醫療器材網路安全評估分析參考範本

「雲端心電圖管理系統」

衛生福利部食品藥物管理署

111 年 3 月

本範本不具法規強制性，僅提供業者建議或參考使用。

引言

本醫療器材網路安全評估分析參考範本係以衛生福利部食品藥物管理署公告之「適用於製造業者之醫療器材網路安全指引」為基礎，協助業者制定醫療器材網路安全評估報告。

本範本不具法規強制性，僅提供業者建議或參考使用。醫療器材業者如有既定網路安全評估格式，只要能涵蓋本署「適用於製造業者之醫療器材網路安全指引」範圍皆可適用。另範本所列各式文字僅供參考，醫療器材業者仍需視產品本身特性及實際操作流程擬訂，並以其為基礎執行網路安全評估。

ABC醫材股份有限公司

醫療器材網路安全評估報告
Cybersecurity Risk Assessment Report for Medical Device

雲端心電圖管理系統

報告基本資訊(Basic Information of the Report)

報告編號 (Report No.)	*CS-001*	報告版本 (Report Version)	C
公司名稱 (Company Name)	ABC醫材股份有限公司		
電話(TEL)	02-2XXXXXXX	傳真(FAX)	02-2XXXXXXX
製造業者地址 (Factory Address)	OO市OO區OO路		
審查者 (Review By)	報告製作者 (Prepared By)	評估日期 (Evaluation Period)	報告日期 (Report Date)
Paul	John	111/03	111/03

中華民國 111年3月

目 錄

1. 簡介(Introduction)

1.1 報告概述(Document Overview)

本報告包括醫療器材「雲端心電圖管理系統」之醫療器材組成元件、軟體物料清單、軟體設計暨發展、網路安全風險評鑑報告、網路安全自我檢核與檢測報告等。因此，本報告包括：

- 風險分析 The risk analysis,
- 風險評鑑報告 The risk assessment report,
- 風險追蹤矩陣 The risk traceability matrix with software requirements.

1.2 評估團隊(Evaluation Team)

表1.2.1、網路安全分析評估人員清單

姓名 Name	部門 Dept.,	職稱 Title	學歷 Education	經歷 Experience	專長 Specialty	工作年資 Seniority	責任 Responsibility
Eric	研發處	協理	OO 大學 資訊管理 博士	OO 院資通所，經理/正工程師	密碼學相關學歷 具 CEH 證照	15 年	產品安全評估，整體全面評估
Jason	研發處	經理	OO 大學資訊工程碩士	OO 院經理	具 CEH 證照	20 年	產品安全評估，開發技術主導
Paul	品質管理部	副理	XX 大學資訊工程學士	工程師/技術經理	系統整合/網站前後端開發設計/ 具 CEH 證照	15 年	產品安全評估，測試項目主導
David	研發處	技術經理	XX 大學資訊工程碩士	技術副理	系統架構研發	22 年	產品安全評估
John	品質管理部	技術副理	OO 科技大學資訊管理學士	一級專員/技術副理	系統功能測試	13 年	產品系統功能測試

1.3 引用文件(Document References)

1.3.1 引用的專案文件(Project References)

表1.3.1.1、參照技術文件

序號 #	文件編號 Document Identifier	文件標題 Document Title
1	D001	軟體確效報告

1.3.2 引用的標準與法規(Standard and Regulatory References)

表1.3.2.1、參照標準與法規

序號 # Document Identifier	文件編號 Document Identifier	文件標題 Document Title
1	ISO 14971:2019	Medical devices -- Application of risk management to medical devices
2	IEC 62304:2015	Medical device software - Software life cycle processes
3	AAMI TIR 57:2016	Principles for medical device security—Risk management
4	IEC 80001-2-8:2016	Application of risk management for IT-networks incorporating medical devices
5	NIST SP 800	Address and support the security and privacy needs of U.S. Federal Government information and information systems.

1.3.3 網路安全評估結果摘要(Summary of Cybersecurity Assessment Results)

雲端心電圖管理系統在設計之初即考量到網路安全需求，機敏性資料傳輸時採用加密之通訊協定，機敏性資料存取方面使用密碼驗證等安全機制。ABC公司已針對系統可能面對的資安風險做出風險項目評估，根據風險項目考慮對應的設計，且經過團隊內具網路安全檢測人員驗證。

ABC公司已對產品相關軟體制定檢查流程，如發現重大資訊或安全相關漏洞時，ABC公司會評估是否需要發布升級程序及更新軟體。

2. 一般要求(General Requirement)

2.1 產品簡介(Product Introduction)

2.1.1 簡介與發展程序(Development Process)

ABC公司已實施合理的管理、技術和實質保護措施，防止產品的安全事件和隱私洩露，前提是產品是按照雲端心電圖管理系統產品的使用說明所操作。然而，隨著系統和威脅的發展，沒有任何系統可以保護所有漏洞。我們認為我們的客戶是維護安全和隱私保護的最重要合作夥伴，在適當的情況下，我們將通過產品變更、技術公告或是披露相關資訊給客戶和監管機構。 ABC公司透過以下措施不斷努力提高整個產品生命週期內的安全性和隱私性：

- 隱私和安全設計
- 產品和供應商風險評估
- 漏洞和更新管理
- 安全編碼原則和分析
- 漏洞掃描和測試
- 適用於客戶數據的存取控制
- 事件應變
- 確保雙向通訊暢通無阻

本文檔的目的是詳細說明**ABC公司**安全和隱私範例如何應用於**本產品**，及您應該如何維護該產品安全的知識，以及我們如何與您合作，以確保該產品整個生命週期的安全。

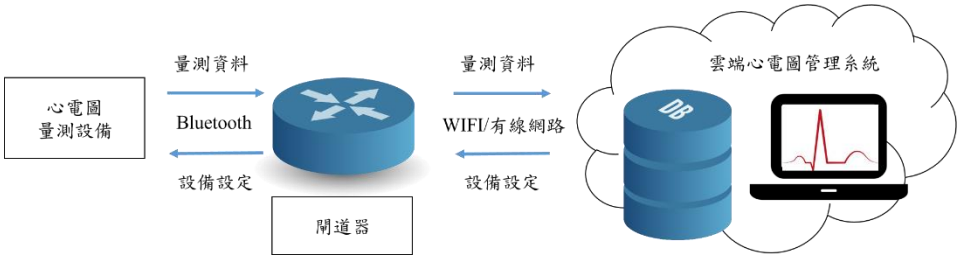
2.1.2 預期用途(Intended Use)

雲端心電圖管理系統為一個封閉場域內之雲端平台，目的在於接收、儲存、顯示成人的心電圖資訊。本產品可以透過網路持續地接受從特定設備量測的單導程心電圖資訊以及心率量測數據，醫事人員可以操作軟體，透過網路資料傳輸後檢視接收的心電圖資訊。

本產品必須由擁有專業執照的醫事人員於醫療機構或照護中心使用。本系統不適合用在急重症患者身上。

2.1.3 軟硬體系統運作架構與軟體物料清單(System Operating Architecture And Software Bill Of Materials)

本產品系統架構如下：



本系統是以自有雲架構開發的「雲端心電圖管理系統」，為純軟體的醫療器材，主要功能有：

系統設定

- 病人帳號管理、病人與心電圖量測儀配對管理。
- 心電圖設備管理：心電圖量測設備使用狀態、電量、機器資料查詢等
- 提供網路端點(URL)上傳心電圖資料
- 網路加密連線

心電圖資料管理功能

- 心電圖資料管理系統以網頁呈現，無須安裝應用程式。
- 可顯示連續即時心電圖、事件記錄心電圖
- 心電圖歷史紀錄查詢、顯示
- 網路連線均有加密保護

表2.3.1.1、ABC心電圖管理系統應用情境

應用情境	說明	資產
雲端心電圖管理系統安裝	受過訓練後的管理人員，進行系統安裝作業	心電圖管理系統、系統設定檔、管理人員帳號
心電圖量測設備配對病人	使用者透過系統設定功能綁定受測者及心電圖量測設備	心電圖管理系統、系統設定檔、使用者帳號、病人資料
心電圖量測資料傳輸	心電圖量測設備開始進行量測並透過經由加密通訊協定傳送量測資料至心電圖管理系統	心電圖管理系統、系統設定檔、心電圖量測資料
觀看病人量測資料	使用者透過心電圖資料管理功能觀察受測者心電圖	心電圖管理系統、病人資料
心電圖量測設備異常狀況通知	心電圖量測設備異常時，會顯示在心電圖管理介面網頁，以通知管理人員進行異常排除	心電圖管理系統
雲端心電圖管理系統更新	受過訓練後的管理人員，進行系統更新作業	心電圖管理系統、系統設定檔、管理人員帳號

雲端心電圖管理系統運作時所需組成元素(資產)如下表所示。

表2.3.2.2、雲端心電圖管理系統資產分類表

資產名稱	說明
程序	執行應用程式伺服器，資料庫，使用者介面，包含檔案系統之核心軟體
系統組態檔	心電圖管理系統運作時所需之組態設定，包含提供服務之網路位置設定及加密通訊所需之金鑰

機敏性資料	使用者帳號、受測者資料和受測者心電圖量測數據等
日誌資料	系統運行日誌，包含裝置對系統操作紀錄，及使用者操作管理系統之紀錄
通訊協定	心電圖量測裝置和心電圖管理系統間所使用的加密通訊協定

雲端心電圖管理系統之軟體物料清單如下：

1. Name: Django
   https://docs.djangoproject.com/en/3.2/releases/3.2.9/

發行日期	來源	版本
2021.11.01	Django Software Foundation	3.2.9

2. Name: Python 3
   https://www.python.org/downloads/release/python-380/

發行日期	來源	版本
2019.10.14	Python Software Foundation	3.8

3. Name: Docker
   https://docs.docker.com/engine/release-notes/19.03/

發行日期	來源	版本
2021.02.01	Docker, Inc.	19.03.15

4. Name: Ubuntu Linux
   https://wiki.ubuntu.com/TrustyTahr/ReleaseNotes

發行日期	來源	版本
2021.08.26	Canonical Ltd.	20.04.3

5. Name: PostgreSQL
   https://www.postgresql.org/docs/9.6/release-9-6.html

發行日期	來源	版本
2016.09.29	The PostgreSQL Global Development	9.6

6. Name: OpenSSL Library
   https://www.openssl.org/

發行日期	來源	版本
2021.09.7	OpenSSL Software Foundation	3.0.0

本產品中的資料受到密碼、權限、加密、系統內安全連接的保護。

- 密碼 – 所有帳戶都必須使用強化密碼。密碼建立規則用於確保使用者建立的密碼難以讓他人猜中。使用者需要保護好自行建立的密碼， 為保密資料的安全負責。
- 權限 - 系統依角色區分使用權限，僅授與使用者帳號運作時所需要的最低權限。

