

國立中正大學

網路與資通安全管理系統建置案

需求說明書

中華民國 112 年 5 月

## 目錄

壹、 專案說明.....	1
一、 專案名稱.....	1
二、 專案目標.....	1
三、 現況說明.....	1
四、 專案時程.....	1
貳、 專案需求及規格.....	1
一、 系統功能需求.....	1
二、 資通安全功能需求.....	3
三、 開發、建置及運作條件.....	3
四、 需求訪談.....	3
五、 系統測試.....	4
六、 技術檢測及漏洞修補.....	4
七、 伺服器與系統管理服務.....	4
八、 教育訓練.....	4
參、 專案管理.....	5
一、 專案工作計畫書.....	5
二、 專案品質與時程管理.....	5
三、 廠商資格與專案組織.....	5
肆、 作業期限及交付成果.....	6
一、 作業期限.....	6
二、 交付成果.....	6
伍、 驗收與付款方式.....	7
陸、 保固維護及後續責任.....	7
柒、 資通安全暨保密條款.....	7
捌、 其他規定.....	9
玖、 企劃書內容及格式.....	9
一、 裝訂及交付.....	9
二、 一般要求.....	10
三、 企劃書內容.....	10
附表 1-資安管理作業自我評估表.....	12
附表 2-單價分析表.....	14

## 壹、專案說明

### 一、專案名稱

國立中正大學網路與資通安全管理系統建置案，以下簡稱本專案。

### 二、專案目標

本專案規劃開發網路與資訊安全管理系統（以下簡稱本系統），主要提供 IP 位址與網段分層管理功能，讓各單位管理者及使用者即時更新 IP 位址配發及使用情形，以利於發生資安事件或接獲資安情資時，可迅速通知相關人員。

本系統另須提供文件管理、帳號管理與代理人管理等功能，系統管理者可依使用者身分別設定不同權限。使用者與管理者均透過本校單一認證系統登入本系統，針對重要異動均須保留紀錄並提供查詢及匯出報表功能。

### 三、現況說明

本校 IP 位址及網段係由資訊處規劃建置後，配發各單位管理者運用，因各單位管理方式不一且無集中管理機制，導致偶有 IP 位址遭佔用或 IP 位址使用狀況不明情形，當發生資安事件時不易查找當事人，無法於第一時間有效處置。

此外本校已於全校範圍導入資通安全管理與個資保護機制，相關管理文件須考量可公開範圍，有效傳達所有人員知悉，惟目前並無結合身分管理之文件下載區。

### 四、專案時程

決標次日起 150 日曆天內完成本專案之功能建置及系統上線。

## 貳、專案需求及規格

### 一、系統功能需求

- (一)系統首頁顯示最後一次登入紀錄及系統公告。
- (二)系統使用者包含本校所有教職員工及學生，須介接本校單一認證系統（以下簡稱 SSO），所有使用者與管理者均透過 SSO 身分認證。

(三)系統提供使用者設定代理人及開關電子郵件通知功能，使用者電子郵件資訊依身分別分別來自本校學籍系統、人事系統與計畫系統。

(四)系統包含網管子系統、文件管理子系統、帳號管理子系統、記錄子系統等功能，各子系統需求如下：

#### 1. 網管子系統

- (1) 提供 IP 網段分層管理功能，管理者共有 3 層，依序為校級網管、單位管理者及各組/實驗室管理者，各層管理者可分配 IP 位址區間給下一層管理者或使用者。
- (2) 校級網管可查詢所有 IP 位址配發及使用資訊。
- (3) 使用者可檢視受分配之 IP 位址清單，維護或批次匯入 IP 位址的設備資訊（如：MAC 位址、設備類型、作業系統等）。

#### 2. 文件管理子系統

- (1) 提供文件上傳功能，可設定文件類別、名稱、階層、版次、上版日期、下架日期及開放範圍（僅限教職員工或不限）等資訊。
- (2) 提供文件下載功能，可依文件階層結構檢視所有文件，並依身分別下載文件（如：學生無法下載僅限教職員工之文件）。
- (3) 提供個別文件下載固定連結，可下載該文件上架之最新版本。

#### 3. 帳號管理子系統

- (1) 管理者可新增修改角色，並調整及具備功能及權限（瀏覽、新增、修改及刪除）。
- (2) 管理者可指定帳號及對應之角色，其他未設定角色之帳號，進入系統後均具備使用者角色。

