家顧問

核心資通系統籌獲案，應聘請外部資安專家為顧問或委員，於重點里程碑中，協助檢視履約程序與成果之相關資安管理作為。

獨立驗證與認證 (IV&V)

核心系統且委託金額達千萬以上者，應評估導入IV&V機制，且評估結果應經委託機關資通安全長確認。

委外資安評估：(三) 維運階段作業規範

[階段核心] 於系統維運階段，落實日常管理、專責人員配置，並於契約有效期間內確實執行分級與事件型資安稽核。

01_資安管理

落實維運資安管理

- **專責監督：**委託機關之資安專責人員應協助維運單位確認作業。
- **落實項目：**確認包含登入維護、資料備份、效能調校與版本更新。

02_團隊配置

受託者配置專責人員

- **配置規範：**受託者應依約配置適當之資通安全專責人員。
- **協助履約：**監督執行階段作業是否完全符合雙方資安規範。

03_資安稽核

維運期資安稽核作業

- **自主稽核：**可依規模與性質要求受託者自行辦理。
- **定期分級：**「高級」應定期稽核；「中級」得視需求辦理。
- **事件觸發：**知悉重大事件時應即時辦理，成果陳報主管機關。

管理規範：校內 B008 程序書與權責劃分

[FILE] B008_資訊作業委外安全管理程序書

承辦單位 負責日常監督、需求提出、廠商管理及合約執行之第一線查核。

業務單位 負責資安政策的落實、定期稽核計畫執行及整體風險評估。

security[!] 實體安全與遠端存取規範

嚴格限制廠商攜帶設備進入機房，禁止私自複製或攜出限閱資料，確保實體隔離與資料完整性。

委外安全：管理目的與適用範圍

[01 / PURPOSE 目的]

保障委外作業安全

確保國立臺南大學（以下簡稱本校）資訊作業委外之安全，降低潛在之資安風險。

[02 / SCOPE 適用範圍]

適用於本校資訊委外作業項目：

- 主機系統委外採購與維護
- 網路相關硬體設備委外採購與維護
- 應用系統委外開發及維護
- 應用系統套裝軟體客製化及維護
- 資料服務委外
- 設備租用服務委外
- 專業顧問服務委外

作業說明：一般條款

[SECTION 5.1] 委外廠商安全與法規遵循要求 (5.1.1 - 5.1.10)

[01 / EXECUTION 執行規範]

5.1.1應提供系統維護、窗口與電話詢答，必要時配合駐點。

5.1.3作業人員應簽署「合約商保密切結書」並盡保密義務。

5.1.5工具軟體與作業紀錄，本校保有進行安全稽核之權利。

5.1.6應確實留存異常處理紀錄，以利本校隨時查核與調閱。

5.1.9離職時應繳回借用設備、軟體，並立即繳回作業權限。

[02 / COMPLIANCE 法律責任]

5.1.2處理個人資料應嚴格遵守「個資法」及學校相關規定。

5.1.4限用合法軟體，如有違反智慧財產權須負完全法律責任。

5.1.7若交付標的侵害第三人合法權益，應由廠商承擔法律責任。

5.1.8因員工執行業務過失造成本校損失，廠商應負損害賠償。

5.1.10執行業務時所獲知之限閱等級以上資訊，嚴禁對外透露。

委外安全：資訊系統委外服務提出

[SECTION 5.2] 資訊系統委外服務與安全可靠性要求 (5.2.1 - 5.2.4)

[01 / PROCUREMENT 採購與評估]

5.2.1 評估委外必要性：提出資訊委外服務前，主辦單位應適當評估其必要性。

5.2.2 系統需求規劃：主機系統採購應做好規劃，確保足夠的處理與儲存容量。

5.2.3 招標說明規範：RFP須包含資通安全與個人資料管理等合規規定與作業要求。

[02 / CONTRACT 合約安全要求]

5.2.4.1 責任與罰則明訂：發生錯誤或資安事件時由得標廠商負責更正，並依採購法明訂罰則。

5.2.4.2 保密措施與切結：廠商人員均應依規定填具「合約商保密切結書」，若洩密需負法律賠償責任。

5.2.4.3 建立資安規範：依「政府資訊作業委外資安參考指引」及「資通安全管理法」要求，建立相關資安規範。

委外安全：風險評鑑與需求選擇

[SECTION 5.3 & 5.4] 資資產辨識、風險評鑑與安全需求選擇 (5.3 - 5.4)

[01 / RISK ASSESSMENT 風險評鑑]

5.3 資產辨識與風險評鑑作業

5.3.1 評估威脅與弱點

- 應依據「資訊資產管理程序書」與「風險評鑑與管理程序書」辦理。
- 依照委外標的之資訊資產價值、機密性、可用性等級，適當評估其可能之威脅及弱點。

[02 / REQUIREMENTS 安全需求]