- 加密 – 傳輸資料時採用了加密來保護保密資訊，方法是除預定使用者之外的任何人均無法讀取資料 。
- 安全連接 – 資料傳輸僅透過與受信任的系統進行安全連接。

2.2 網路安全要求(Security Requirement Specification, SRS)

本產品之網路安全要求乃參照衛生福利部食品藥物管理署「適用於製造業者之醫療器材網路安全指引」[1]及行政院國家資通安全會報技術服務中心[2]所規範之資通安全需求如下表2.2.3：

表2.2.3、網路安全要求檢核表

分類	問題	答案 (是/否/不適用)	SRS
機密性	機敏資料傳輸時，採用加密機制	是	SRS-01
	機敏資料儲存時，採用加密機制	不適用	
	使用公開、國際機構驗證且未遭破解的演算法	是	SRS-02
	使用該演算法支援的最大金鑰長度	是	SRS-03
	不使用自行創造的加密方式	是	SRS-04
	加密金鑰具有保護機制	是	SRS-05
	加密金鑰或憑證週期性更換	否	
完整性	重要資料產生 HASH 值，確保其完整性	是	SRS-06
	重要資料傳輸過程，使用防止竄改的協定	是	SRS-07
	提供下載的資料，產生 HASH 值供比對其完整性	不適用	
可用性	評估服務重要性，設定可用性要求	否	
	採用「高可用性」(High Availability) 架構或機制	否	
	重要資料定時同步至備援環境	是	SRS-08
輸入驗證	採用過濾機制，以防止輸入惡意命令或資料	否	
	驗證使用者輸入資料	是	SRS-09
	驗證外部取得的資料	不適用	
	驗證系統參數合理性	是	SRS-10

[1] 衛生福利部食品藥物管理署. (2021). 適用於製造業者之醫療器材網路安全指引. Available: https://www.fda.gov.tw/TC/newsContent.aspx?cid=3&id=27018

[2] 行政院國家資通安全會報技術服務中心. 系統安全發展流程實務.

	於伺服器端檢查輸入資料合法性	否	
身分認證	除了允許匿名存取的功能外，所有功能都必須經過認證才允許存取	不適用	
	身分認證機制位於伺服端且採用集中管理機制	是	SRS-11
	採用多重因素認證(兩種以上認證類型)	不適用	
	採用 CAPTCHA 機制於身分認證或重要交易行為，以防範自動化程式之嘗試	不適用	
	身分認證相關資訊不以明文傳輸	是	SRS-12
	身分認證相關資訊不存於源碼中，並限制存取	是	SRS-13
	身分認證失敗達一定次數後鎖定該帳號	不適用	
	身分認證發生錯誤時，預設不允許存取任何功能	是	SRS-14
	密碼添加亂數資料(Salt)後進行雜湊函數(HASH)處理，才加以儲存	不適用	
	密碼須符合複雜度(長度限制、具備英文大小寫及特殊字元等)	是	SRS-15
	限制需定期更換密碼	不適用	
	重要交易行為要求再次身分認證	不適用	
授權與存取控制	採用伺服端的集中管理機制檢查使用者授權	是	SRS-16
	執行功能或存取資源前，檢查使用者授權	否	
	除特殊管理者權限外，其他角色或權限無法修改授權資料及存取控制列表(ACL)	是	SRS-17
	使用者/角色賦予所需的最小權限	是	SRS-18
	軟體程序(process)以最小的權限執行，不以系統管理員或最高權限執行	是	SRS-19
	重要行為由多人/角色授權後才得以進行	不適用	
日誌紀錄	認證失敗、存取失敗、輸入驗證失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行 Log 記錄	是	SRS-20
	Log 紀錄考慮包含以下項目 1.識別使用者之 ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型(例如，成功或失敗)。5.事件優先權(priority)。6. 事件詳細描述。7.事件代碼。8.網路位址	是	SRS-21

	採用單一的 Log 機制，確保輸出格式的一致性	是	SRS-22
	Log 進行適當保護及備份，避免未經授權存取	是	SRS-23
會話管理	會話識別碼(Session ID)是隨機產生且不可預測	是	SRS-24
	使用者的會話階段，設定在合理的時間內失效	是	SRS-25
	使用者的會話階段，使用者登出後失效	不適用	
	使用者重新登入後，會話識別碼(Session ID)會改變	是	SRS-26
	不將會話識別碼(Session ID)或使用者 ID 顯示於使用者可以改寫處	不適用	
錯誤及例外管理	所有的功能都會進行錯誤及例外處理，並將資源正確釋放	是	SRS-27
	軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息及代碼，不包含詳細的錯誤訊息或除錯用訊息	是	SRS-28
	嚴重錯誤採用通知機制(例如電子郵件或簡訊)	否	
組態管理	管理者介面限制存取來源或不允許遠端存取	不適用	
	參數設定或系統設定存放處，限制存取或進行適當保護	是	SRS-29
	依賴的外部元件或軟體，不使用預設帳號密碼	是	SRS-30
	作業平台定期更新、關閉不必要服務、注意安全設定	不適用	
	依賴的外部元件或軟體，注意其安全漏洞通告，必要時評估更新	不適用	

本產品根據上述自主檢查表，確認網路安全要求如表2.2.4：

表2.2.4、適用項目需求分析

SRS 編號 No. (SRS)	網路安全要求規格說明(Security Requirement Specification SRS Description)
SRS-01	使用者帳號及心電圖量測資料傳送時需採用加密通訊協定
SRS-02	資料傳輸加密通訊協定及使用者機敏性資料應使用公開、國際機構驗證且未遭破解的演算法
SRS-03	心電圖管理系統內選用之加密演算法使用安全機構建議支援的金鑰長度
SRS-04	心電圖管理系統內選用之加密演算法須為非自行創造的加密方式
SRS-05	心電圖管理系統內選用之加密金鑰具有保護機制

SRS-06	心電圖管理系統內使用者密碼產生 HASH 值，確保其完整性
SRS-07	重要資料傳輸過程，使用防止竄改的協定
SRS-08	心電圖管理系統重要資料定時同步至備援環境
SRS-09	心電圖管理系統需驗證使用者輸入資料
SRS-10	心電圖系統安裝時需驗證系統參數合理性
SRS-11	心電圖管理系統身分認證機制位於伺服端且採用集中管理機制
SRS-12	心電圖管理系統身分認證相關資訊不以明文傳輸
SRS-13	心電圖管理系統身分認證相關資訊不存於源碼中，並限制存取
SRS-14	心電圖管理系統身分認證發生錯誤時，預設不允許存取任何功能
SRS-15	心電圖管理系統使用之密碼須符合複雜度(長度限制且具備英文大小寫或特殊字元等)
SRS-16	心電圖管理系統採用伺服端的集中管理機制檢查使用者授權
SRS-17	心電圖管理系統除特殊管理者權限外，其他角色或權限無法修改授權資料及存取控制列表(ACL)
SRS-18	心電圖管理系統使用者/角色賦予所需的最小權限
SRS-19	軟體程序(process)以最小的權限執行，不以系統管理員或最高權限執行
SRS-20	心電圖管理系統認證失敗、存取失敗、輸入驗證失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行 Log 記錄
SRS-21	心電圖管理系統 Log 紀錄包含以下項目 1.識別使用者之 ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型。5.事件優先權(priority)。6. 事件詳細描述。7.事件代碼。8.網路位址
SRS-22	心電圖管理系統採用單一運行紀錄機制，確保輸出格式的一致性致性
SRS-23	心電圖管理系統運行紀錄進行適當保護及備份，避免未經授權存取
SRS-24	心電圖管理系統會話識別碼(Session ID)是隨機產生且不可預測
SRS-25	心電圖管理系統使用者的會話階段，設定在合理的時間內失效
SRS-26	心電圖管理系統使用者重新登入後，會話識別碼(Session ID)會改變
SRS-27	心電圖管理系統所有的功能都會進行錯誤及例外處理，並將資源正確釋放
SRS-28	心電圖管理系統軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息及代碼，不包含詳細的錯誤訊息或除錯用訊息
SRS-29	心電圖管理系統參數設定或系統設定存放處，限制存取或進行適當保護
SRS-30	心電圖管理系統依賴的外部元件或軟體，不使用預設帳號密碼

2.3 網路安全細部設計(Security Detail Design, SDD)

本產品網路安全細部設計(Security Detail Design, SDD)，根據SRS的要求落實於產品，確認本產品之網路安全要求。

表2.3.1、網路安全細部設計

SDD編號 **No. (SDD)**	網路安全設計規格說明(Security Detail Design SDD Description)
SDD-01	心電圖管理系統中的資料傳輸皆透過 TLS 1.2 或 TLS 1.3 進行資料加密(非明文傳輸)，並防止被竄改
SDD-02	採用 NIST Special Publication 800-57 Part 3 建議，使用 2048 bit 長度金鑰
SDD-03	加密金鑰位於受保護之檔案系統內，需具系統管理權限才能進行存取
SDD-04	帳號密碼使用 PBKDF2 演算法並使用 SHA256 進行 Hash
SDD-05	心電圖管理系統重要資料定時同步至備援環境
SDD-06	心電圖管理系統對於資料輸入進行驗證檢查
SDD-07	心電圖管理系統在安裝時進行參數設置檢查
SDD-08	使用心電圖管理系統採用 Client/Server 架構，帳號皆須透過伺服端進行認證
SDD-09	心電圖管理系統帳號密碼存於伺服端，需授權存取，且身分認證發生錯誤時，不允許存取任何功能
SDD-10	心電圖管理系統密碼要求長度6碼以上且具備英文大小寫或有特殊字元
SDD-11	心電圖管理系統之使用者會在登入時依角色授與適當權限
SDD-12	心電圖管理系統之使用者權限於伺服端集中控管，只有系統管理者具權限調整存取控制列表
SDD-13	心電圖管理系統透過存取控制列表給予使用者操作時所需最低權限，客戶端只具有維護權限
SDD-14	心電圖管理系統執行之服務程序以最小的權限執行，不以系統管理員或最高權限執行
SDD-15	心電圖管理系統各項服務程序皆有運行紀錄，並依嚴重程度區分紀錄等級
SDD-16	心電圖管理系統運行紀錄包含以下項目 1.識別使用者之ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型。5.事件優先權(priority)。6.事件詳細描述。7.事件代碼。8.網路位址
SDD-17	心電圖管理系統皆採 rsyslog 運行紀錄機制
SDD-18	心電圖管理系統運行紀錄存於伺服端，需授權存取，並於系統維護週期內進行人工備份
SDD-19	心電圖管理系統身份認證機制其會話識別碼(Session ID)是隨機產生且不可預測
SDD-20	心電圖管理系統身份認證機制其使用者的會話階段，設定在合理的時間內失效
SDD-21	心電圖管理系統使用者重新登入後，會話識別碼(Session ID)會改變
SDD-22	心電圖管理系統所有的功能都會進行錯誤及例外處理，並將資源正確釋放

