資本門採購案件執行流程目錄

<table>
<tr><td>採購方式</td><td colspan="5">公開招標第 5 案</td></tr>
<tr><td>案件名稱</td><td colspan="5">防火牆日誌紀錄器（採購案號：1130203887）</td></tr>
<tr><td>執行期間</td><td colspan="5">113.10.09～113.12.30</td></tr>
<tr><td>採購金額</td><td>238 萬 9,800 元</td><td colspan="2">機關補助金額</td><td>238 萬 9,800 元</td><td>■適用政府採購法第 4 條
□適用校內辦法</td></tr>
<tr><td>預算金額</td><td colspan="5">238 萬 9,800 元</td></tr>
<tr><td>核定底價</td><td colspan="5">198 萬元</td></tr>
<tr><td rowspan="2">決標總價</td><td rowspan="2">190 萬元</td><td rowspan="2">經費來源</td><td>113 年度獎勵補助經費</td><td colspan="2">190 萬元</td></tr>
<tr><td>學校自籌經費（或其他來源）</td><td colspan="2">--</td></tr>
</table>

檔　　號：113/　　收發文號：
保存年限：　　收發日期：
電子簽核　結案日期：113年10月09日　　創稿文號：1132103340
1132103340

簽　於　資訊處　日期：中華民國113年10月01日
附　　件：（1件）1132103340_1_113年獎補助資安資本門清單_11309.pdf （附件1資安設備資本門清單）

主旨：依全校資訊需求，擬購置供全校師生教學研究使用的資訊安全設備，呈請 鈞長核示預算來源。

說明：

一、因應日益增多之校園資安事件，為降低資安風險，提供安全的教學研究資訊環境，資訊處擬購置相關資訊安全資本門設備，未議價前共約5,350,000元。設備清冊與使用成效說明詳列如附件一。

二、資訊處本年度未編列相關預算，懇請 鈞長指示該預算來源。

三、如蒙 鈞長同意，擬儘速依照採購相關作業準則辦理。

創稿文號：1132103340

公文簽核流程表

項次	簽核名單	代理/加簽	簽核單位	簽收時間	核稿時間	狀態
1	萬序恬副資訊長		資訊處		113-10-01 09:12	創文
2	葉雨婷資訊長		資訊處	113-10-01 15:00	113-10-01 15:26	串簽
一、經外部資安顧問檢視本校資安防護(管發採購之資安顧問服務-奧義)，建議本校優先就校務及非校務服務之網路架構進行區隔，管控非必要之VPN遠端連線，並增加網路流量管制及儲存容量。 二、擬依本校資安防護之重要性與緊急度排列優先順序如附件，懇請 鈞長同意。						
3	秘書處單位		秘書處	113-10-01 22:39	113-10-02 17:03	串簽
4	財務處單位		財務處	113-10-04 09:18	113-10-04 09:19	串簽
5	林靜怡組長	[財務處加簽]	會計服務組	113-10-04 17:43	113-10-04 17:54	串簽
本簽所請113學年度新增計畫未編列經費來源，陳請核示；如蒙核可，敬請依此簽儘速通知財務處主辦林靜怡小姐協助辦理。						

6	許淑群財務長	[財務處加簽]	財務處	113-10-04 19:34	113-10-04 19:36	串簽
擬、本簽請詳財務處林組長說明，陳請核示。						
7	秘書處單位	[秘書處加簽]	秘書處	113-10-07 14:00	113-10-07 14:58	串簽
8	蔡宛真主任秘書	[秘書處加簽]	秘書處	113-10-07 22:34	113-10-08 08:07	串簽
9	賴婷吟組長	[蔡宛真加簽]	校務企劃組	113-10-08 12:06	113-10-08 12:16	串簽
一、本簽所請符合獎補助款支用規定，擬建議由113年度獎補助款預算支應；本案如蒙核可，敬請單位確實掌握請採購時程。 二、陳請鈞長核示。						
10	蔡宛真主任秘書	[蔡宛真加簽]	秘書處	113-10-08 13:46	113-10-08 13:55	串簽
為降低全校資安風險，擬請鈞長同意單位所請，購置附件所列五項設備，餘擬如婷吟組長所擬，陳請鈞長核示。						
11	朱娟秀副校長	[秘書處加簽]	副校長室	113-10-08 13:56	113-10-08 14:00	串簽
擬如主秘擬						
12	吳麥斯校長	[秘書處加簽]	校長室	113-10-09 10:44	113-10-09 10:44	決行
如擬						
13	萬序恬副資訊長		資訊處	113-10-09 13:08		撤回