5.4 選擇或新增安全需求

5.4.1 明訂安全需求於合約

- 應依據上述風險評鑑結果，進行風險管理作業。
- 選擇適用之安全需求項目，並確實明訂於合約之中，以確保委外作業安全可靠。

委外安全：委外廠商資通安全要求

[SECTION 5.5] 委外廠商作業資通安全要求 (5.5.1 - 5.5.7)

01_專案與人員

專案管理與人員管控

- 5.5.2 交付計畫書：提供工作說明或專案管理計畫書。
- 5.5.3 成員變更控制：專案主持人或重要成員未經同意不得更換。
- 5.5.5 指定地點執行：應於本校所指定之作業地點執行業務。

02_法令遵循

法律與安全規範遵循

- 5.5.1 守法與防洩密：人員執行業務應遵守資安與個資保護法令，違者依法辦理。
- 5.5.6 協力廠商同等：合作或協力廠商皆應併同遵循法律與校方各項規定。

03_應變與稽核

應變維運與安全稽核

- 5.5.4 應變回復程序：重要資通系統廠商應訂定緊急應變與回復標準程序，確保持續運作。
- 5.5.7 配合安全稽核：廠商須配合本校進行資通安全與個人資料管理稽核作業。

委外安全：服務交付與硬體維護

[SECTION 5.6 & 5.7] 委外服務交付管理與硬體採購維護 (5.6 - 5.7)

[5.6 / SERVICE DELIVERY 委外交付]

5.6 委外服務交付管理

- **5.6.1 進出管制**：委外人員進出辦公或機房區域，依據「實體安全管理程序書」辦理。
- **5.6.2 專人陪同**：委外人員於本校執行業務時，應由業務負責同仁全程陪同處理。
- **5.6.3 設備攜出入**：攜帶資訊設備出入辦公或機房區域，依「實體安全管理程序書」辦理。
- **5.6.4 遠端存取**：外部遠端存取維護時，依「存取控制」及「通信與作業管理」程序書辦理。

[5.7 / HARDWARE MAINTENANCE 硬體維護]

5.7 硬體採購與維護

- **5.7.1 廠商技術支援與維護義務：**
  廠商應提供與設備主機之架構、操作、管理、維護等相關之操作手冊、文件與技術支援。
- **教育訓練要求：**
  如有必要，廠商亦應提供對應之教育訓練課程，確保管理人員具備操作與維護能力。

開發安全：系統開發與維護規範

[SECTION 5.8] 系統開發與維護安全要求 (5.8.1 - 5.8.6)

[5.8.1 - 5.8.3 / DEVELOPMENT & CONTROL]

5.8.1 - 5.8.3 架構與版本管控

- **5.8.1 完整架構說明**：廠商開發應提供系統架構說明、分析設計、資料庫設計等文件，經確認後執行。
- **5.8.2 版本一致性控管**：委外廠商應確實控管程式與文件版本之一致性。
- **5.8.3 嚴禁外洩業務資料**：開發與維護時，不得任意複製或攜出本校限閱等級以上之業務資料。

[5.8.4 - 5.8.6 / SECURITY & DEPLOYMENT]

5.8.4 - 5.8.6 安全保證與上線規範

- **5.8.4 確保系統無惡意程式**：廠商應保證交付系統內不含後門程式、隱密通道及特洛伊木馬。
- **5.8.5 嚴格測試驗收上線**：由委外或權責單位進行測試及驗收，符合需求後，依「系統開發與維護程序書」上線。
- **5.8.6 變更遵循例外審核**：修改與開發需遵守程序書規定，例外須經資訊單位主管同意後實施。

帳號安全：系統帳號管理規範

[SECTION 5.9] 系統帳號安全與權限管理規範 (5.9.1 - 5.9.5)

[5.9.1 - 5.9.3 / 帳號申請與授權]

5.9.1 - 5.9.3 帳號與權限管控

- **5.9.1 最高權限保管**：系統及資料庫最高權限帳號由本校人員保管，不得直接授與委外廠商。
- **5.9.2 提出存取申請**：因作業需存取系統時，由本校人員填寫「資訊服務申請表」代為提出申請。
- **5.9.3 獨立帳號建立**：申請表應載明作業需求、所需權限及有效時間，核准後建立獨立帳號供廠商使用。

[5.9.4 - 5.9.5 / 使用責任與監督]

5.9.4 - 5.9.5 帳號保管與操作監督

- **5.9.4 善盡保管之責**：廠商人員對系統帳號應善盡保管責任，嚴禁任意交由非作業相關人員使用。
- **5.9.5 盡監督與稽核責**：管理者應監督其操作且嚴禁非工作範圍之行為，並於廠商完成工作後檢視系統紀錄。

營運安全：緊急應變與變更管理

[SECTION 5.10 - 5.12] 緊急應變、例外與服務變更管理規範

[5.10 / EMERGENCY]