SDD-23	心電圖管理系統軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息及代碼，不包含詳細的錯誤訊息或除錯用訊息
SDD-24	心電圖管理系統參數設定或系統設定存放處，限制存取或進行適當保護，只有管理理帳號可進行系統參數設定及存取
SDD-25	心電圖管理系統依賴的外部元件或軟體，不使用預設帳號密碼

2.4 網路安全驗證確效測試(Security Validation & Verification, SVV)

表 2.4.1、網路安全驗證確效測試(測試1)

測試編號	SVV-01
軟體版本	V1.0.0
測試項目	使用者帳號及心電圖量測資料傳送時需採用加密通訊協定
測試人員	John
測試日期	2021/05/27
測試方法依據	使用工具確認伺服端與瀏覽器間通訊協定採用 TLS 1.2 或 TLS 1.3 進行
測試通過標準	1. 登入網址後使用瀏覽器開發工具看到Security的連線通訊協定採用TLS 1.3 2. 於client使用wireshark抓取封包 3. 透過 wireshark 輸入 ip.addr == PTMS_IP filter之後，傳輸的 protocol 顯示 TSLv1.2 或 TSLv1.3
測試結果	Pass

表 2.4.2、網路安全驗證確效測試(測試2)

測試編號	SVV-02
軟體版本	V1.0.0
測試項目	資料傳輸加密通訊協定及使用者機敏性資料應使用公開、國際機構驗證且未遭破解的演算法
測試人員	John
測試日期	2021/05/27
測試方法依據	使用工具確認伺服端與瀏覽器間通訊協定採用 TLS 1.2 或 TLS 1.3 進行
測試通過標準	1. 登入網址後使用瀏覽器開發工具看到Security的連線通訊協定採用TLS 1.3 2. 於client使用wireshark抓取封包 3. 透過 wireshark 輸入 ip.addr == PTMS_IP filter之後，傳輸的 protocol 顯示 TSLv1.2 或 TSLv1.3
測試結果	Pass

表 2.4.3、網路安全驗證確效測試(測試3)

測試編號	SVV-03
軟體版本	V1.0.0
測試項目	心電圖管理系統內選用之加密演算法使用安全機構建議支援的金鑰長度
測試人員	John
測試日期	2021/05/27
測試方法依據	採用 NIST Special Publication 800-57 Part 3 建議，使用 2048 bit 長度金鑰，使用瀏覽器開發工具觀察測試伺服端與瀏覽器間通訊協定採用金鑰長度為 2048 bit
測試通過標準	使用 Chrome 瀏覽器開發工具於 Security 下開啟”Open full certificate details”，並於詳細資料內的公開金鑰需顯示RSA(2048 Bits)
測試結果	Pass

表 2.4.4、網路安全驗證確效測試(測試4)

測試編號	SVV-04
軟體版本	V1.0.0
測試項目	心電圖管理系統內選用之加密演算法須為非自行創造的加密方式
測試人員	John
測試日期	2021/05/27
測試方法依據	使用工具確認伺服端與瀏覽器間通訊協定採用 TLS 1.2 或 TLS 1.3 進行
測試通過標準	1. 登入網址後使用瀏覽器開發工具看到Security的連線通訊協定採用TLS 1.3 2. 於client使用wireshark抓取封包 3. 透過 wireshark 輸入 ip.addr == PTMS_IP filter之後，傳輸的 protocol 顯示 TSLv1.2 或 TSLv1.3
測試結果	Pass

表 2.4.5、網路安全驗證確效測試(測試5)

測試編號	SVV-05
軟體版本	V1.0.0
測試項目	心電圖管理系統內選用之加密金鑰具有保護機制
測試人員	John
測試日期	2021/05/27

測試方法依據	加密金鑰位於受保護之檔案系統內，需具系統管理權限才能進行存取
測試通過標準	1. 以系統管理者帳號登入系統 2. 確認加密金鑰存放於受保護之檔案系統內，且可進行存取。
測試結果	Pass

表 2.4.6、網路安全驗證確效測試(測試6)

測試編號	SVV-06
軟體版本	V1.0.0
測試項目	心電圖管理系統內使用者密碼產生HASH值，確保其完整性
測試人員	John
測試日期	2021/05/27
測試方法依據	1. 帳號密碼使用 PBKDF2 演算法並使用 SHA256 進行 Hash 2. 創建一個新的使用者帳號可以正常登入網站且其密碼為 hash值
測試通過標準	1. 創建一個使用者帳號並確認使用者帳號可以登入系統 2. 以後台管理工具觀查密碼是否為 hash 值
測試結果	Pass

表 2.4.7、網路安全驗證確效測試(測試7)

測試編號	SVV-07
軟體版本	V1.0.0
測試項目	重要資料傳輸過程，使用防止竄改的協定
測試人員	John
測試日期	2021/05/27
測試方法依據	使用標準的TLSv1.2或TLSv1.3進行資料加密，並防止被竄改
測試通過標準	1. 登入網址後使用瀏覽器開發工具看到Security的連線通訊協定採用TLS 1.3 2. 於client使用wireshark抓取封包 3. 透過 wireshark 輸入 ip.addr == PTMS_IP filter之後，傳輸的 protocol 顯示 TSLv1.2 或 TSLv1.3
測試結果	Pass

表 2.4.8、網路安全驗證確效測試(測試8)

測試編號	SVV-08
軟體版本	V1.0.0
測試項目	心電圖管理系統重要資料定時同步至備援環境

測試人員	John
測試日期	2021/05/27
測試方法依據	1. 系統設定檔同步於兩台機器間 2. 資料庫資料同步於兩台機器間
測試通過標準	1. 系統設定檔可同步於兩台機器間 2. 資料庫資料可同步於兩台機器間
測試結果	Pass

表 2.4.9、網路安全驗證確效測試(測試9)

測試編號	SVV-09
軟體版本	V1.0.0
測試項目	心電圖管理系統對於資料輸入進行驗證檢查
測試人員	John
測試日期	2021/05/27
測試方法依據	1. 使用者輸入不合法資料，系統不接受輸入結果並顯示錯誤訊息 2. 使用者輸入不合法數值範圍，系統不接受輸入結果並顯示錯誤訊息
測試通過標準	1. 使用者輸入不合法資料，系統不接受輸入結果並顯示錯誤訊息 2. 使用者輸入不合法數值範圍，系統不接受輸入結果並顯示錯誤訊息
測試結果	Pass

表 2.4.10、網路安全驗證確效測試(測試10)

測試編號	SVV-10
軟體版本	V1.0.0
測試項目	心電圖系統安裝時需驗證系統參數合理性
測試人員	John
測試日期	2021/05/27
測試方法依據	進行系統安裝時輸入不合法數值，安裝程式回報錯誤並顯示參數錯誤訊息
測試通過標準	1. 進行系統安裝時輸入不合法 IP 位址 2. 安裝程式回報錯誤並顯示參數錯誤訊息
測試結果	Pass

表 2.4.11、網路安全驗證確效測試(測試11)

測試編號	SVV-11
軟體版本	V1.0.0

測試項目	身分認證機制位於伺服端且採用集中管理機制
測試人員	John
測試日期	2021/05/27
測試方法依據	1. 使用心電圖管理系統採用 Client/Server 架構，帳號皆須透過伺服端進行認證。 2. 於登入輸入未建立之使用者帳號密碼將回傳錯誤訊息 3. 於登入輸入已建立之使用者帳號密碼將成功登入
測試通過標準	1. 登入心電圖系統介面時，輸入錯誤的帳號密碼後，無法登入且會有錯誤提示告知使用者(operation denied, please check your account and permissions) 2. 登入心電圖系統介面時，輸入正確的帳號密碼後即可成功登入首頁並繼續其他功能操作
測試結果	Pass

表 2.4.12、網路安全驗證確效測試(測試12)

測試編號	SVV-12
軟體版本	V1.0.0
測試項目	心電圖管理系統身分認證相關資訊不以明文傳輸
測試人員	John
測試日期	2021/05/27
測試方法依據	於登入頁面輸入已建立之使用者帳號及密碼後，以網路封包觀察工具確認封包沒有以明文傳送密碼欄位
測試通過標準	1. 於client使用wireshark抓取封包 2. 於ECG首頁輸入已建立之使用者帳號及密碼並登入 3. 透過 wireshare 抓封包時開啟 find the packet 並選擇 Packet details 且輸入帳號搜尋並無資訊
測試結果	Pass

表 2.4.13、網路安全驗證確效測試(測試13)

測試編號	SVV-13
軟體版本	V1.0.0
測試項目	心電圖管理系統帳號密碼存於伺服端，需授權存取，且身分認證發生錯誤時，不允許存取任何功能
測試人員	John
測試日期	2021/05/27
測試方法依據	1. 新增一使用者，確認新增之使用者正確/錯誤密碼身分驗證是否正確。

