高雄捷運股份有限公司

「110 及 111 年度資安檢測服務」工作說明書

110.03.10 資訊室制定

一、 專案說明

高雄捷運股份有限公司(簡稱本公司)為降低駭客利用本公司系統及服務漏洞進行攻擊與遵循資通安全管理法，本公司營運之捷運系統為關鍵基礎設施系統(簡稱關鍵系統)與承攬之腳踏車系統以及辦公資訊系統為檢測標的，擬委請第三方資安專業評估單位對本公司進行資安專業相關檢測與服務，提早發現潛在之資安威脅與弱點，同時藉以實施技術面與管理面相關控制措施，以改善並提升本公司各系統資安防護能力。

二、 專案目標

甲方：高雄捷運股份有限公司

乙方：得標資安專業評估單位

(一) 甲方系統包括關鍵系統、屏東公共腳踏車系統以及資訊系統等系統為本案資安檢測服務標的。

(二) 乙方提供必要之安全性檢測與資安健診，應達成下列目標：

1. 提早找出漏洞，協助甲方修補，預防並降低資安漏洞所帶來之資安威脅。
2. 模擬駭客手法，找出甲方防禦漏洞。
3. 檢視甲方網路架構、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定。
4. 檢測前與檢測後之風險分析評估。
5. 檢測報告分析並提供甲方建議資安改進方案。

三、 專案服務範圍

本案原則每年至甲方指定地點進行**安全性檢測**包括：網站安全弱點掃描檢測(含初測、複測)、主機與網路設備弱點掃描檢測(含初測、複測)、

滲透測試(含初測、複測)以及**資安健診**為檢測範圍及評估服務，為期 2 年；含初、複測服務項目算為 1 次，各項檢測服務 2 年總次數如下表與詳附件一清單：

(一) 安全性檢測

序號	項目	次數
1	網站安全弱點掃描檢測(含初、複測)	18
2	主機與網路設備弱點掃描檢測(含初、複測)	80
3	滲透測試(含初、複測)	1

(二) 資安健診

序號	項目	次數
1	網路架構檢視	8
2	網路惡意活動檢視	1
3	使用者端電腦惡意活動檢視	8
4	伺服器主機惡意活動檢視	8
5	防火牆連線設定檢視	2

四、 專案服務時程

本案依系統與系統別分別於 110 年及 111 年為期 2 年，辦理各項資安檢測作業，原則每年辦理時程如下，若甲方因業務需求得以修改檢測時程：

(一) 關鍵系統：每年 7 月開始，9 月前完成。

(二) 屏東公共腳踏車系統：每年分 2 階段 4 月開始，6 月前完成與 10 月開始，12 月前完成。

(三) 資訊系統：每年 10 月開始，12 月前完成。

五、 專案時程規定

本案服務時程，乙方須達成工作要求項目及有效管控，並預防不符合作業之情事發生與降低委外作業風險，規定說明如下：

(一) 執行檢測時程

1. 安全性檢測初測：每次以 5 日為限。

2. 安全性檢測複測：每次以 5 日為限。

3. 資安健診：每次以 5 日為限。

4. 檢測結果報告書：乙方執行安全性初測、複測與資安健診結束後 3 日內，須交付「檢測結果報告書」予甲方審視。

5. 檢測結果報告會議:乙方執行安全性初測或資安健診結束後 10 日內召開報告會議，並須於會議前 3 日交付會議簡報檔，會議結束後 5 日內交付會議記錄。

6. 檢測完成要求：乙方應依「四、專案服務時程」範圍期限內，完成本案服務事項。

（二） 資安維護時程

1. 若發生資安事件，應提供協助甲方進行改善作業之服務。

2. 資安改善方案應綜整甲方系統運行環境，提出優先改善順序。

3. 於上班時間收到甲方任何方式諮詢時，應於當日回應，若需要更多作業時間，亦需當日回覆所需處理工時與進度。

（三） 未達規定之相關罰則：詳「十、報價、驗收與付款辦法」。

六、 專案服務內容

本案安全性檢測之網站安全弱點掃描檢測、主機與網路設備弱點掃描檢測、滲透測試以及資安健診 等各檢測項目與內容應至少包含但不限於本案提出之檢測項目與內容。

（一） 檢測流程作業

1. 資料蒐集

執行檢測前，乙方應先就甲方系統架構及本項服務之標的及環境進行瞭解，對受測目標進行資料蒐集與資訊分析，以取得相關資訊作為執行本案之決策。

2. 風險管理

承上，乙方應提出對受測目標進行安全維護建議，避免發生非

預期事件造成資料或系統運作異常。在本案各項作業執行檢測前或期間，若需執行具侵入性質之檢測作業，皆須與甲方所屬系統之權責單位進行確認，並於雙方議定後之適當時間且具備適當應變措施與風險評估後，方可進行相關檢測作業。