5.10 緊急應變與備援

- **關鍵業務演練**：委外涉及關鍵業務應定期進行永續計畫測試。整體委外依最高資產價值評估演練週期。
- **備援機制建立**：依資訊資產價值及可用性等級考量，必要時建立異地備援機制。

[5.11 / EXCEPTION]

5.11 例外安全作業

- **安全需求提案**：主辦單位應依規範提出安全需求。若因成本、時效等因素無法完全適用，得以簽呈或會議決議方式，提出其他適切之替代安全規劃。

[5.12 / CHANGE]

5.12 服務變更管理

- **核可變更程序**：如有變更，承辦人需以簽呈通報主管並附風險評鑑，核可後方可實施。
- **六大變更範疇**：包含網路架構改變、新技術導入、版本轉換、新開發工具/環境、設備搬遷，及更換廠商或人員。

相關文件：合規與程序書清單

[SECTION 6] 資安制度合規與參考之程序書、表單 (6.1 - 6.10)

[6.1 - 6.5 / 法規與管理政策]

核心安全政策與管理程序書

- **6.1 個人資料保護法**：遵循個資法規定，確保相關個人隱私資料之蒐集與保護。
- **6.2 資通安全管理政策**：明訂機關整體資通安全之指導方針與最高指導原則。
- **6.3 資訊資產管理程序書**：建立資訊資產清冊、分類與分級之風險管控程序。
- **6.4 風險評鑑與管理程序書**：定期評估各資產之風險威脅，並採取適切控制措施。
- **6.5 系統開發與維護程序書**：規範安全軟體開發生命週期(SSDLC)及安全要求。

[6.6 - 6.10 / 安全控制與表單]

控制程序書與執行表單切結

- **6.6 存取控制管理程序書**：管理系統帳號權限，落實最低權限與帳號申請原則。
- **6.7 實體安全管理程序書**：防護實體機房與辦公環境，控管人員進出與安全。
- **6.8 通信與作業管理程序書**：規範網路傳輸安全、系統備份以及日常維運維護作業。
- **6.9 資訊服務申請表**：外部或異動需求時，落實申請、評估、核准後執行程序。
- **6.10 合約商保密切結書**：確保合作委外廠商人員善盡保密協定、保護機密資訊。

安全軟體開發生命週期 (SSDLC) 全流程

STAGE 01
需求分析
[REQUIREMENT]

定義安全需求與法規合規性基準，於規劃初期納入資安考量。

STAGE 02
設計與架構
[DESIGN & ARCH]

落實核心安全原則：

- 最小權限原則
- 預設安全配置
- 威脅建模分析

STAGE 03
安全程式碼
[DEVELOP]

撰寫安全程式碼：

- 遵循安全開發指引
- 原始碼掃描 (SAST)
- 避免 OWASP 漏洞

STAGE 04
測試與部署
[TEST & DEPLOY]

多重驗證把關：

- 弱點掃描 (DAST)
- 第三方函式庫檢測
- 清除測試與後門

STAGE 05
維運監控
[MONITOR]

持續監控、稽核、威脅應變修補。

委外資安評估：需求分析指標說明

[補充說明] 於規劃與招標初期明確界定安全需求，將合規性與資安防護基準納入評估流程。

01_安全需求定義

定義安全需求與標準

合規基準：分析法規與組織政策，明訂委外系統必須達成的安全控制措施與法規遵循要件。

初期規劃：於專案發起階段納入資安核心考量，確保安全機制非事後修補，降低後期修改成本。

02_招標規範納入

招標文件明訂資安規範

規格擬定：將系統弱點掃描、效能壓力測試及源碼檢測等技術規格，具體載明於招標條款中。

責任義務：於合約草案中明訂受託廠商之資安維護責任、事件通報法定義務與損害賠償條款。

03_廠商資格審查

嚴格篩選合作夥伴

能量評估：審查投標廠商之資安證照、歷史實績與團隊專業能力，確保具備足夠的安全開發能量。

實地評選：評選過程中針對廠商的安全管理制度進行審查，排除缺乏基本防護能力之不合格廠商。

委外資安評估：設計與架構指標說明

[補充說明] 於系統設計與架構規劃階段落實核心安全原則，並透過威脅建模與主動防禦設計，確保系統本質安全。

01_最小權限與防禦

落實核心安全設計原則

最小權限：嚴格限制系統服務與帳戶權限，僅開放業務所需之最低存取路徑與核心功能。

預設安全：系統出廠預設關閉不必要之服務、連接埠與共享機制，將暴露風險降至最低。

02_安全架構與威脅

執行威脅建模與架構審查

威脅建模：於設計初期針對資料流、外部介面與信任邊界執行威脅建模（Threat Modeling）分析。

防禦設計：依據評估結果，於整體網路與系統架構中，佈署相對應之安全控制措施。

03_縱深防禦與隔離

落實多層次縱深防禦

區域隔離：規劃明確之網段劃分，將展示層、業務邏輯層與資料庫層進行實體或邏輯隔離。

主動防禦：整合入侵偵測、網頁防火牆（WAF）等防禦機制，建立多層次的安全防護網。

委外資安評估：安全程式碼指標說明

[補充說明] 於程式碼開發與撰寫階段落實安全編碼標準，透過自動化原始碼掃描與漏洞防範，確保軟體本體之安全性。

01_安全開發指引

遵循安全開發與編碼標準

標準落實：規範開發團隊落實安全程式碼撰寫規範，從源頭阻斷 OWASP Top 10 等常見系統安全性弱點。

教育訓練：要求委外廠商技術人員具備安全編碼意識，定期進行最新資安防範與安全撰寫指引培訓。

02_原始碼檢測

靜態原始碼掃描 (SAST)