	2. 變更一已存在之使用者密碼，確認新密碼是否可用於身分認證，舊密碼是否失效。 3. 刪除一已存在之使用者，確認該使用者是否能用於身分認證。 4. 確認身份認證資訊位存取是否需系統管理員權限。 5. 隨機輸入不符合之帳號密碼，確認無法存取任何功能。
測試通過標準	1. 新增一使用者，確認新增之使用者正確/錯誤密碼身分驗證是否正確。 2. 變更一已存在之使用者密碼，確認新密碼是否可用於身分認證，舊密碼是否失效。 3. 刪除一已存在之使用者，確認該使用者是否能用於身分認證。 4. 確認身份認證資訊位存取是否需系統管理員權限。 5. 輸入不符合之帳號密碼，無法存取任何功能。
測試結果	Pass

表 2.4.14、網路安全驗證確效測試(測試14)

測試編號	SVV-14
軟體版本	V1.0.0
測試項目	心電圖管理系統使用之密碼須符合複雜度(長度限制且具備英文大小寫或特殊字元等)
測試人員	John
測試日期	2021/05/27
測試方法依據	1. 於系統創建帳號時輸入小於六位字元之密碼，帳號將無法建立並顯示錯誤訊息 2. 於系統創建帳號時輸入全英文小寫之密碼，帳號將無法建立並顯示錯誤訊息 3. 於系統創建帳號時輸入全英文大寫之密碼，帳號將無法建立並顯示錯誤訊息 4. 於系統創建帳號時輸入無英文之密碼，帳號將無法建立並顯示錯誤訊息
測試通過標準	1. 輸入小於六位字元之密碼，帳號無法建立並顯示錯誤訊息 2. 輸入全英文小寫之密碼，帳號無法建立並顯示錯誤訊息 3. 輸入全英文大寫之密碼，帳號無法建立並顯示錯誤訊息 4. 輸入無英文之密碼，帳號無法建立並顯示錯誤訊息
測試結果	Pass

表 2.4.15、網路安全驗證確效測試(測試15)

測試編號	SVV-15
軟體版本	V1.0.0

測試項目	心電圖管理系統採用伺服端的集中管理機制檢查使用者授權
測試人員	John
測試日期	2021/05/27
測試方法依據	於登入輸入未建立之使用者帳號密碼無法正常登入且回傳錯誤訊息
測試通過標準	1. 登入雲端心電圖中控儀表板時，輸入錯誤的帳號密碼後，會有錯誤提示告知使用者(The username and/or password you specified are not correct) 2. 登入雲端心電圖監測管理軟體時，輸入錯誤的帳號密碼後，會有錯誤提示告知使用者(The username and/or password you specified are not correct)
測試結果	Pass

表 2.4.16、網路安全驗證確效測試(測試16)

測試編號	SVV-16
軟體版本	V1.0.0
測試項目	心電圖管理系統除系統管理者權限外，其他角色或權限無法修改授權資料及存取控制列表(ACL)
測試人員	John
測試日期	2021/05/27
測試方法依據	1. 登入具系統管理者權限之帳號，確認可以更改存取控制列表 2. 登入非系統管理者權限之帳號，確認無法存取控制列表
測試通過標準	1. 使用系統管理者權限帳號登入後台可以更改存取控制列表 2. 使用非系統管理者權限帳號無法登入後台且無法存取控制列表
測試結果	Pass

表 2.4.17、網路安全驗證確效測試(測試17)

測試編號	SVV-17
軟體版本	V1.0.0
測試項目	心電圖管理系統使用者/角色賦予所需的最小權限
測試人員	John
測試日期	2021/05/27
測試方法依據	一般使用者無法存取系統設定檔
測試通過標準	一般使用者登入心電圖管理系統後，無法看到系統設定檔
測試結果	Pass

表 2.4.18、網路安全驗證確效測試(測試18)

測試編號	SVV-18
軟體版本	V1.0.0
測試項目	軟體程序(process)以最小的權限執行，不以系統管理員或最高權限執行
測試人員	John
測試日期	2021/05/27
測試方法依據	軟體程序 (process) 以非 root 角色執行
測試通過標準	1. 登入伺服端系統管理者權限之帳號 2. 確認心電圖管理系統以非 root 角色執行
測試結果	Pass

表 2.4.19、網路安全驗證確效測試(測試19)

測試編號	SVV-19
軟體版本	V1.0.0
測試項目	心電圖管理系統認證失敗、存取失敗、輸入驗證失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行 Log 記錄
測試人員	John
測試日期	2021/05/27
測試方法依據	心電圖管理系統執行重要操作時，會記錄對應的 log
測試通過標準	於心電圖管理系統內執行下列動作 1. 認證失敗：確認系統紀錄檔內含有上述動作紀錄 2. 存取失敗：確認系統紀錄檔內含有上述動作紀錄 3. 輸入驗證失敗：確認系統紀錄檔內含有上述動作紀錄 4. 功能錯誤：確認系統紀錄檔內含有上述動作紀錄 5. 管理者行為：確認系統紀錄檔內含有上述動作紀錄
測試結果	Pass

表 2.4.20、網路安全驗證確效測試(測試20)

測試編號	SVV-20
軟體版本	V1.0.0
測試項目	心電圖管理系統 Log 紀錄包含以下項目 1.識別使用者之ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型。5.事件優先權(priority)。6.事件詳細描述。7.事件代碼。8.網路位址
測試人員	John

測試日期	2021/05/27
測試方法依據	心電圖管理系統紀錄檔需包含各類重要紀錄
測試通過標準	於心電圖管理系統內執行下列動作 1. 認證失敗後，Log 記錄檔包含以下項目: (1).識別使用者之ID(不可為個資類型)。(2).經系統校時後的時間戳記。(3).執行的功能或存取的資源。(4).事件類型。(5).事件優先權(priority)。(6).事件詳細描述。(7).事件代碼。(8).網路位址 2. 存取失敗後，Log 記錄檔包含以下項目: (1).識別使用者之ID(不可為個資類型)。(2).經系統校時後的時間戳記。(3).執行的功能或存取的資源。(4).事件類型。(5).事件優先權(priority)。(6).事件詳細描述。(7).事件代碼。(8).網路位址 3. 輸入驗證失敗後，Log 記錄檔包含以下項目: (1).識別使用者之ID(不可為個資類型)。(2).經系統校時後的時間戳記。(3).執行的功能或存取的資源。(4).事件類型。(5).事件優先權(priority)。(6).事件詳細描述。(7).事件代碼。(8).網路位址 4. 功能錯誤後，Log 記錄檔包含以下項目: (1).識別使用者之ID(不可為個資類型)。(2).經系統校時後的時間戳記。(3).執行的功能或存取的資源。(4).事件類型。(5).事件優先權(priority)。(6).事件詳細描述。(7).事件代碼。(8).網路位址 5. 管理者行為後，Log 記錄檔包含以下項目: (1).識別使用者之ID(不可為個資類型)。(2).經系統校時後的時間戳記。(3).執行的功能或存取的資源。(4).事件類型。(5).事件優先權(priority)。(6).事件詳細描述。(7).事件代碼。(8).網路位址
測試結果	Pass

表 2.4.21、網路安全驗證確效測試(測試21)

測試編號	SVV-21
軟體版本	V1.0.0
測試項目	心電圖管理系統採用單一運行紀錄機制，確保輸出格式的一致性
測試人員	John
測試日期	2021/05/27
測試方法依據	心電圖管理系統紀錄格式需一致
測試通過標準	心電圖管理系統皆採 rsyslog 運行紀錄機制，存取紀錄與事件紀錄格式一致均包含下列欄位 1. 時間 2. 事件分類 3. 來源 4. 事件描述

測試結果	Pass

表 2.4.22、網路安全驗證確效測試(測試22)

測試編號	SVV-22
軟體版本	V1.0.0
測試項目	心電圖管理系統運行紀錄進行適當保護及備份，避免未經授權存取
測試人員	John
測試日期	2021/05/27
測試方法依據	確認系統日誌僅能由具系統管理權限帳號存取
測試通過標準	1. 系統管理權限帳號登入系統可以存取系統日誌 2. 非系統管理權限帳號登入系統無法存取系統日誌並顯示 Permission denied
測試結果	Pass

表 2.4.23、網路安全驗證確效測試(測試23)

測試編號	SVV-23
軟體版本	V1.0.0
測試項目	心電圖管理系統會話識別碼(Session ID)是隨機產生且不可預測
測試人員	John
測試日期	2021/05/27
測試方法依據	1. 登入兩個不同之使用者帳號，確認會話識別碼不同 2. 登入同個使用者帳號兩次，確認會話識別碼不同
測試通過標準	1. 透過瀏覽器開發工具 Network 內的 Request header 之 session id 來確認登入兩個不同之使用者帳號，確認會話識別碼會不同 2. 透過瀏覽器開發工具 Network 內的 Request header 之 session id 來確認登入相同使用者帳號兩次，確認會話識別碼會不同
測試結果	Pass

表 2.4.24、網路安全驗證確效測試(測試24)

測試編號	SVV-24
軟體版本	V1.0.0
測試項目	心電圖管理系統使用者的會話階段，設定在合理的時間內失效
測試人員	John
測試日期	2021/05/27
測試方法依據	登入使用者所屬會話階段在系統預設時間失效

測試通過標準	確認登入使用者所屬會話階段在系統預設時間失效
測試結果	Pass

表 2.4.25、網路安全驗證確效測試(測試25)

測試編號	SVV-25
軟體版本	V1.0.0
測試項目	心電圖管理系統使用者重新登入後，會話識別碼(Session ID)會改變
測試人員	John
測試日期	2021/05/27
測試方法依據	確認心電圖管理系統使用者重新登入後，會話識別碼(Session ID)會改變
測試通過標準	透過瀏覽器開發工具 Network 內的 Request header 之 session id 來確認登入使用者帳號與登出後再次登入的會話識別碼不相同
測試結果	Pass

表 2.4.26、網路安全驗證確效測試(測試26)

測試編號	SVV-26
軟體版本	V1.0.0
測試項目	心電圖管理系統所有的功能都會進行錯誤及例外處理，並將資源正確釋放
測試人員	John
測試日期	2021/05/27
測試方法依據	量測期間內的資源使用率以及錯誤例外處理
測試通過標準	心電圖量測期間，系統處理器，記憶體，磁碟空間使用率皆在監控數值範圍內，於非尖峰使用時監控數值穩定
測試結果	Pass

表 2.4.27、網路安全驗證確效測試(測試27)