3. 執行方式

具備資料蒐集與風險管理作業後，乙方應依工作說明書或計畫書內排定之時程執行檢測作業，應與甲方系統所屬權責單位協調後取得適當執行方式與時間後，方可執行檢測作業。

4. 分析報告

根據檢測結果，將所發現之問題與過程詳實紀錄，對結果進行統計分析，並提出檢測報告、風險評估與相關改善建議，同時乙方應主動召開討論會議(含會議簡報檔案與會議記錄)，並針對應修補之弱點進行追蹤管理，包括彙整甲方之弱點修補情形，維護未修補清單中未修補或其他原因等。

(二) 安全性檢測項目作業內容

1. 網站安全弱點掃描檢測

對甲方內外網站進行掃描，檢測項目須符合 OWSAP TOP 10 2017 項目：

(官方網站如有公布更新資訊內容，請資安評估單位以最新內容檢測)

(A) A1-Injection

(B) A2-Broken Authentication

(C) A3-Sensitive Data Exposure

(D) A4-XML External Entities (XXE)

(E) A5-Broken Access Control

(F) A6-Security Misconfiguration

(G) A7-Cross-Site Scripting (XSS)

(H) A8-Insecure Deserialization

(I) A9-Using Components with Known Vulnerabilities

(J) A10-Insufficient Logging & Monitoring

2. 主機與網路設備弱點掃描檢測

對甲方作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描的檢測項目，須符合 Common Vulnerabilities and Exposures (CVE)發布的弱點內容(最新版)，應至少包含以下項目：

(A) 作業系統未修正的漏洞掃描

(B) 常用應用程式漏洞掃描

(C) 網路服務程式掃描

(D) 木馬、後門程式掃描

(E) 帳號密碼破解測試

(F) 系統之不安全與錯誤設定檢測

(G) 網路通訊埠掃描

3. 滲透測試

檢測類型	檢測類別	檢測項目與內容(應包含但不限於下列示)
作業系統	遠端服務	至少包含遠端服務套件弱點測試等項目。
	本機服務	在已取得系統控制權限的條件下，可執行至少包含本機服務套弱點測試等項目。
網站服務	設定管理	至少包含應用程式設定測試、檔案類型處理網站爬行後端管介面及 HTTP 協定測試等項目。
	使用者認證	至少包含機敏資料是否透過加密通道進行傳送及使用者帳號列舉測試等項目。

	連線管理	至少包含 Session 管理測試、Cookie 屬性測試、 Session 資料更新測試、Session 變數傳遞測試及 CSRF 測試等項目。
	使用者授權	至少包含目錄跨越測試、網站授權機制及限控管等項邏輯漏洞。
	輸入驗證	至少包含 XSS 漏洞測試、SQL/LDAP/XML/SSI/XPath/Code Injection 測試、OS Commanding 測試及偽造 HTTP 協定測試等項目。
	Ajax	至少包含 Ajax 弱點測試等項目，如輸入驗證缺失、權限控管及套件應用程式。
應用程式	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺失、權限控管及等項目。
	檔案傳輸服務套件	至少包含 FTP、NETBIOS 及 NFS 等常見檔案傳輸服務之弱點測試，如設定缺失、權限控管及套件項目。
	遠端連線服務套件	至少包含 SSH 、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如設定缺失、權限控管及套件項目。
	網路服務套件	至少包含 DNS、PROXY 及 SNMP 等常見網路服務之弱點測試，如設定缺失、權限控管及套件項目。
	其他	包含 Firewall、IDS/IPSIDS/IPSIDS/IPS IDS/IPS、Database、LDAP 及 SMB SMB 等常見應用程式或網路套件之弱點測試項目。
密碼破解	密碼強度測試	至少包含 WEB、FTP、SSH、TELNET、SMTP SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC 及 Database 等常見對外服務之密碼字典檔測試。