#### 4. 紀錄子系統

- (1) 保留使用者登入、IP 位址配發與更新、角色權限異動及帳號角色異動等重要資料異動紀錄。
- (2) 提供使用者登入紀錄、網管異動紀錄及帳號異動紀錄等紀錄查詢及匯出功能。

(五)系統儲存之資料如涉及個人資料或其他機密資料，除屬於系統鍵值或因其他因素不可加密儲存者，均須以適當方式加密存放。

## 二、資通安全功能需求

本系統之資通系統分級為中級，須符合資通安全責任等級分級辦法附表十資通系統防護基準中，普級及中級的所有控制措施要求，廠商於系統開發建置時，應將資通系統防護基準納入考量，驗收時須提交符合性說明。

## 三、開發、建置及運作條件

- (一)系統須可運行於建置在 VMware ESXi 虛擬主機，虛擬主機作業系統使用 Ubuntu 22.04 LTS 版本，未來須可升級至 Ubuntu 24.04 LTS，所使用相關軟體套件須一併升級。
- (二)使用者端程式應相容於 Windows、MacOS、Ubuntu 等作業系統安裝之 Google Chrome、Microsoft Edge、Mozilla Firefox 及 Safari 網路瀏覽器，各類瀏覽器須支援版本及認定方式如下：
  - 1. Google Chrome 最新 Stable 版本，參閱 <https://chromestatus.com/roadmap>。
  - 2. Microsoft Edge 最新 Stable 版本，參閱 <https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-stable-channel>。
  - 3. Mozilla Firefox 最新 Release 版本，參閱 <https://www.mozilla.org/en-US/firefox/releases/>。
  - 4. MacOS Safari 13.X(含)以上版本之瀏覽器。
- (三)伺服器端程式限使用 PHP 8.1(含)以上之版本，相關套件必須皆可經由 apt 指令進行更新，並提供套件清單。
- (四)關聯式資料庫限使用 PostgreSQL；NO-SQL 資料庫限使用 MongoDB。
- (五)如有使用 Java 的服務或軟體，皆須運行於 Open JDK 11(含)以上版本。
- (六)上述軟體皆須使用 Ubuntu 22.04 套件管理服務提供之最新版本，皆須使用 apt 指令安裝與更新，未來升級至 Ubuntu 24.04 LTS 時亦同。

## 四、需求訪談

廠商應依系統功能與資通安全功能需求，設計系統操作流程、各項功能 Wireframe 及主要介面（首頁/內頁）之 UI/UX 設計風格，並規

劃系統建置策略及日後維護方式，與本校資訊處進行需求訪談後提出需求訪談報告，經本校同意後執行。

## 五、系統測試

廠商應依本專案所列各類功能（系統功能與介面）、非功能（績效與安全）需求，執行各項功能面與非功能面（含資安）之測試，並提出測試使用之工具、方法、資料來源及測試經過與發現，另對測試發現之問題應提供解決方案並提交最後完成之測試報告。

## 六、技術檢測及漏洞修補

- (一)本案於上線前及保固期間每年須完成至少 1 次主機與網頁弱點掃描及修補作業，廠商應修補中以上風險之漏洞並交付弱點掃描複測報告，做為修補及驗收佐證資料。
- (二)弱點掃描可由本校資訊處以 Nessus Pro 及 Webinspect 檢測工具執行，或由廠商自建環境執行，惟廠商使用之弱點掃描工具應更新至最新版，不得使用雲端版以避免系統漏洞資訊留存公有雲遭濫用，且符合以下功能要求，並經本校資訊處認可後執行。
- (三)主機弱點掃描檢測項目須符合 Common Vulnerabilities and Exposures(CVE)發布的弱點內容（最新版），並至少包含作業系統未修正的漏洞掃描、常用應用程式漏洞掃描、網路服務程式掃描、木馬及後門程式掃描、帳號密碼破解測試、系統之不安全與錯誤設定檢測、網路通訊埠掃描等項目。
- (四)網頁弱點掃描檢測項目應至少包含 OWASP TOP 10 2021 等漏洞。