測試編號	SVV-27
軟體版本	V1.0.0
測試項目	心電圖管理系統軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息或代碼，不包含詳細的錯誤訊息或除錯用訊息
測試人員	John
測試日期	2021/05/27

測試方法依據	心電圖管理系統於使用者介面之錯誤訊息提示
測試通過標準	確認心電圖管理系統軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息及代碼，不包含詳細的錯誤訊息或除錯用訊息
測試結果	Pass

表 2.4.28、網路安全驗證確效測試(測試28)

測試編號	SVV-28
軟體版本	V1.0.0
測試項目	心電圖管理系統參數設定或系統設定存放處，限制存取或進行適當保護
測試人員	John
測試日期	2021/05/27
測試方法依據	確認心電圖管理系統參數設定或系統設定存放處，僅供具有系統管理權限帳號進行存取
測試通過標準	1. 只有系統管理權限帳號可以登入後台並存取，非系統管理權限帳號無法登入後台 2. 只有系統管理權限帳號可以存取下列路徑下的資訊，一般管理帳號無法存取 (顯示 Permission denied) ● /opt/debs ● /opt/sweeper ● /opt/siuser 路徑下皆不能存取
測試結果	Pass

表 2.4.29、網路安全驗證確效測試(測試29)

測試編號	SVV-29
軟體版本	V1.0.0
測試項目	心電圖管理系統依賴的外部元件或軟體，不使用預設帳號密碼
測試人員	John
測試日期	2021/05/27
測試方法依據	確認心電圖管理系統依賴的外部元件或軟體，不可使用預設帳號密碼登入
測試通過標準	1. 訊息服務元件預設帳密 guest/guest 無法正常登入(顯示Login failed)) 2. 資料庫預設帳密 postgres/postgres，執行 psql -h IP -U postgres -W 並輸入密碼 postgres會顯示 psql: error: could not connect to server: Connection refused
測試結果	Pass

2.5 追溯性矩陣(Traceability Matrix)

表2.5.1、追溯性矩陣

軟體需求編號	軟體設計規格編號	軟體 V&V 測試編號
SRS-01	SDD-01	SVV-01
SRS-02	SDD-01	SVV-02
SRS-03	SDD-02	SVV-03
SRS-04	SDD-01	SVV-04
SRS-05	SDD-03	SVV-05
SRS-06	SDD-04	SVV-06
SRS-07	SDD-01	SVV-07
SRS-08	SDD-05	SVV-08
SRS-09	SDD-06	SVV-09
SRS-10	SDD-07	SVV-10
SRS-11	SDD-08	SVV-11
SRS-12	SDD-01	SVV-12
SRS-13	SDD-09	SVV-13
SRS-14	SDD-09	SVV-13
SRS-15	SDD-10	SVV-14
SRS-16	SDD-11	SVV-15
SRS-17	SDD-12	SVV-16
SRS-18	SDD-13	SVV-17
SRS-19	SDD-14	SVV-18
SRS-20	SDD-15	SVV-19
SRS-21	SDD-16	SVV-20
SRS-22	SDD-17	SVV-21
SRS-23	SDD-18	SVV-22
SRS-24	SDD-19	SVV-23
SRS-25	SDD-20	SVV-24
SRS-26	SDD-21	SVV-25
SRS-27	SDD-22	SVV-26
SRS-28	SDD-23	SVV-27
SRS-29	SDD-24	SVV-28
SRS-30	SDD-25	SVV-29

3. 網路安全評估(Cybersecurity Assessment)

3.1 網路安全評估計畫(Cybersecurity Assessment Plan)

本產品參照 NIST SP 800 標準，針對產品進行：

- 本產品軟硬體元件之盤點與分類
- 本產品之網路安全威脅建模
- 本產品之網路安全風險評估
- 本產品之網路安全風險控制措施
- 本產品之網路安全檢測與報告

3.1.1 網路安全威脅建模方法(Security Requirement Specification & Threat Modeling)

網路安全威脅建模包括：

1. 識別資產
2. 產生資料流向圖（Data Flow Diagram, DFD）
3. 分析網路安全威脅。在DFD中每一類部件都有對應STRIDE [假冒（Spoofing）、篡改（Tampering）、否認性（Repudiation）、資訊泄露（Information disclosure）、阻斷服務（Denial of service）、權限提高（Elevation of privilege）]模型威脅。輸出威脅列表，對每個威脅項進行評估處理。

3.1.2 識別資產(Assets Identification)

針對系統的資產識別，可以將系統資產加以分類：

表3.1.2.1、識別資產分類描述

分類	描述
機敏資料	任何資料其機密性、完整性、可用性遭到破壞時，將會遭受重大不利影響者，如系統組態檔
外部實體	驅動軟體的某人或某物，且為軟體本身無法控制者
程序	處理輸入資料的工作或行為，並輸出資料者，如作業系統、韌體
資料流	資料於軟體或系統中移動的方法，如通訊協定
資料儲存庫	軟體中資料暫時或持續的儲存區，如日誌資料

表3.1.2.2、雲端心電圖管理系統識別資產

分類	資產名稱	說明
機敏資料	系統組態檔	系統參數設定檔及系統網路設定
機敏資料	帳號資料	使用者的帳號及病患資料等
機敏資料	量測數據	病患心電圖量測數據
外部實體	使用者	系統操作者

程序	操作介面	心電圖監控儀表板及管理工具
資料流	HTTPS通訊協定	裝置或系統間的通訊協定

3.2 資料流向圖(Data Flow Diagram, DFD)

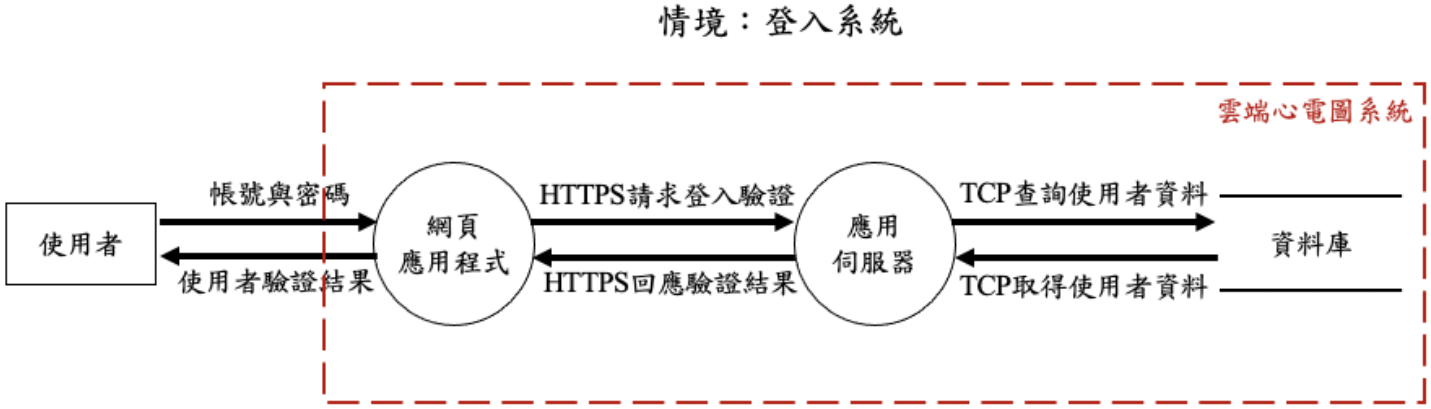
表3.2.1、資料分級之參考

資料安全等級	等級	資安防護特性		
		機密性	完整性	可用性
	高	只有限制性的系統角色才能揭露資料	資料遭到竄改會造成嚴重危害	資料遭到毀壞會造成嚴重危害
	中	系統角色可揭露資料	資料遭到竄改會造成中度危害	資料遭到毀壞會造成中度危害
	低	資料可以公開揭露	資料遭到竄改會造成輕度危害	資料遭到毀壞會造成輕度危害

以從資料的角度來描述一個系統。元素如下：

- Flow( )
- File/Database ( )：表示文件、資料庫
- Function（ ）
- Input/Output（ ）：系統的端點，例如人。
- 信任邊界（ ）：表示可信元素與不可信元素之間的邊界。