（三） 資安健診項目作業內容

1. 資安健診項目

1.1 網路架構檢視

1.2 網路惡意活動檢視

1.3 使用者端電腦惡意活動檢視

1.4 伺服器主機惡意活動檢視

1.5 目錄伺服器設定及防火牆連線設定檢視

2. 資安健診內容至少包含但不限於下列工作內容：

2.1 檢視網路架構之配置、資訊設備安全管理規則之妥適性等，以評估可能之風險，採取必要因應措施。

2.2 檢視單點故障最大衝擊與風險承擔能力。

2.3 檢視對於持續營運所採取相關措施之妥適性。

2.4 進行網路封包監聽與分析，並檢視內部電腦或設備是否有對外之異常連線或 DNS 查詢等檢查。

2.5 檢視網路與資安設備紀錄檔，分析紀錄檔是否有對外異常連線紀錄。

2.6 檢視使用者電腦與伺服器之網路封包是否存在異常連線或異常網域名稱解析伺服器查詢，並比對是否為已知惡意IP、中繼站或有符合網路惡意行為的特徵。

2.7 檢測使用者電腦與伺服器是否存在惡意程式，包括具惡意行為之可疑程式、有不明連線之可疑後門程式、植入一個或多個重要系統程式之可疑函式庫、非必要之不明系統服務、具隱匿性之不明程式及駭客工具、異常帳號與群組等。

2.8 作業系統與使用者電腦與伺服器主機安裝之Microsoft 各項應用程式安全性更新作業系統或其他平台作業系統、Office 應用程式、Adobe Acrobat、Adobe flash player 及 Java 應用程式 等更新檢視，包含檢視使用者電腦是否使用已經停止支援之作業系統或軟體(如 Windows XP 或 Office 2003)針對使用者電腦防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。

2.9 針對使用者個人電腦組態設定，依行政院國家資通安全會報技術服務中心，官方網站「政府組態基準」專區所公布

安全性檢視之內容為主。

2.10 檢視防火牆的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性。

七、 專案管理需求與規劃

(一) 基本要求

1. 本案簽約日起 15 日內提出「專案服務執行計畫書」，經甲方審視並同意後，召開專案啟動會議。
2. 乙方於本案使用之各項檢測工具，包含第三方開發之產品，得提供原廠開立之合法商用授權證明(文件)予甲方備查，以符合中華民國著作權法規定，如隱瞞事實或取用未經合法授權使用之軟體，致甲方遭受任何損失或聲譽損害時，乙方應負所有損害賠償責任，若弱點掃描、滲透測試及原碼檢測之檢測工具，另須符合包括但不於 OWSAP 或其他國際資安標準規範或單位認可。
3. 本案所應用之任何掃描檢測工具應為合法商用授權版且不可為教育版，若執行檢測之設備為甲方所有，應於每次執行作業前，確認將檢測工具相關資料庫更新至最新版本；若執行檢測之設備為非為甲方所有，應於每次執行作業前，進行該設備之全機病毒掃描，期防毒軟體應為合法商用授權版，且確認所用之檢測工具相關資料庫更新至最新版本，上述作業前均須提供佐證資料。
4. 本案服務期間，乙方須依甲方需求，不定期召開會議，會議目的為檢討專案計畫執行狀況、研商待解決問題與協調事項等。乙方應由專案管理人率領主要工作人員參與，並負責撰寫會議紀錄、工作報告等。

5. 執行任何可能影響系統正常服務之檢測作業前，乙方需取得甲方授權同意後，始得執行該項檢測作業。
6. 乙方不應甲方受測標的系統升級、變更而終止服務。
7. 甲方因業務需求，於本案數量與次數範圍內可不限本案既有系統別與受測設備等標的物進行變更，乙方應予以受理，若有新增或減少，詳「十、報價、驗收與付款辦法」說明。

（二） 資安管理要求

1. 乙方於執行本案相關工作時，須確實遵守與配合甲方資安相關規範與主管機關法令法規等規定，且所有參與本案相關人員皆須簽署甲方保密協議相關文件。
2. 本案所有內容及檢測相關資訊不得揭露予非本案相關任何第三人知悉，且應採取適當及必要之保護措施。
3. 傳輸報告及機敏資料時，應將檔案壓縮加密保護，密碼交付得採用多元驗證或親自交付方式。
4. 本案執行期間，乙方如發現有疑似駭客入侵行為、跡象或重大弱點時，應立即通報甲方，並以任何溝通方式，協助甲方釐清權責及進行緊急處置，待處置完畢後始得繼續進行原檢測作業服務。
5. 本案服務執行期間若發現有風險時，乙方須提供立即轉移或控制風險之建議方案。
6. 乙方應配合甲方要求，回覆與解決本案相關資安技術問題。