## 七、伺服器與系統管理服務

- (一)提供系統及資料庫定期自動異機備份服務，異地備份主機與磁碟空間由本校資訊處提供
- (二)提供可手動觸發備份功能，並可變更備份使用之帳號、密碼及路徑等參數。
- (三)提供系統異常主動通報機制。

## 八、教育訓練

- (一)廠商應辦理使用者操作與系統管理技術轉移共 12 小時的教育訓練，課程內容至少包含系統操作、系統安裝 Shell Script、系統

參數設定、相關設計概念及程式碼解說。

(二)各項教育訓練內容與時數與本校資訊處討論後實施，並應於本專案時程內完成。

## 參、專案管理

### 一、專案工作計畫書

(一)廠商須於決標次日起 15 日曆天內提出專案工作計畫書，經本校資訊處審查通過後，做為工作交付及專案執行之依據。

(二)專案工作計畫書內容至少包含專案組織與成員分工、工作項目與時程、建構管理（包含紙本或電子檔案管理、程式碼版本管理與組態設定管理）及需求異動管理。

### 二、專案品質與時程管理

為確保本專案執行品質及進度，廠商於完成本專案規定工作事項前，應與本校每月至少召開一次工作會議，並撰寫會議紀錄，會議目的在檢討專案執行狀況，明定未確定事項，討論雙方應配合及協調事項。

### 三、廠商資格與專案組織

(一)廠商不得為大陸地區廠商或第三地區含陸資成分廠商。

(二)廠商不得將本專案分包給其他廠商。

(三)廠商不得將開發工作移至本國以外地區或其指定排除之國家。

(四)廠商應成立專案小組，其成員至少包含專案負責人、程式設計師與資通安全專業人員，負責本專案之各項需求規劃、協調、分析、設計、測試及資安維護等工作。

(五)專案小組成員須為廠商正職人員，不得為人力派遣公司人員或「按時」、「按月」、「按件」計酬之臨時人員、工讀生，且實際履約人員應與提出之專案小組成員名單相同。

(六)專案小組成員須具有中華民國國籍，不得為外籍勞工或大陸來台人士，廠商應提供勞健保等相關證明文件供本校審核。

(七)專案小組成員須具資訊安全相關技能，每年接受至少 3 小時資通安全教育訓練。

(八)資通安全專業人員應接受資通安全相關訓練或取得相關證照，符

合以下任一情形：

1. 課程或證照符合行政院數位發展部資通安全署網站公告之資通專業證照清單。
2. 參加依法設立 2 年以上之職業訓練機構或短期補習班或學術研究機構或財團法人或公私立大專院校開辦之課程，課程內容與資通安全策略、管理或技術訓練相關，近 3 年累計達 12 小時以上。

(九) 專案小組成員如有異動，廠商應檢附接替人員學經歷與勞健保相關證明文件，於 2 週前函報本校審核同意後更換。

(十) 對不符本專案執行需要之人員，本校得要求廠商更換，廠商應提供適當人選經本校審核通過後於 2 週內完成人員交接。

## 肆、作業期限及交付成果

### 一、作業期限

廠商應於機關決標次日起 150 日曆天內完成本專案之功能建置及系統上線工作。

### 二、交付成果

本案最後驗收須交付之項目如下：

- (一) 系統使用授權書與保固證明書各 2 份。
- (二) 需求訪談報告書面 2 份。
- (三) 系統建置手冊書面 2 份。
- (四) 系統使用操作手冊書面 2 份。
- (五) 系統功能測試報告書書面 2 份。
- (六) 弱點掃描報告書面 2 份。
- (七) 程式碼清冊（含使用之外部元件或外部軟體清單）書面 2 份。
- (八) 資料庫說明表（含 Table、View、Stored Procedure、Trigger 清單）書面 2 份。
- (九) 資通系統防護基準符合性說明書面 2 份。
- (十) 委外廠商無使用大陸廠牌資通訊設備切結書書面 2 份。
- (十一) 系統原始程式及執行檔電子檔光碟 2 份。
- (十二) 系統安裝 Shell Script。在已安裝好 Ubuntu 22.04.x 之系統執行此系統安裝 Shell Script 即可將本專案所含各項系統重建。



(十三)書面文件之電子檔光碟兩份。

#### 伍、驗收與付款方式

- 一、本案採一次驗收與付款；系統上線前，須經技術檢測無中風險以上漏洞，並經本校資訊處召開審查會議確認功能符合需求後付款。
- 二、廠商應於完成全案履約相關事宜後申請驗收，以利本校資訊處排定驗收事宜。
- 三、本案逾期違約金依契約總額千分之一計算，以契約價金總額 20%為上限。