雲端心電圖管理系統所具有之資料流向圖如下：



3.2.1、資料流向圖：登入系統

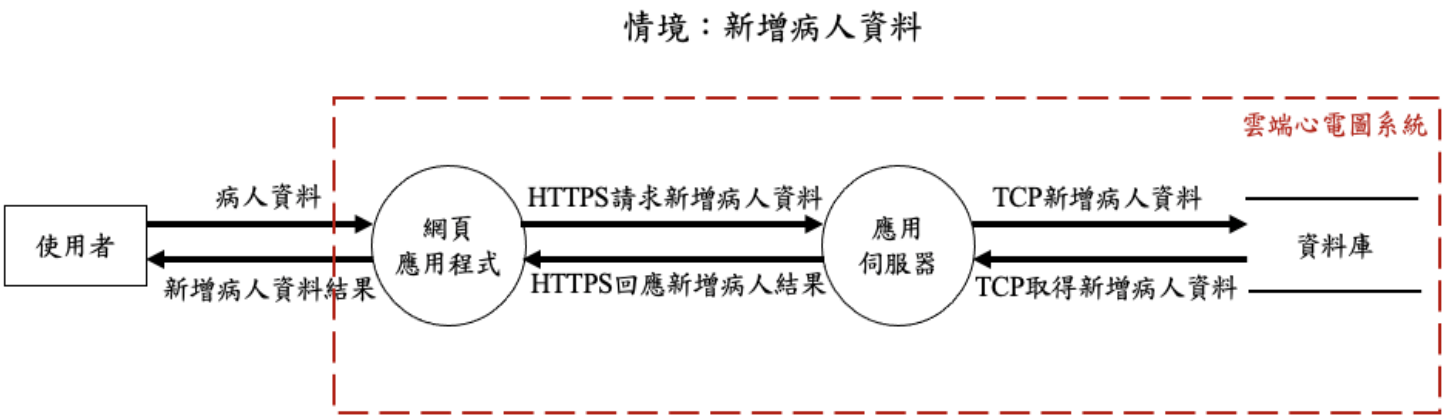


圖3.2.2、資料流向圖：新增病人資料

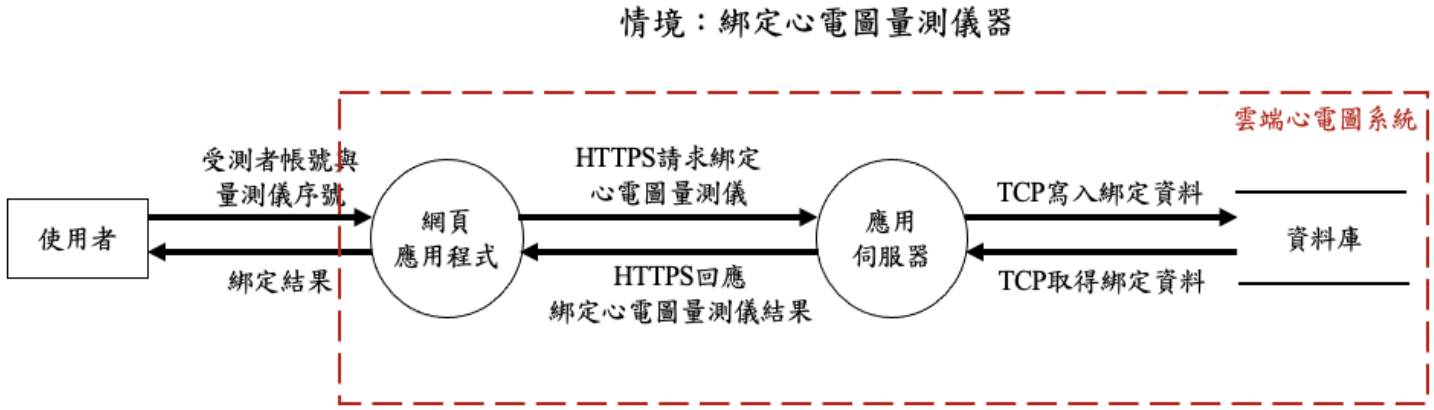


圖3.2.3、資料流向圖：綁定心電圖量測儀器

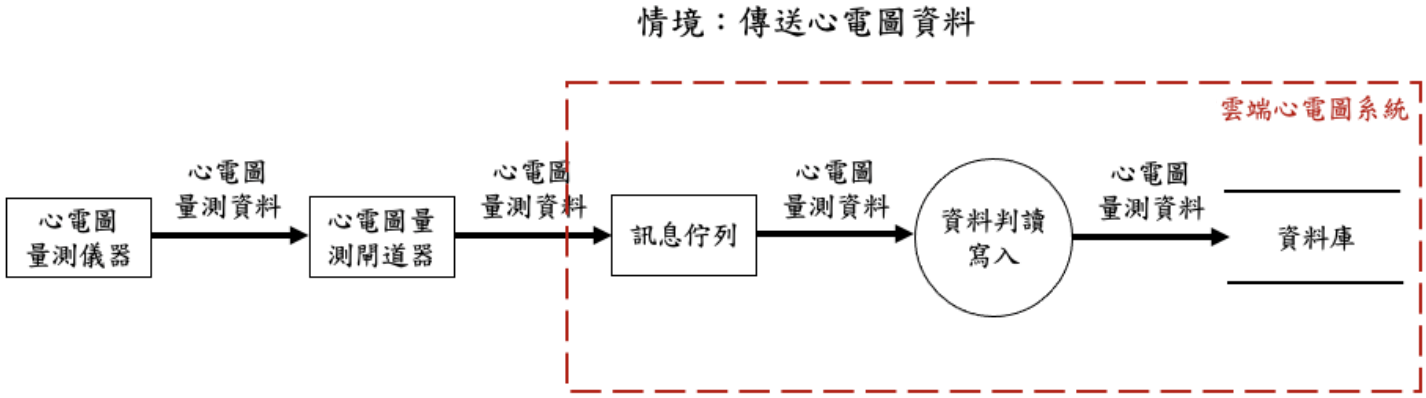


圖3.2.4、資料流向圖：傳送心電圖資料

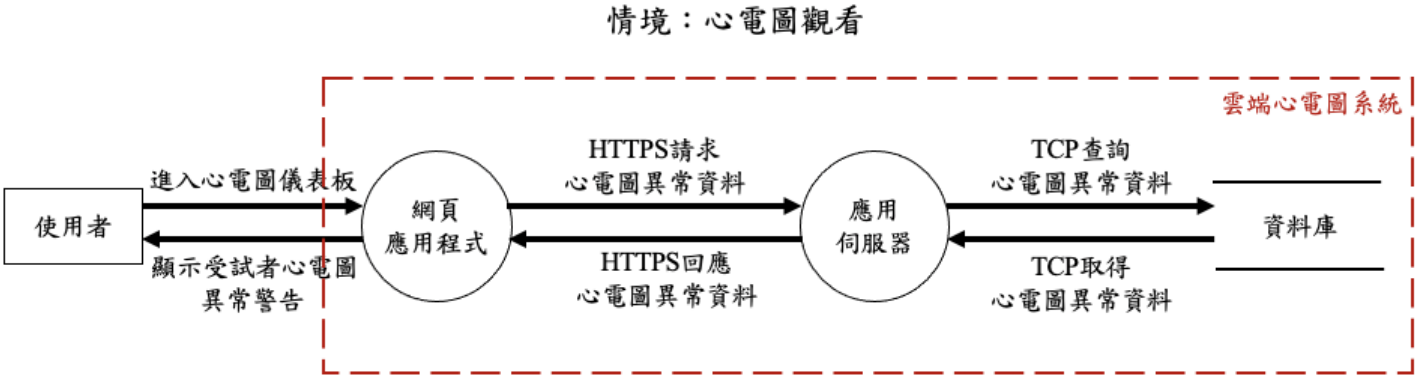


圖3.2.5、資料流向圖：觀看受測者即時心電圖資料

3.3 分析網路安全威脅(Cybersecurity Threat Analysis)

表3.3.1、STRIDE模型之類別說明

類別	描述	資安防護特性
假冒 (Spoofing)	涉及非法存取然後使用其他使用者的驗證資訊，例如使用者名稱和密碼。	身分認證 (Authentication)
竄改 (Tampering)	涉及惡意修改資料。例如在未經授權的狀況下變更資料庫中保存的持續性資料，以及修改在兩部電腦之間透過開放式網路(例如網際網路) 流動的資料。	完整性 (Integrity)
否認性 (Repudiation)	與拒絕執行動作但沒有其他任何一方有辦法另外證明的使用者有關，例如使用者在無法追蹤違禁作業的系統中執行非法作業。不可否認性是指系統對抗否認性威脅的能力。概念近似於購買商品的使用者可能必須在收到商品時簽名。然後，廠商可以使用簽名收據做為使用者已收到包裹的證據。	不可否認性 (Non-repudiation)
資訊洩漏 (Information Disclosure)	涉及將資訊暴露給不應具有其存取權的個人，例如，使用者可以讀取其未被授權可存取的檔案，或入侵者能夠讀取在兩部電腦之間傳輸的資料。	機密性 (Confidentiality)
阻斷服務 (Denial of Service, DoS)	阻斷服務攻擊可阻斷對有效使用者提供的服務，例如，藉由讓網頁伺服器暫時無法存取或無法使用。您必須防止特定類型的DoS威脅，以便提升系統的可取得性和可靠性(availability and reliability)。	可用性 (Availability)
權限提高 (Elevation of Privilege)	未授權的使用者取得授權的存取權，因此有足夠存取權危害或摧毀整個系統。提高權限威脅包含攻擊者已有效地滲透所有系統防禦，並成為受信任系統本身的一部分，這確實是危險的情況。	授權 (Authorization)

表3.3.2、風險降低類別[3]

類別	描述
稽核和記錄	誰在何時做了什麼？稽核和記錄是指應用程式記錄安全性相關事件的方式
驗證	您是誰？驗證是某實體證明另一個實體身分識別的程序 (通常透過使用者名稱和密碼等認證)
授權	您可以做什麼授權是應用程式針對資源和作業提供存取控制的方式
通訊安全性	您在與誰對話？通訊安全性可確保所有通訊是在最安全的情況下進行的
組態管理	應用程式的執行身分為何其所連線到的資料庫為何？應用程式的管理方式為何如何保護這些設定？ 組態管理指的是應用程式處理這些作業問題的方式
密碼編譯	如何保護機密資料(機密性)？如何防止資料或程式庫遭到竄改(完整性)如何為必須是密碼編譯增強式的隨機值提供種子？密碼編譯是指應用程式強制執行機密性與完整性的方式
例外狀況管理	當應用程式中的呼叫失敗時，應用程式會如何處理？ 您要顯示多少資料？您要對使用者傳回容易理解的錯誤資訊嗎？ 您要將重要例外狀況資訊傳回給呼叫者嗎？應用程式會呼叫失敗嗎？
輸入驗證	您如何知道應用程式收到的輸入是有效且安全的？ 輸入驗證指的是應用程式如何先篩選、消除或拒絕輸入再進行其他處理。請考慮透過進入點限制輸入並透過退出點編碼輸出。您是否信任來源的資料，例如來自資料庫和檔案共用？
機敏性資料	應用程式如何處理機敏性資料？ 機敏性資料指的是應用程式如何處理記憶體中、透過網路或持續性存放區中必須受到保護的任何資料
會話管理	應用程式如何處理和保護使用者工作階段？ 工作階段是指使用者與 Web 應用程式之間的一系列相關互動

[3] Microsoft 威脅模型化工具風險降低. Available: https://docs.microsoft.com/zh-tw/azure/security/develop/threat-modeling-tool-mitigations

表3.3.3、網路安全威脅分析表

資產名稱	假冒(S)	竄改(T)	否認行為(R)	資訊洩露(I)	拒絕存取服務(D)	權限提高(E)	威脅列表
作業系統					V	V	D1：透過入侵作業系統關閉相關服務或應用系統 E1：作業系統遭到入侵後，可透過創建帳號並提權。
系統組態檔		V			V		T1：透過組態設定變更，更改系統服務。 D2：透過組態設定開啟相關通訊介面，以揭露資訊。
帳號資料		V			V		T2：透過組態設定變更，更改系統服務。 D3：透過組態設定開啟相關通訊介面，以揭露資訊。
操作介面						V	E2：作業系統遭到入侵後，可透過創建帳號並提權。
HTTPS通訊協定				V			I1：針對未保護的通訊管道揭露資訊
心電圖量測資料	V						S1：未對使用者進行驗證 S2：透過重送攻擊來進行假冒攻擊
日誌資料			V				R1：竄改日誌資料，修改相關存取記錄