自動編譯：導入自動化靜態程式碼分析工具，於系統編譯與建置階段，主動偵測程式碼潛在之邏輯漏洞。

零高風險：規範交付之程式碼於 SAST 檢測中，不得含有任何「高風險」等級以上之安全缺陷與漏洞。

03_避免已知漏洞

第三方函式庫與威脅防範

套件合規：針對引入之開放原始碼與第三方套件（SCA）進行安全性檢測，避免使用已知含有資安弱點之版本。

防範威脅：持續追蹤最新零日（Zero-day）漏洞，建立快速漏洞修補與程式庫升級流程，確保底層組件安全。

委外資安評估：測試與部署指標說明

[補充說明] 於系統測試與部署階段，落實自動化與多重安全驗證，確保程式交付與環境配置符合資安基準。

01_動態弱點掃描

執行 DAST 動態掃描

模擬攻擊：於系統測試環境部署完成後，利用自動化工具模擬黑客攻擊行為，檢測執行期漏洞。

即時阻斷：針對 SQL 注入、跨站腳本 (XSS) 等常見網頁漏洞進行全面掃描，確保無高風險安全漏洞。

02_第三方元件檢測

軟體組成分析 (SCA)

開源審查：清點並檢測系統所引用之開源套件與第三方函式庫，防範引入已知漏洞之組件。

授權合規：同步審查開源授權合規性，降低法規與智慧財產權授權違約之潛在法律風險。

03_部署完整性校驗

清除測試環境與後門

環境清理：於正式上線前，徹底移除開發與測試階段殘留之測試帳號、臨時檔案與除錯工具。

後門稽核：嚴格審查程式碼與設定檔，確保無殘留惡意後門、硬編碼憑證或高特權隱藏帳號。

委外資安評估：維運監控指標說明

[補充說明] 系統上線後應落實持續性的安全監控與應變機制，確保能即時偵測威脅，並在發生安全事件時迅速啟動應變與漏洞修補程序。

01_持續安全監控

建立全天候監控機制

即時偵測：配置自動化安全偵測工具，監控系統流量、異常行為與潛在的入侵企圖。

威脅告警：建立即時通報與告警流程，當偵測到高風險異常時能第一時間派單處理。

02_定期合規審查

落實資安稽核與評估

例行稽核：定期針對維運帳號使用狀況、特權授權進行審查，避免權限蔓延與後門殘留。

配置合規：持續核對系統設定是否符合基準規範，防止因日常變更產生安全防護破口。

03_應變與修補

安全事件與威脅應變

快速修補：針對新揭露之零日漏洞（0-Day），落實限期熱修補，防範漏洞遭主動利用。

事件演練：定期實施資安事件緊急應變演練，優化通報通聯與系統備份復原之執行效率。

國立臺南大學委外廠商資通安全管理措施查核自評表

廠商名稱：　　(加蓋公司大小章)

系統(網頁)名稱：

填表日期：　年　月　日

填表單位：

填表人員：　　職稱：

公司印鑑

負責人

填表說明：

自評結果填寫「符合」需附紀錄文件或佐證資料，若自評結果為不符合或不適用，請填寫說明欄。

自評項目	自評內容	自評結果			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？	□	□	□	
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	
	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？	□	□	□	
	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？	□	□	□	
	1.5 是否維時公告資通安全相關訊息？	□	□	□	
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、推動及管導等事項？	□	□	□	
	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？	□	□	□	
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	
3.配置適當之資	3.1 是否訂定人員之安全評估措施？	□	□	□	
通安全專業人員及適當之資源	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	
	3.3 是否具備相關專業資安證照或認證？	□	□	□	
	3.4 是否配置適當之資源？	□	□	□	
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，並維時維護更新？	□	□	□	
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	□	□	□	
	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？	□	□	□	
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？	□	□	□	
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	
	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？	□	□	□	
	5.4 電腦機房操作人員是否維時注意環境監控系統，掌握機房溫度及濕度狀況？	□	□	□	
	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？	□	□	□	
	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？	□	□	□	
	5.7 重要資訊處理設施是否有特別保護機制？	□	□	□	
	5.8 重要實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、電磁輻射或民間暴動等可能對設備之危害？	□	□	□	