#### 陸、保固維護及後續責任

- 一、本案保固期間為驗收合格次日起至 2024 年 12 月 31 日止，保固範圍為本專案開發之系統功能，並包含本系統環境使用的作業系統、軟體、套件及其他使用到的服務設定及更新，但 VMware VM 除外。
- 二、廠商須配合本校要求將本系統使用的 Ubuntu 作業系統、PHP、PostgreSQL 及相關服務升級指定版本，例如將 Ubuntu 升級至 24.04 LTS、PHP 升級至 PHP 8.2.X，同時進行相關程式碼、畫面、功能與服務的升級。
- 三、廠商應就本案所交付之系統功能與系統安裝 shell script 提供免費保固維護及諮詢服務。
- 四、配合本校要求每年執行一次技術檢測及漏洞修補。
- 五、廠商須指定人員，負責本專案標的物之保固維護及諮詢。
- 六、保固期間履約標的之故障維修，廠商應於接獲叫修通知起 24 個小時內進行故障排除，若是使用者端問題，得進行遠端維護服務，並於 3 日內完修。
- 七、保固期間若發生隱藏式錯誤或重大影響系統運作之程式瑕疵者，廠商須負責更正維護。

#### 柒、資通安全暨保密條款

- 一、廠商辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證，經填具「受託者查核項目表」以自評，本校得以稽核或其他適當方式確認廠商自評情形。
- 二、廠商應配置充足且經適當之資格訓練、擁有資通安全專業證照（符合行政院數位發展部資通安全署網站公告之資安專業證照清單）或具有類似業務經驗之資通安全專業人員。

- 三、廠商對於受託業務得複委託之範圍及對象，應符合專案要求並經本校審查同意，複委託之廠商仍應具備完善之資通安全維護措施或通過第三方驗證，且廠商對複委託之範圍仍應負完全責任。
- 四、廠商需具結無使用大陸廠牌資通訊產品，交付「委外廠商無使用大陸廠牌資通訊設備切結書」，並於驗收時檢視是否符合要求，作為本案驗收條件之一。
- 五、廠商於執行受託業務時，使用之資訊設備（如：筆記型電腦）應具備良善資安防護措施，如使用防毒軟體、作業系統及程式更新至最新版。
- 六、廠商如須遠端維護，採「原則禁止、例外開放」方式進行，廠商應遵守本校遠端維護要求，透過本校建置之跳板機進行維護，本校得側錄操作過程，如有特殊情形無法配合者，須經本校同意。
- 七、廠商交付電子形式檔案時，需自行檢測是否含有病毒或惡意程式。
- 八、專案如涉及資通系統之開發維運，廠商所交付之資通系統須符合「資通安全責任等級分級辦法」附表十資通系統防護基準(□高、■中、□普)的要求，驗收時須提交符合性說明，以下為驗收重點項目：
  - (一)應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。
  - (二)原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。
  - (三)於系統發展生命週期之維運階段，應執行版本控制與變更管理。
  - (四)開發、測試以及正式作業環境應為區隔。
  - (五)使用者輸入資料合法性檢查應置放於應用系統伺服器端。
- 九、專案如涉及資通系統之開發維運，廠商須依資通安全責任等級分級辦法資通系統防護基準之「系統與服務獲得」構面，重新檢視系統發展生命週期(SSDLC)於需求、設計、開發、測試、部署與維運等階段之各項安全要求，驗收時須提交「資通系統資安需求項目查檢表」(□高、■中、□普)符合性說明。
- 十、專案如涉及資通系統之開發維運，廠商於交付資通系統前，應與本校協商安全性檢測執行方式，廠商如自行或委託第三方進行安全性檢測，檢測內容至少包含應用程式弱點掃描，提交報告人員需具CEH(Certified Ethical Hacker)證照或受過該類課程訓練，廠商應修補中以上風險之漏洞，並提交修補佐證資料。
- 十一、廠商執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應 1 小時內通知本校及時採行之補救措施，須協助本校辦理資通安全事件狀況處理相關作業程序及查明原因，並於 36 小時內提供改善情形