基於STRIDE與DFD結果，便可以針對系統組成元素分析其網路安全威脅，以及可能的攻擊樹(Attack Tree)，如下圖3.3.1所示：

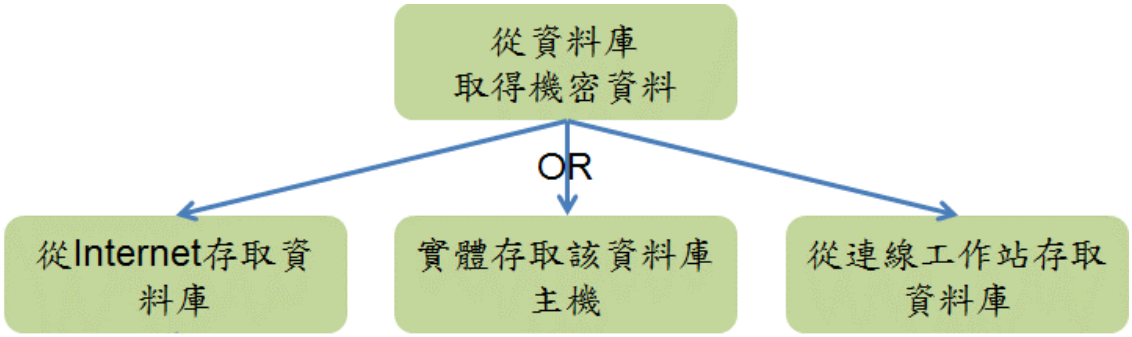


圖3.3.1、攻擊樹狀圖簡單案例圖

3.4 網路安全風險評鑑方法(Cybersecurity Risk Assessment Methodology)

醫療器材的風險評鑑方法，可以參考醫療器材的網路安全風險評鑑框架：

1. 識別威脅來源與弱點
2. 網路安全威脅/風險情境分析
3. 可用性評估
4. 影響性評估
5. 風險評分
6. 風險管理與控制措施

上述步驟1 (識別威脅來源與弱點)以及步驟2 (網路安全風險情境分析)即為第2.2.4節分析網路安全威脅的結果。本章節主要來針對前述網路安全威脅列表的所有威脅進行各別的網路安全風險評鑑。醫療器材之網路安全風險因素主要可分為以下兩種，詳細網路安全因素與風險值由表3.4.1所示：

- 威脅(外部因素)：主要從攻擊者的角度，來探討其針對醫療器材造成網路安全威脅的風險狀況，其評估因子有技能等級、動機、機會與資源3項。
- 弱點(內部因素)：主要從防禦方以及醫療器材本身的安全漏洞，來探討醫療器材之網路安全漏洞可被利用而造成網路安全風險的狀況，其評估因子有發現難易度、可用性與入侵偵測3項。

威脅來源可能來自於使用者、維護廠商、醫院醫工、其他可能碰觸者或網路惡意攻擊者。

表3.4.1、表3.4.2、表3.4.3分別描述了影響醫療器材網路安全的可用性、影響性與發生可能性的相關數值，並經由表3.4.4中的計算公式，將上述所提及的數值合併成代表醫療器材的整體風險值。

表3.4.1、醫療器材的網路安全因素與風險值[4]

可利用性	Threat Agent Factors 威脅因素			Vulnerability Factors 弱點因素		
風險因素與風險值	**T1** Skill level 技能等級	**T2** Motive 動機	**T3** Opportunity & Resources 機會與資源	**V1** Ease of Discovery & Awareness 發現的難易度	**V2** Ease of Exploiting 可用性	**V3** Intrusion Detection 入侵偵測

[4] 行政院衛生福利部關鍵基礎設施資安工作推動專案辦公室. 醫療器材的網路安全因素與風險值.

說明	就已知現狀電腦技能選最高	資料有價值或量大可轉賣獲利/新上市高貴儀器可出名	權限管理、實體環境/系統運作介面之控管	視使用作業系統，若為主流設備(設備市佔高)或作業系統廠商較能支援	若為主流作業系統，網路上可搜尋到較多的入侵工具	是否有安全偵測、有入侵日誌、能自動偵側
1	無技術性技能或具一般電腦能力	低度或無獎勵或無誘因，如無個資為一般性設備	實體環境/系統運作介面有加以控管且有特殊權限	1.設備市佔高或設備之作業系統為大宗，廠商能支援程式修補，2.作業系統客製化攻擊意願較低	非大宗、非主流作業系統或設備市佔低，網路入侵工具較少	有檢附防護機制或人員對入侵能即時偵測
2	具備部分技術性技能或具備網路與程式撰寫能力	可能有獎勵與誘因，如檢查量大設備且有醫療資訊	僅有權限管理但無實際人員/角色管理	使用的作業系統非大宗或較舊作業系統但廠商仍支援程式修補	使用的作業系統非大宗或較舊作業系統，但網路入侵仍有工具	人員對入侵後知後覺
3	具備資安滲透技能	高度獎勵與誘因，如攻擊尖端設備可成名，或取得具價值的醫療資訊	實體環境/系統運作介面有加以控管，但不需任何權限或資源可達成入侵目的	舊作業系統之弱點廠商已不支援程式修補	設備市佔高、設備作業系統為大宗或主流，網路入侵工具較多	人員對入侵不知不覺

表3.4.2、醫療器材網路安全風險的影響等級

影響等級	嚴重程度
說明	病人安全影響的嚴重程度
1	無損害或造成病人不方便之情況
2	間接傷害，指當下未造成病人直接傷害但病人有潛在傷害的風險
3	直接傷害，指當下即造成病人的損傷或傷害，嚴重者可能追成病人死亡

表3.4.3、醫療器材網路安全風險的發生可能性數值

發生可能性數值	可能由插槽/系統運作介面遭受的風險機會
1	設備無插槽另提供外接或 設備有插槽且有使用者管控措施
2	設備有插槽但無使用者管控措施

表3.4.4、醫療器材風險值的計算

風險值	**風險值 ＝可用性風險值 × 影響性風險值 × 發生可能性數值** （風險值最高值為 18，最低值為 1）
	● 可用性風險值 = 6項風險因素值的平均 (1~3) ● 影響性風險值 = 病人安全影響程度風險值 (1~3) ● 發生可能性數值= 可能由插槽/系統運作介面遭受的風險機會 (1~2)
風險等級	● **A級(高風險)**：風險值介於13.0 ~ 18.0 ，**不可接受(Unacceptable)** ● **B級(中風險)**：風險值介於7.0 ~ 12.9，**可能接受的(Potentially Acceptable)** ● **C級(低風險)**：風險值介於1.0 ~ 6.9，**可接受的(Acceptable)**

表3.4.5、醫療器材網路安全風險等級檢核表

醫療器材組成元件	威脅類型	(I) Impact factor 影響程度 (低:1~高:3)	可利用性						(R) 風險值 (低：1~高：3)	(P) 發生可能性 (低：1~高：2)	(E) 風險結果	(R) 風險等級 A:高風險 (不可接受) B:中風險 (可能接受的) C:低風險 (可接受)	風險編號	風險控制措施
			(T) Threat Agent Factors 威脅因素 (低：1~高：3)			(V) Vulnerability Factors 弱點因素 (低：1~高：3)								
元件	威脅	病人危害程等	(T1) 技能等級	(T2) 動機	(T3) 機會與資源	(V1) 發現的難易度	(V2) 可用性	(V3) 入侵偵測	R=avg(T+V) 平均值	由插槽/系統運作介面遭遇的風險機會	I*R*P	A:13~18 B:7.0~12.9 C:1.0~6.9	風險	控制措施
作業系統	D1	3	3	2	1	1	2	2	1.83	1	5.49	低風險(可接受)	Risk-01	SDD-25: 給予使用者操作時所需最低權限
作業系統	E1	3	3	2	1	1	2	2	1.83	1	5.49	低風險(可接受)	Risk-02	SDD-25: 給予使用者操作時所需最低權限
系統組態檔	D2	3	3	2	1	1	2	2	1.83	1	5.49	低風險(可接受)	Risk-03	SDD-24：設定權限管理
系統組態檔	T1	3	3	2	1	1	2	2	1.83	2	10.98	中風險 (可能接受的)	Risk-04	SDD-24：設定權限管理

帳號資料	D3	3	3	1	1	1	2	2	1.67	1	5	低風險(可接受)	Risk-05	SDD-24：設定權限管理
帳號資料	T2	3	3	1	1	1	2	2	1.67	2	10	中風險 (可能接受的)	Risk-06	SDD-22:操作權限集中控管
操作介面	E2	3	3	1	1	1	2	2	1.67	2	10	中風險 (可能接受的)	Risk-07	SDD-27：異常事件紀錄
HTTPS通訊協定	I1	3	3	1	1	1	2	1	1.5	2	9	中風險 (可能接受的)	Risk-08	SDD-03：傳輸時進行機敏性資料加密。
心電圖量測資料	S1	1	3	1	1	1	2	2	1.67	2	3.3	低風險(可接受)	Risk-09	SDD-03：傳輸時進行機敏性資料加密。 SDD-08：設置加密的金鑰管理模組
心電圖量測資料	S2	1	3	1	1	1	2	2	1.67	2	3.3	低風險(可接受)	Risk-10	SDD-12：對於資料輸入進行驗證檢查
日誌資料	R1	1	3	1	1	1	2	1	1.5	2	3	低風險(可接受)	Risk-11	SDD -14：設備身分管理機制

3.5 網路安全檢測方法(Cybersecurity Testing Methodology)

3.5.1 漏洞掃描(Vulnerability Scanning)

漏洞掃描是針對已知的系統漏洞，對該系統進行掃描、攻擊、測試。漏洞掃描可瞭解現有環境中各種網路設備、系統與主機所存在之漏洞狀況，並透過漏洞掃描結果分析報告獲得有效的改善方案。漏洞通常因缺陷 (flaws) 或錯誤配置(misconfigurations)而產生。缺陷是由產品的設計缺陷造成，常見軟體缺陷是緩衝區溢出(buffer overflow)。錯誤配置例如薄弱的錯誤配置存取控制表、開放的埠和不必要的服務，OWASP網站(https://owasp.org/www-community/Vulnerability_Scanning_Tools)列舉漏洞掃描工具可供參考。