自評項目	自評內容	自評結果 符合	不符合	不適用	說明
	5.9 電源之供應及備接電源是否作安全上考量？	□	□	□	
	5.10 通訊線路及電纜線是否作安全保護措施？	□	□	□	
	5.11 設備是否定期維護，以確保其可用性及完整性？	□	□	□	
	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？	□	□	□	
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設密碼、檔案加密、專人看管)？	□	□	□	
	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？	□	□	□	
	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？	□	□	□	
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	
	5.19 是否定期執行各項系統漏洞修補程式？	□	□	□	
	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)？	□	□	□	
	5.21 重要的資料及軟體是否定期作備份處理？	□	□	□	
	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？	□	□	□	
	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？	□	□	□	
	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？	□	□	□	
	5.25 是否訂定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？	□	□	□	
	5.27 密碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	□	□	□	
	5.28 密碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	
	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？	□	□	□	
	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？	□	□	□	
	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)？	□	□	□	
	5.32 重要系統是否使用憑證作為身份認證？	□	□	□	
	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？	□	□	□	
	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？	□	□	□	
6.訂定資通安全事件通報及應變之程序及機制	5.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	
	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？	□	□	□	

自評項目	自評內容	自評結果			說明
		符合	不符合	不適用	
	5.3 是否留有資通安全事件處理之紀錄文件，紀錄中並有改善措施？	☐	☐	☐	
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？	☐	☐	☐	
	7.2 是否對同仁進行資安評量？	☐	☐	☐	
	7.3 同仁是否依層級定期參辦資通安全教育訓練？	☐	☐	☐	
	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？	☐	☐	☐	
8.資通安全維護計畫實施情形之持續改善機制	8.1 是否設有稽核機制？	☐	☐	☐	
	8.2 是否定有年度稽核計畫？	☐	☐	☐	
	8.3 是否定期執行稽核？	☐	☐	☐	
	8.4 是否改正稽核之缺失？	☐	☐	☐	
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？	☐	☐	☐	
	10.2 是否追蹤過去缺失之改善情形？	☐	☐	☐	
	10.3 是否定期召開持續改善之管理審查會議？	☐	☐	☐	

危害國家資安產品限制使用原則

// SECURITY_ALERT

嚴禁採購
大陸廠牌
資通訊產品

產品範圍
包含硬體、軟體及各項資通訊服務，均不得使用大陸廠牌。

人員限制
廠商執行團隊成員不得為陸籍人士，確保開發與維運安全。

招標規範
辦理採購時，必須在招標文件明確列入排除條款。

BCCS 漢昕科技
- 離你最近的資安專家 -

採購契約的選擇與應用指南

	[採購標的]		[適用契約類型]
01	**資通系統建置與維護** 細項：系統開發、系統整合、維護保養	→	**資訊服務採購契約**
02	**套裝軟體與硬體設備** 細項：伺服器、網路設備、套裝軟體授權	→	**財務採購契約**
03	**資安顧問與專業服務** 細項：資安健診、滲透測試、顧問與培訓	→	**勞務採購契約**

// KEY_INSIGHT

選對契約範本，是確保合約包含正確資安條款的第一步。

合約必備：RFP 資安需求與關鍵法律條款

// RFP_REQUIREMENTS

- 明訂資安評比項目與權重
- 服務水準協議 (SLA) 之量化指標
- 廠商對機敏資料的絕對保密義務

// LEGAL_LIABILITY

- 資安事件發生時的損害賠償責任
- 違反資安規定之罰則與解約條款

/var/log/legal/penalty_clause

合約應載明：若因廠商疏失導致資安事件，廠商須負擔所有調查、復原及法律訴訟費用。

明訂資安評比項目與權重說明

BCCS 漢昕科技
- 離你最近的資安專家 -

資安權重
最少 20%

依主管機關規定，委外資訊服務採購案中，資安評比之配分或權重原則上不得低於整體 20%。

技術與管理評比 (15%)

著重於廠商的技術能力與日常資安管理維護規範。

- 資安證照與實績
- 系統防護與加密技術
- 日常維運監控計畫

應變與應急機制 (5%)

評估當面臨突發資安事件時，廠商的通報與復原處理效能。

- 事件通報流程時效
- 災難復原演練計畫
- 應變小組編組與編制

服務水準協議 (SLA) 之量化指標說明

系統可用率
最少 99.9%

每月系統持續運作時間比例，扣除計畫性維護時間後，須達合約承諾之高可用性標準。

事件響應與處理時效

依資安事件等級 (High / Medium / Low) 明訂對應的時效要求：

- **通報時效**：知悉發生資安事件後，應於 **1 小時內** 通知機關（或接獲機關通知 1 小時內），並採取適當之應變措施。
- **損害控制與復原**：應於知悉資通安全事件後 **72 小時**（若是重大資安事件為 **36 小時**）內完成損害控制或復原作業。