泰瑩科技股份有限公司

TEL: 886-2-2578-1133 FAX: 886-2-2578-0334
105 台北市松山區南京東路四段130號4樓

報價單

公司：	臺北醫學大學	報價單編號：	TW-241018-1Q
地址：	110 臺北市信義區吳興街250號	交易條件：	月結30天
姓名：	陳韋伸	報價人：	陳妤嘉Yoga Chen
電話：		連絡電話：	0908-590-611
傳真：		日期：	2024/10/24
E-Mail：	wilson@tmu.edu.tw	報價有效期限：	2024/11/23
稅別碼：		案名：	防火牆日誌紀錄器
統一編號:			

報價明細

項次	品項	規格	單價	數量	總價
1	防火牆日誌紀錄器	FAZ-810G Centralized log & analysis appliance - 4x GE RJ45, 2x GE SFP, 16TB self-encrypting storage, up to 200 GB/Day of Logs 原廠保固一年	$1,138,000	2	$2,276,000
		上述報價含首次安裝設定建置費用			
				未稅金額：	$2,276,000
				稅額：	$113,800
				總計金額：	$2,389,800

備註：

1.以上報價含5%營業稅。
2.付款方式：月結30天。
3.保固方式：提供原廠一年保固及泰瑩一年5x8人力到場維護服務(不含備品服務)。
4.交貨日期：下單後約6~8週。
5.交貨地點：依雙方議定之地點交貨。
6.依客戶需求訂購或預訂的貨品，一經本公司進行採購作業，即不得取消或變更訂單。
7.本報價單一經客戶簽回，即視同正式訂單並表示接受以上條款。

泰瑩科技股份有限公司 業務部 報價專用章 TEL:2578-1133 台北市南京東路4段130號4樓

採購單位簽章：

本單若經 貴單位確認傳回,則視同採購單。或請 貴公司另下採購單至本公司,以確認採購。

臺北醫學大學
請採購驗收紀錄

請購紀錄

採購案號：	113020388700			作業狀態：	請款結案
學年度：	113	請購日期：	113/10/28	立案日期：	113/11/12
請購單位：	資訊處	請購人：	陳暐傑	預估金額：NT$	2,389,800
採購名稱：	防火牆日誌紀錄器				
使用/保管人：	陳韋伸	到貨地點：	醫綜前棟RF1		
採購分類：	一般採購(>10萬元)	採購品項分類別：	電腦與資訊 電腦硬體設備		
請購說明：					

預算來源

主預算來源：	教育部獎勵私立大學校院校務發展計畫	預算編號：	113-3600-001-212	預算會科：	134101
		預算主持人：		申請預算：	**1,900,000**
次預算：	無次預算				
次預算來源：					

採購經辦紀錄

議比價金額(含稅)：	**1,900,000**
成交廠商：	泰瑩科技股份有限公司
備註：	本案經政府電子採購網第一次公告後共計三家廠商投標，經資、規格標審標結果三家廠商皆符合招標文件規定，提本會進行比減價。 ;由泰瑩科技股份有限公司以新台幣壹佰玖拾萬元整得標。

議價會議

本案經 113 學年度
採購委員會會議
第 9 次會議記錄通過

標號： **TMU113-103**
合約： **TMU113-035W**

請購明細

序	品 名	規 格	採購數量	單位	採購單價	採購金額
1	防火牆日誌紀錄器	faz-810G centralized log & analysis appliance -4x GE RJ45, 2x GE SFP, 16 TB self-encrypting storage, up to 200 GB/Day of Logs	2	台	950,000	1,900,000
					總計NT$	1,900,000