及建議報告書。

(一)資訊資料遭洩漏。

(二)資通系統遭竄改。

(三)系統之運作受影響或停頓。

十二、本校保有對廠商進行資安稽核之權力，本校應定期或於知悉廠商發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。稽核內容包含但不限「受託者查核項目表」。

十三、廠商應遵守「資通安全管理法」、相關子法及其他公布或函文相關規定。

十四、廠商須簽署本校資通安全管理規範「合約商保密切結書」，本專案之專案人員須簽署「保密同意書」。

## 捌、其他規定

一、廠商於本案作業使用之相關軟體工具不得有侵害他人著作權或專利權之情事，否則由廠商自行負責與機關無涉。

二、本專案交付成果及各項維護增修功能、各項分析設計報告書、交付文件及檔案等，機關取得全部權利，其著作權及所有權歸屬於機關所有。

三、廠商因本案需求提供或使用之各項軟體，應依著作權等相關規定，如有違反情事發生，廠商須承擔所有法律責任，與機關無關。如因廠商違反之情事導致機關遭受損失或聲譽損害時，廠商應負一切損害賠償責任，並放棄法律之先訴抗辯權。

四、未盡事宜依照政府採購法及有關法令等規定辦理。

五、作業期間與本專案相關法規如有異動則另案辦理。

六、本專案所提功能需求為最低要求，如與需求訪談有異，以政府法規及需求訪談為主。

## 玖、企劃書內容及格式

### 一、裝訂及交付

(一)繕打方式：由左至右橫式繕打。

(二)紙張尺寸：A4 紙張雙面列印（若以 A3 格式印製，須折成 A4 格式一致大小）。

(三)裝訂方式：以左側裝訂成冊，加頁碼。

(四)份數：1 式 5 份。

- (五)封面應註明本專案名稱、投標廠商名稱及提出日期。
- (六)企劃書內容，包括其他相關文件，應以正體中文呈現；屬於原文之資料，應翻譯為中文敘述；唯專業用語仍得以原文專有名詞呈現，必要時加註說明。
- (七)交付方式：依投標須知規定於投標截止期限前蓋公司及負責人印章，以郵遞或專人送達。

## 二、一般要求

- (一)企劃書交付後，所有權歸本校所有。
- (二)製作企劃書及簽約前所需之成本，由投標廠商自行負擔。
- (三)投標文件僅提供本專案投標之用，不得引用於其它目的。
- (四)企劃書務必說明本專案之報價（費用明細）。
- (五)企劃書撰寫以不超過 40 頁（採雙面列印）為原則，頁數之計算不含應審資格證明文件、封面、封底、目錄及型錄等附件。
- (六)須提供「評審項目與廠商企劃書內容對照表」。

## 三、企劃書內容

- (一)公司簡介及相關經驗與實績說明
  - 1. 投標廠商之商譽、規模與近 3 年營運狀況。
  - 2. 投標廠商近 3 年承接類似專案經驗說明。
  - 3. 投標廠商具備相關資安認證。
- (二)專案團隊人力
  - 1. 專案組織與人力配置。
  - 2. 團隊成員履約能力與經驗。
  - 3. 專案團隊成員是否具備適當之資格訓練或擁有資通安全專業證照。
- (三)專案規劃與技術能力
  - 1. 整體系統架構，說明使用之環境架構、系統開發方法、採用技術及工具。
  - 2. 專案系統功能，說明系統功能規劃、系統操作流程與主要介面（首頁/內頁）之 UI/UX 設計風格。
  - 3. 專案資安技術，說明如何達成資通安全需求之作法，如資通系統防護基準符規、技術檢測、系統套件更新機制、軟體版本控管、系統部署方式等。

4. 教育訓練規劃與師資。
5. 保固服務規劃。
6. 專案規劃與執行管理能力，含各項工作時程控管與交付項目。
7. 專案管理、達成能力及服務品質之控管。

(四) 資通安全管理作為

1. 廠商履約程序及環境之資安管理規劃及執行方式。
2. 廠商履約相關之資安事件通報、應變、處理之規劃機制。
3. 投標廠商資安作為自評情形，填具「資安管理作業自我評估表」。