資料備份與復原指標

確保資料流失與中斷時間控制在容許範圍，確保業務連續性：

- RPO (還原點目標) < 24h
- RTO (還原時間目標) < 4h
- 每日異地、異機備份機制

廠商對機敏資料的絕對保密義務說明

保密義務
無限期有效

廠商對於因本案所知悉或持有之機敏資料，不論在合約期間或合約終止後，均負有絕對保密之責任。

資料安全防護要求

廠商應採取嚴格之技術與管理措施，確保機敏資料之儲存與傳輸安全：

- 機敏資料儲存須全面加密
- 限用安全且加密之傳輸協定
- 存取權限控管與最小授權原則

稽核稽查與銷毀機制

明訂合約終止後之資料處理規範，以及日常配合稽核之義務：

- 專案結束後機敏資料必須銷毀
- 應配合本機關進行安全稽核
- 留存完整存取與銷毀紀錄軌跡

BCCS 漢昕科技
- 離你最近的資安專家 -

實務表單：從切結、自評到結案銷毀流程

01_PROJECT_INIT
// 入案階段

- D020_合約商保密切結書
- 廠商人員資安切結書

02_MAINTENANCE
// 維運階段

- 委外廠商資通安全管理措施查核自評表
- 定期資安稽核紀錄表

03_PROJECT_EXIT
// 結案階段

- 資料返還、銷毀、刪除切結書
- 帳號權限註銷確認單

權限管控：廠商帳號管理三大原則

// PRINCIPLE_01

禁止直接授與最高權限

// PRINCIPLE_02

實名申請與時效管控

// PRINCIPLE_03

凡走過必留下稽核痕跡

原則一：禁止直接授與最高權限說明

// PRINCIPLE_01_DETAIL

嚴禁交付 root 或 admin 帳號

最高管理權限（如 root, administrator, admin 等）直接交付廠商，將導致極大的資安稽核漏洞，且無法釐清實際操作人員之責任。

落實管理之具體作法：

- 採最小權限原則：僅授予執行專案或維護所需的最低權限。
- 僅開放必要功能：限縮存取範圍，不開放無關的系統配置權限。
- 個別建立帳號：禁止共用帳號，必須能識別至個人身分。

原則二：實名申請與時效管控說明

// PRINCIPLE_02_DETAIL

落實實名帳號與時效安全管制

嚴禁任何未經申請或共用之幽靈帳號存取內部系統。所有協力廠商均須以實名填寫申請表，並在任務完成後立即停用權限，確保所有操作皆可明確追溯至個人。

實名與時效控管之具體作法：

- 一人一帳號：全面禁止共用帳號，必須與廠商實際執行人員身分進行一對一連結綁定。
- 時效嚴格管控：依專案合約與派工期程設定帳號有效期限，到期系統將自動停用與鎖定。
- 完工立即註銷：工程或專案任務一旦結束，須立即填寫註銷確認單，主動收回帳號權限。

原則三：凡走過必留下稽核痕跡說明

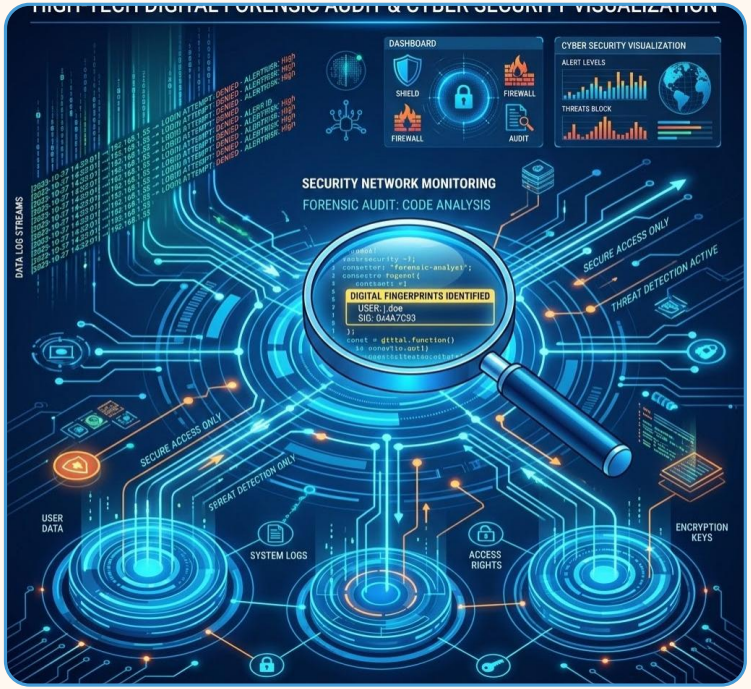
// PRINCIPLE_03_DETAIL

落實完整操作日誌與審查機制

嚴禁任何未留存紀錄或無法追溯之操作行為。系統管理者必須確保所有協力廠商之存取活動均被即時且完整記錄，並透過定期審查機制，確保所有維運軌跡之真實性與合規性。

稽核痕跡留存之具體作法：

- 保留操作日誌：全面啟用系統稽核紀錄，完整留存登入、存取、修改及執行等所有事件日誌。
- 定期稽核對帳：管理人員須定期比對派工申請紀錄與實際系統操作日誌，確保行為皆有授權。
- 日誌防護與防篡改：稽核軌跡須進行集中化加密備份，非經授權人員嚴禁異動或刪除歷史軌跡。