（三） 組織與管理要求

1. 專案時程：依據工作說明書規定，詳「四、專案服務時程」與「五、專案時程規定」以及「八、專案期間」說明。
2. 專案工作規劃：說明專案工作範圍、執行專案工作項目所須成立之專案組織、具體可行之專案執行策略與建議方案，以及專案進行過程中所建立之執行與管控記錄。

3. 專案組織與人力：說明預計投入本案之人數、組織架構、職責分工、人力配置與人員資歷(學經歷、背景與技術專長)，專案人員除應具有相關專案參與及執行經驗外，另須具備資通安全相關資歷或資訊安全管理制度之輔導與執行實務經驗。

4. 專案成員資格要求：

4.1 本案應確保各技術人員服務水準及相互備援，檢附成員姓名、訓練證書或專業證照等認證影本，另須提出本案執行檢測服務項目之對映成員名單與相關認證以供審核，團隊成員須至少有但不限於以下認證：

(A) 資訊安全管理知識或技術：具備 CISSP (Certified Information Systems Security Professional)或 CISA(Certified Information Systems Auditor)證書或通過其他類似相關課程考試合格。

(B) 駭客技術認證:具備 CEH(Certified Ethical Hacker)證書或通過其他類似相關課程考試合格。

(C) 資安分析專家認證：具備 ECSA (EC-Council Certified Security Analyst)證書或通過其他類似相關課程考試合格。

(D) 資安鑑識調查認證：具備 CHFI (Computer Hacking Forensic Investigation) 或通過其他類似相關課程考試合格。

(E) 網路管理與封包分析：具備 CCNA(Cisco Certified Network Associate)證書、NSPA(Network Security of Packet Analysis)證書或通過其他類似相關課程考試合格。

(F) 作業系統檢視：具備 RHCE (Red Hat Certified Engineer)或 LPIC (Linux Professional Institute

Certification)或通過其他類似相關課程考試合格。

4.2 參與本案所有成員需為該公司正式員工，專案管理人須有個人五年(含)以上之資安檢測專業年資，團隊成員須有個人三年(含)以上之資安檢測專業年資，需提供本案成員之上述資格證明影本以供甲方審核。

4.3 本案專案管理人與檢測人員於本案啟動後，非經甲方同意，不得變動，本案執行期間，若本案相關人員服務不佳或違反甲方規定時，甲方得要求更換人員，乙方應配合辦理，並於十日內遞補甲方同意之同等資歷人選。

八、 專案期間

自簽約日起至 111 年 12 月 31 日止。

九、 交付項目

(一) 專案服務執行計畫書

依據「七、專案管理需求與規劃」內容制訂，應至少包括但不限於下列項目與內容：

1. 人員組織表：本案相關人員管理與執行檢測權責，並提供聯絡電話、電子郵件、通訊帳號等基本資料。
2. 本案人力至少應包含但不限於專案管理人 1 員與執行本案各項檢測作業服務人員 2 員(含)以上。
3. 工作分項表：本案每項執行作業項目、範圍、地點、職責分工、人力配置、時間時程表，並應加以甘特圖圖示。
4. 檢測執行計畫流程圖。

(二) 安全性檢測結果報告書

乙方每次執行之網站安全弱點掃描檢測、主機與網路設備弱點掃描檢測、滲透測試 等初、複測結果應轉為報告書，格式內容應符合

如下要求：

1. 依工作說明書規定時程交付，不可直接以軟體工具產生之結果作為本交付事項，須以報表或圖形化展現各類統計資料及分析說明。
2. 交付經乙方核准並完成用印之中、英文版檢測報告書(格式為A4彩色輸出)一份與電子檔。
3. 報告書項目應包括但不限於：
   3.1 執行結果摘要說明。
   3.2 掃描工具說明。
   3.3 掃描方式。
   3.4 弱點統計圖表：包含依風險等級、弱點類別排序等。
   3.5 弱點清單：包含弱點名稱、弱點描述、設備名稱、IP/URL、Port、風險等級、修補建議等。
   3.6 掃描誤判之弱點清單：說明誤判理由。
   3.7 弱點排除清單：包含說明排除理由，如無法修補原因與配套、補強性控制措施等。