雲端心電圖管理系統採業界具公信力之漏洞掃瞄軟體 Nessus ，進系統進行漏洞掃描，並針對可能問題進行修正，發行版本經過 Nessus 十種分類的測試後，掃除了 CRITICAL，HIGH，MEDIUM 等級之漏洞，僅有四項 LOW 等級之測試未通過，此四項經評估後並不影響本系統安全。

以下為測試結果摘要報告

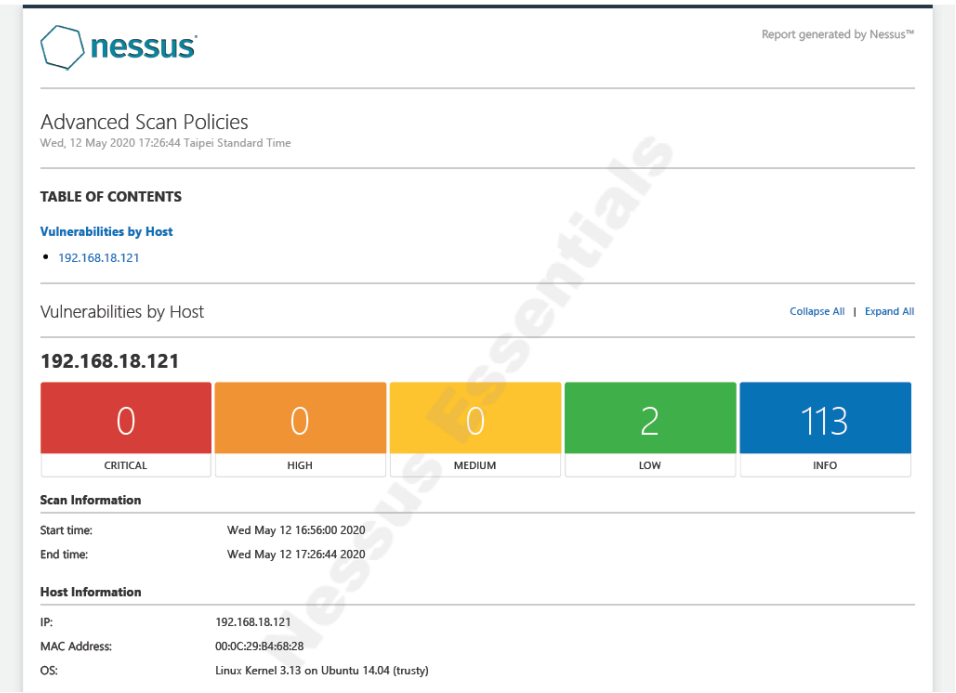


圖3.5.1.1、漏洞掃描測試結果報告 Advanced Scan

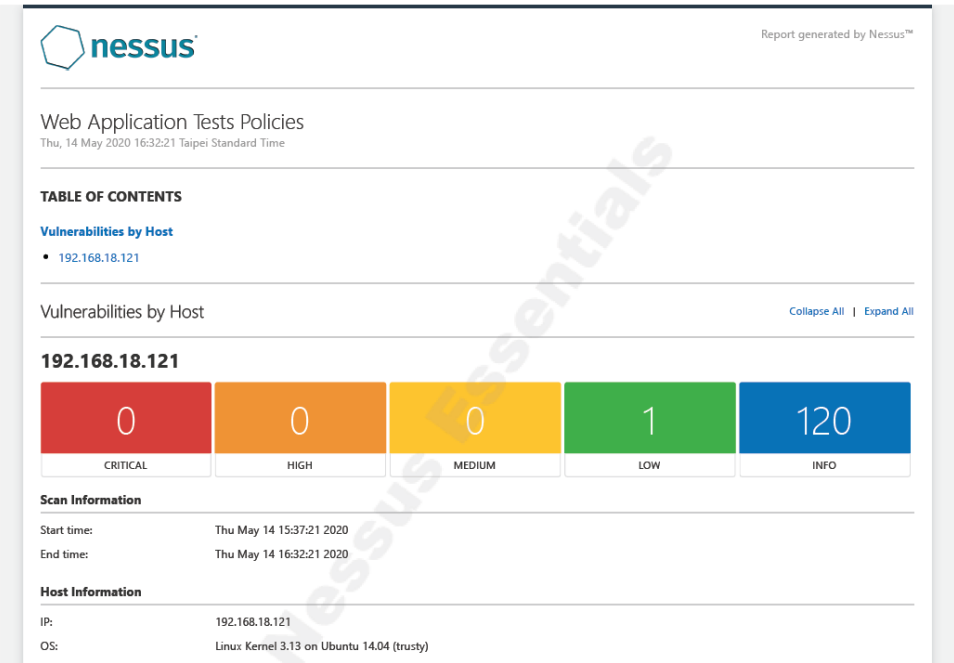


圖3.5.1.8、漏洞掃描測試結果報告 Web Application Tests

3.5.2 滲透測試(Penetration Testing)

滲透測試(Penetration Test)通常是由資安團隊以駭客之思維與行為模式規劃測試內容，利用漏洞掃描軟體或其他的工具，從外部和內部網路進行模擬入侵，收集系統的相關資訊，探查漏洞。

為確保本系統資訊安全，開發團隊選用業界常用之滲透測試工具 Metasploit 進行滲透測試。滲透測試進行流程如下：

1. 確認測試範圍，主要以本系統作業系統及運行於作業系統上之軟體相關測試安裝案例為主
2. 收集測試案例所需之測試資料
3. 進行滲透測試並依據測試失敗項目進行改進

下表為本系統相關案例及其測試結果，表中系統未被成功入侵取得更高權限，表示為通過測試(Pass)。

表3.5.6.1、滲透測試結果報告

項目編號	項目名稱	項目描述	測試結果
PTV-01	Nagios3 history.cgi Host Command Execution	This module abuses a command injection vulnerability in the Nagios3 history.cgi script.	Pass
PTV-02	Nagios3 statuswml.cgi Ping Command Execution	This module abuses a metacharacter injection vulnerability in the Nagios3 statuswml.cgi script. This flaw is triggered when shell metacharacters are present in the parameters to the ping and traceroute commands.	Pass
PTV-03	Nagios XI Network Monitor Graph Explorer Component Command injection	This module exploits a vulnerability found in Nagios XI Network	Pass
PTV-04	Nagios Remote Plugin Executor Arbitrary Command Execution	The Nagios Remote Plugin Executor (NRPE) is installed to allow a central Nagios server to actively poll information from the hosts it monitors. NRPE has a configuration option dont_blame_nrpe which enables command-line	Pass

		arguments to be provided remote plugins. When this option is enabled, even when NRPE makes an effort to sanitize arguments to prevent command execution, it is possible to execute arbitrary commands.	

附錄一：醫療器材網路安全評估—自我檢核表(Cybersecurity Self-Checklist)

使用附件“醫療器材網路安全之業者揭露聲明書”檔案

附錄二：本產品相關醫療器材之網路安全通報 (Related Cybersecurity Alerts)

以ECG為關鍵字在美國國家漏洞資料庫(National Vulnerability Database, NVD https://www.nist.gov/)搜尋，相關漏洞如下表。

表一、NCD資料庫(關鍵字:ECG，僅列出部分資訊)

漏洞編號	說明
CVE-2020-15485	An issue was discovered on Nescomed Multipara Monitor M1000 devices. The onboard Flash memory stores data in cleartext, without integrity protection against tampering.
CVE-2020-15486	An issue was discovered on Dr Trust ECG Pen 2.00.08 devices. Because the Bluetooth LE support is implemented without a requirement for pairing or security, any attacker can access the GATT server of the device and can sniff the data being broadcasted while a measurement is being done. Also, saved data can also be extracted over a Bluetooth connection. In addition, an attacker can launch a man-in-the-middle attack against data integrity.

附錄三：本產品相關之通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE)

通用漏洞揭露(Common Vulnerabilities and Exposures, CVE)是資訊安全相關的資料庫，該資料庫收集各種資安漏洞並給予編號以便於查閱，讓資安管理人員有辦法針對部分CVE所條列的系統弱點逐項檢測。此資料庫現由美國非營利組織 MITRE所屬的National Cybersecurity FFRDC所營運維護。將所獲得資訊羅列。

表一、CVE 資料庫(關鍵字: Django 2.2，僅列出部分資訊)

漏洞編號	說明
CVE-2021-33571	In Django 2.2 before 2.2.24, 3.x before 3.1.12, and 3.2 before 3.2.4, URLValidator, validate_ipv4_address, and validate_ipv46_address do not prohibit leading zero characters in octal literals. This may allow a bypass of access control that is based on IP addresses. (validate_ipv4_address and validate_ipv46_address are unaffected with Python 3.9.5+..) .
CVE-2021-33203	Django before 2.2.24, 3.x before 3.1.12, and 3.2.x before 3.2.4 has a potential directory traversal via django.contrib.admindocs. Staff members could use the TemplateDetailView view to check the existence of arbitrary files. Additionally, if (and only if) the default admindocs templates have been customized by application developers to also show file contents, then not only the existence but also the file contents would have been exposed. In other words, there is directory traversal outside of the template root directories.
CVE-2021-32052	In Django 2.2 before 2.2.22, 3.1 before 3.1.10, and 3.2 before 3.2.2 (with Python 3.9.5+), URLValidator does not prohibit newlines and tabs (unless the URLField form field is used). If an application uses values with newlines in an HTTP response, header injection can occur. Django itself is unaffected because HttpResponse prohibits newlines in HTTP headers.

表二、CVE 資料庫(關鍵字: Postgres 9.6)

漏洞編號	說明
CVE-2021-32027	A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25696	A flaw was found in the psql interactive terminal of PostgreSQL in versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If an interactive psql session uses \gset when querying a

	compromised server, the attacker can execute arbitrary code as the operating system account running psql. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25695	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

表四、CVE 資料庫(關鍵字: Nginx 1.1)

漏洞編號	說明
CVE-2017-20005	NGINX before 1.13.6 has a buffer overflow for years that exceed four digits, as demonstrated by a file with a modification date in 1969 that causes an integer overflow (or a false modification date far in the future), when encountered by the autoindex module.
CVE-2019-20372	NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.
CVE-2018-16845	nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.