(五) 成本及費用之合理性：依本案「單價分析表」詳列，並簡述各費用分析與其他相關費用之合理性。

(六) 本系統之後續擴充建議，或其他有助於提升本專案效益之行為，但未列入專案需求者。

附表 1-資安管理作業自我評估表

資安管理作業自我評估表

日期： 年 月 日

評估項目	辦理情形
<b>1. 管理面</b>	
1.1 辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	<input type="checkbox"/> 辦理本專案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ <input type="checkbox"/> 辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) <input type="checkbox"/> 本專案受託業務之相關程序及環境未導入適當資安管理措施  備註：_____
1.2 本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	<input type="checkbox"/> 本專案之資安負責人(專案主管)為_____ <input type="checkbox"/> 本專案之資安人員為_____ <input type="checkbox"/> 本專案未指派資安負責人、資安專責主管或其他資安人員  備註：_____
1.3 本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	<input type="checkbox"/> 本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於_____文件，已(將)採取對應之控制措施詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) <input type="checkbox"/> 未就本專案進行資安風險評估  備註：_____
1.4 本專案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程	<input type="checkbox"/> 本專案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於_____文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於__小時內向甲方等相關利害關係人通報，通報對象包含_____ <input type="checkbox"/> 未就本專案訂定相關資安事件通報及應變程序  備註：_____
1.5 由招標公告日起算，過去3年是否發生因管理議題肇因之重大資安事件	<input type="checkbox"/> 過去3年無發生因管理議題肇因之資安事件 <input type="checkbox"/> 是，共__次，事件發生主要根因為_____  備註：_____
<b>2. 技術面</b>	
2.1 本專案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本專案業務所	<input type="checkbox"/> 本專案範圍內之資通系統將規劃執行_____ (如源碼掃描、弱點掃描、滲透測試)，檢測項目及本案範圍為：_____

評估項目	辦理情形
需使用之業務、行政相關資通系統，辦理安全性檢測	<input type="checkbox"/> 未就本專案範圍內之資通系統規劃安全性檢測 備註：_____
2.2辦理本專案受託業務環境及設備導入之相關資通安全防护措施	<input type="checkbox"/> 本專案受託業務之環境及設備已(將)導入(啟用)_____ (如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等)，導入項目及本案範圍為：_____ <input type="checkbox"/> 本專案受託業務之環境及設備未導入相關資通安全防护措施 備註：_____
2.3本專案範圍內之資通系統及專案資料之存取控制等權限管理機制，如 PM、系統管理員、一般使用者帳號之權限分級原則及控管方式	<input type="checkbox"/> 本專案範圍內之資通系統帳號或使用者權限分成__種等級，相關存取控制、權限管理機制說明如下：_____ <input type="checkbox"/> 未規劃本專案範圍內之資通系統及專案資料相關存取控制及權限管理機制 備註：_____
<b>3. 認知訓練面</b>	
3.1本專案直接履約相關人員之資安教育訓練	<input type="checkbox"/> 本專案直接履約相關人員之資安教育訓練包含__小時之資安通識教育訓練，對象包含____；__小時之資安專業教育訓練，對象包含____ <input type="checkbox"/> 未規劃相關資安教育訓練 備註：_____
3.2本專案團隊人員取得之資通安全專業證照	<input type="checkbox"/> 本專案具資安證照之團隊成員有：__位 <input type="checkbox"/> 本專案團隊人員未具備資通安全專業證照 備註：_____

附表 2-單價分析表

單價分析表

採購單位：國立中正大學

採購名稱：網路與資通安全管理系統建置案

單位：新臺幣元

編號	項目	單位	數量	單價	複價
1	系統功能	式	1		
1-1	網管子系統	式	1		
1-2	文件管理子系統	式	1		
1-3	帳號管理子系統	式	1		
1-4	紀錄子系統	式	1		
1-5	其他（含首頁、介接 SSO、代理人管理、電子郵件通知等其他功能）	式	1		
2	資通安全相關要求	式	1		
2-1	技術檢測與弱點修補	式	1		
2-2	資通系統防護基準符規作業	式	1		
3	教育訓練	式	1		
3-1	使用者操作教育訓練	式	1		
3-2	系統建置與日常維護技術移轉	式	1		
合 計					

註：以上單價、複價、合計等皆內含營業稅

報價廠商：

(蓋章)

負責人：

(蓋章)

地址：

電話：

營利事業統一編號：

中 華 民 國 1 1 2 年 月 日