(三) 資安健診檢測報告書

乙方每次執行之資安健診結果應轉為報告書，格式內容應符合如下要求：

1. 依工作說明書規定時程交付，不可直接以軟體工具產生之結果作為本交付事項，須以圖行化展現各類統計資料及說明。
2. 交付經乙方核准並完成用印之中、英文版檢測報告書(格式為A4彩色輸出)一份與電子檔。
3. 報告書項目應包括但不限於：
   3.1 執行結果摘要說明。
   3.2 檢測執行計畫書。
   3.3 各服務項目執行結果

(A) 網路架構檢視：依照網路架構安全設計、備援機制設計、網路存取管控、網路設備管理、主機設備配置等風險類型分別說明檢視結果。

(B) 使用者端電腦與伺服器主機網路惡意活動：封包監聽與分析、說明內部電腦或設備是否有對外之異常連線或 DNS 查詢，發現異常連線之電腦或設備需確認使用狀況與用途。

(C) 使用者端電腦與伺服器主機惡意程式或檔案檢視：依檢視之使用者電腦或伺服器 IP 為序，分別說明檢視結果及發現之惡意程式檔名，並針對使用者個人電腦，組態設定進行安全性檢視，並記錄測試結果。

(D) 防火牆連線設定檢視：檢視防火牆的連線設定規則，例如外網對內網、內網對外網、內網對內網是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性，並表列說明需改善之規則名稱與檢視結果，檢視結果內容如可進行匿名登入、未啟用此服務、不需提供遠端連線等資訊等。

3.4 改善建議項說明。

3.5 改善排除清單：包含說明排除理由，如無法修補原因與配套、補強性控制措施等。

（四） 專案執行過程相關記錄

歷次各項會議之會議記錄、各系統檢測結果、改善建議、發現與處置惡意行為或惡意程式之過程記錄(若有發現)、惡意程式(若有發現)、外洩資料列表(若有發現)、資安事件發現與處置之過程記錄(若有發現)等。

十、 報價、驗收與付款辦法：

（一） 報價辦法

1. 乙方報價時須依甲方估價單，填列各檢測項目與服務分項單價、數量、單位、次數與總價金額，以作為將來增減受測標的付款之依據。
2. 乙方因執行本案所衍生之各項費用均以包含在報價中。
3. 報價均以新台幣不含加值型營業稅方式報價。

（二） 驗收辦法

1. 依據本契約之工作說明書及「專案服務執行計畫書」內容進行驗收。
2. 乙方應以本案年度完成檢測作業後 30 日內，應以正式書面通知甲方進行驗收。
3. 驗收提交相關估驗資料應備妥予甲方審核，作為每次請款驗收依據，提交項目內容應包含但不限於如：各項檢測報告、會議資料 等。
4. 乙方應依本案排定時程完成各項服務作業與應交付項目予甲方簽收，每延遲 1 日(工作日)或未達「五、專案時程規定」，則扣罰契約價款千分之五作為違約金，並同意甲方得自未付價款中逕行扣除，違約金以契約總價之 25%為上限，如違約金逾25%時，甲方得以書面通知乙方終止契約或解除契約之部份或全部，且不補償乙方所生之損失，若逾 20 日(日曆天)以上，甲方得逕行解除合約。
5. 乙方應於議價後，詳列各項工作項目成本，如驗收時，經審查發現有不合格之工作項目，乙方應依期限予以改正，如未改正，甲方有權扣除該項工作之款項。

（三） 付款辦法

1. 本契約採實作實算方式分次計價，分別於乙方完成年度各項服務作業與應交付項目，經甲方確認及驗收事項無誤後，始辦理

支付本契約該次計價報表之金額，同時乙方應以正式書面提供請款相關文件(含發票)予甲方辦理付款作業。

2. 每次計價報表之金額依據訂價單所列服務項目及金額不含加值型營業稅計給，且應含實作實算估驗項目、單價、數量、單位及總價金額。
3. 甲方因業務需要，得隨時增減受測標的及決定是否將其檢測項目追加減為本案之服務範圍，乙方須配合進行必要服務，同時追加服務項目數量之計價方式將依據本契約訂價單各項服務之單價進行計價，若有新增工作項目時，得由雙方協議新單價，作為計價之依據。