BCCS 漢昕科技
- 離你最近的資安專家 -

資安事件通報與緊急應變程序

[通報時機]知悉異常登入、中毒或資料外洩時，應立即啟動通報程序。

// PHASE_01
損害控制
隔離受影響系統，防止損害擴大。

// PHASE_02
事件調查
分析日誌與跡證，釐清入侵路徑。

// PHASE_03
復原作業
系統修補與還原，確認服務正常。

// PHASE_04
改善報告
檢討原因並提出長期防護對策。

// CRITICAL_SYSTEM_REQUIREMENT

針對涉及關鍵業務之系統，須要求廠商配合建立緊急應變計畫，並定期進行異地備援與切換測試。

步驟一：緊急事件之損害控制說明

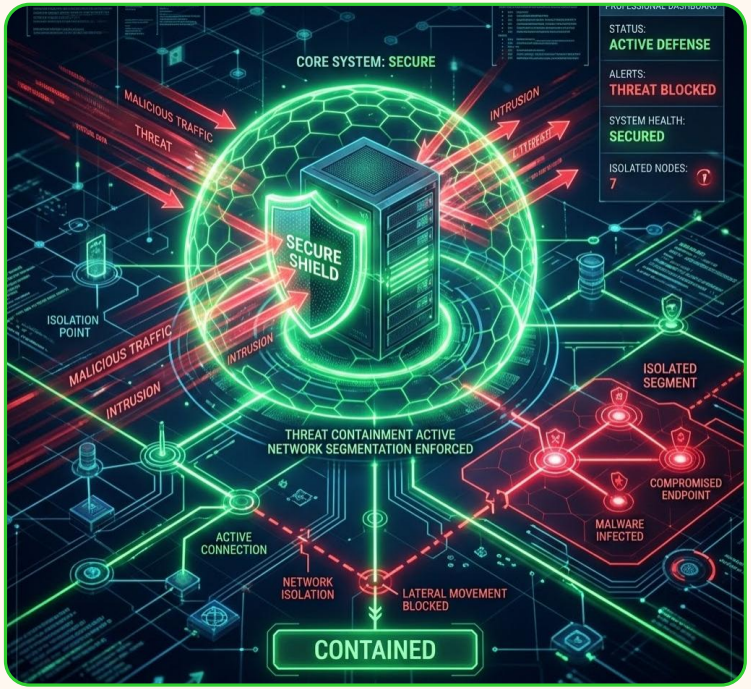
// EMERGENCY_CONTAINMENT

即時損害控制與威脅隔離

當系統偵測到異常活動或接獲通報時，必須以「阻斷損害擴大」為最高指導原則。本階段重在阻斷攻擊源、保護未受感染的乾淨網段，同時確保營運關鍵服務維持最低運作限度。

應變階段之具體作法：

- 網路與主機隔離：立即將受駭伺服器切離核心網路，關閉未受波及之連外通訊埠，防止橫向滲透。
- 阻斷惡意連線：強制清除可疑之連線階段，針對已辨識的惡意 IP 或網域進行網頁防火牆封鎖。
- 保護備份快照：立即將系統備份檔案與快照離線保存，避免備份資料同步遭受勒索軟體加密毀損。



步驟二：緊急事件之事件調查說明

// INCIDENT_INVESTIGATION

深度事件調查與入侵路徑釐清

當損害獲得控制後，應立即啟動全面調查。本階段著重於分析系統日誌、採集數位跡證、釐清攻擊者之入侵路徑，並找出關鍵安全漏洞，以作為防護改善之事實依據。

事件調查之具體作法：

- 完整日誌分析：收集網頁防火牆、作業系統及應用程式之存取紀錄，以釐清攻擊手法與歷程。
- 數位跡證保存：妥善封存受駭主機之記憶體與磁碟映像檔，並確保採證過程符合司法證據力。
- 弱點與根因分析：確認攻擊者所利用的安全漏洞與權限提升途徑，建立完整的損害事件報告。

步驟三：緊急事件之復原作業說明

// SYSTEM_RECOVERY_PHASE

系統修補還原與服務可用性確認

在確認威脅完全隔離與根因釐清後，應穩健啟動系統復原作業。本階段著重於安全地重建與修補受駭系統，導入強化之防護機制，並在重新上線前進行嚴格的安全驗證，確保業務運作順暢無虞。

復原作業之具體作法：

- 安全重建與純淨還原：使用已知安全之備份來源還原系統，或全新安裝作業系統與應用軟體，徹底清除殘留惡意程式。
- 漏洞修補與配置強化：在上線前強制安裝所有安全更新，修補先前被利用的弱點，並依照最新基準強化安全配置。
- 服務驗證與監控：執行功能與效能測試，確認資料完整性，並在重新上線後實施 72 小時不間斷之高強度安全監控。

資安事件改善報告程序說明

[改善宗旨]**透過根本原因分析與長期防禦規劃，防堵重複事件，強化組織數位韌性。**

// STEP_01

檢討原因 (Root Cause Analysis)

- **人為因素分析**：評估操作失誤、資安意識不足或社交工程之誘因影響。
- **技術漏洞釐清**：盤點未修補漏洞、系統配置不當或防禦機制的短板。
- **流程阻礙審查**：檢討通報延遲、權限管理缺失或應變程序執行的卡點。

// STEP_02

長期防護對策 (Defense-in-Depth)

- **架構強化升級**：導入零信任架構、強化微隔離及落實特權帳號管理。
- **主動防禦建置**：布署端點偵測回應（EDR）及強化日誌集中監控機制。
- **持續教育訓練**：定期辦理社交工程演練，確保同仁通報應變程序純熟。

持續維運：資安日常化管理與日誌保存機制

// VULNERABILITY_MGMT

持續弱點追蹤與漏洞修補

導入 VANS 資通安全弱點通報機制，持續追蹤並修補系統漏洞，確保系統安全性。

// PATCH_&_UPDATE

定期更新機制與元件防護

建立定期更新機制，確保系統元件、防護軟體及作業系統處於最新安全版本。

// LOG_RETENTION

日誌保存機制最少 6 個月

遵循日誌保存政策，妥善留存下列關鍵操作與存取日誌：

- 使用者登入紀錄
- 權限變更紀錄
- 機敏資料存取紀錄

持續維運：持續弱點追蹤與漏洞修補

// VULNERABILITY_DETECTION

弱點偵測與通報機制

藉由自動化工具與標準化程序，建立即時的系統弱點檢知，縮短從漏洞暴露到安全防護的空窗期：

- 導入 VANS 資通安全弱點通報機制
- 每日比對最新情資與資產列表
- 精準識別潛在受威脅的系統元件

// PATCH_MANAGEMENT

漏洞修補與生命週期

針對已確認的安全漏洞實施嚴格的生命週期管理，結合風險分級，在不影響業務連續性的前提下安全部署更新：

- 依據 CVSS 風險評級制定修補優先順序
- 於隔離測試環境驗證更新相容性
- 執行版本控制與防護成效持續追蹤

定期更新機制與元件防護規範

// PATCH_MANAGEMENT_POLICY

系統更新與元件防護三大原則

透過標準化與自動化的更新流程，降低系統漏洞被利用的風險，確保整體資訊安全環境之完整性：

- 定期漏洞掃描與弱點評估
- 自動化更新發佈與測試驗證機制
- 關鍵元件與防護軟體特徵庫即時同步

持續維運：日誌保存機制與稽核管理規範

最少保存 6 個月
法規遵循底線

依據資通安全管理法，關鍵系統與防護設備日誌必須妥善保存至少 180 天，以利後續資安事件調查與追溯。

使用者登入與驗證紀錄 (AUTHENTICATION)

保存所有帳號登入嘗試、來源 IP 位址、登入時間與身分識別結果，精確掌握人員存取軌跡。

帳號與權限變更紀錄 (AUTHORIZATION)

詳實留存群組政策異動、管理員權限指派、帳號新增與停用等高風險異動事件。

機敏資料與系統存取紀錄 (DATA_ACCESS)

針對核心資料庫與關鍵系統檔案，追蹤所有讀取、修改、刪除等操作，防止內部洩密風險。

D054資通系統防護基準查檢表

依據「資通安全責任等級分級辦法」制定「D054資通系統防護基準查檢表」

為協助各單位評估所管資通系統的資安防護等級與控制措施是否合規，請各單位資通系統(含網站)管理人員填報「D054資通系統防護基準查檢表」。

每一個資通系統(含網站)均須填報一份對應等級的查檢表。

資通系統(含網站)的安全等級，於南大入口之「資通系統防護需求分級鑑別 」進行評估，評估結果安全等級1為普級，安全等級2為中級，安全等級3為高級。

「D054資通系統防護基準查檢表」三版本(普中高)，請從本校文件管理系統下載。ISMS-->B003-->D054

文件管理系統網址：https://system.nutn.edu.tw/cc_doc/

D054資通系統防護基準查檢表→從本校文件管理系統下載

結論與測驗：確保學習成效與雙向交流

BCCS 漢昕科技

- 離 你 最 近 的 資 安 專 家 -

Thank you

FOR YOUR ATTENTION

Get in touch:

雲安維運　聯防設備　風險檢測　顧問諮詢　資安學苑