表單附件

項次	文件類別	文件說明	文件格式	檔案名稱
1	採購重要規格		電子檔	2024採購規格書-防火牆日誌紀錄器.docx
2	驗收文件	出貨單	電子檔	FAZ-出貨單.pdf
3	驗收文件	功能驗收單	電子檔	防火牆日誌紀錄器-功能驗收單.pdf
4	驗收文件	測試報告	電子檔	防火牆日誌記錄器_測試報告.pdf
5	會議紀錄	含核定簽呈	電子檔	113採購委員會第09次會議-會議記錄含核定簽呈113.11.2
6	估價單	估價單	電子檔	20241024FAZ.pdf

臺北醫學大學
請採購驗收紀錄

表單附件

項次	文件類別	文件說明	文件格式	檔案名稱
7	底價分析表(簽核後)	底價分析表	電子檔	2024防火牆日誌紀錄器-底價分析表.pdf

簽核紀錄

單位	資訊處	資訊支援組	資訊處	事務組	資訊處	資訊支援組
職稱	資訊長	組長	資訊長	組長	資訊長	組長
姓名	葉雨婷	游千瑩	葉雨婷	李彥蓉	葉雨婷	游千瑩
日期	113/10/29 16:05	113/10/30 11:01	113/10/31 22:14	113/11/06 16:00	113/11/09 09:26	113/11/09 18:09
結果	核准	核准	核准	不核准	核准	核准
意見				請修正採購規格		
請購申請簽核/會簽						

單位	資訊處	事務組	事務組	事務組	依採購相關會議辦理	保管組
職稱	資訊長	組長	組員	組長		組長
姓名	葉雨婷	李彥蓉	李清萬	李彥蓉		趙容旋
日期	113/11/09 18:11	113/11/12 11:34	113/12/02 09:45	113/12/02 10:46		113/12/03 18:17
結果	核准	核准	申請	核准		核准
意見		分案	申請人		財務處	
請購申請簽核/會簽						
採購核決						
財務監辦						

單位	總務處	副校長室	校長室			
職稱	總務長	副校長	校長			
姓名	張正恆	朱娟秀	吳麥斯			
日期	113/12/04 09:21	113/12/04 16:33	113/12/05 07:22			
結果	核准	核准	核准			
意見						
採購核決						

驗收歷程

NO.	驗收日期	驗收類型	驗收人	單位	驗收結果	備註	下位驗收人
1	113/12/05	新增驗收單	李清萬	事務組	符合	送出驗收	陳暐傑
2	113/12/13	到貨點收	陳暐傑	網路通訊組	符合		陳韋伸
3	113/12/13	功能驗收	陳韋伸	網路通訊組	符合	符合採購規格，功能驗收合格。	葉雨婷
4	113/12/13	主管審核	葉雨婷	資訊處	符合		保管組會驗
5	113/12/18	會驗	簡郁嘉	保管組	符合	驗收符合	
6	113/12/18	會驗	李清萬	事務組	符合		
7	113/12/18	會驗	張正恆	總務處	符合	總務長會簽	
8	113/12/18	會驗	羅意美	財務規劃組	符合	財務處會驗	
9	113/12/18	會驗	趙容旋	保管組	符合	保管組組長會簽	

臺北醫學大學
請採購驗收紀錄

驗收歷程

NO.	驗收日期	驗收類型	驗收人	單位	驗收結果	備註	下位驗收人
10	113/12/19	待請款	簡郁嘉	保管組	符合	驗收完成轉待請款	AF_END

結案請款資料

請款日：	113/12/23	實際採購金額：	1,900,000	最後總結案：	Y

憑證資訊

序	廠商名稱	憑據類別	憑據日期	憑據號碼	憑據金額	說明
1	泰瑩科技股份有限公司	發票	113/12/23	HF61953097	1,900,000	

財編資料 （本請購驗收紀錄得兼具財產增加單功能）

■ 財產大類:機械儀器及設備
財產編號:2-1-35-99 ～ 2-1-35-100(單價:950,000元，數量:2台，總計:1,900,000元)

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

臺北醫學大學採購規格書

採購名稱：防火牆日誌紀錄器

項次	採購規格 / 勞務工作規範 ※請參酌『資格及規格訂定注意事項』，並依採購個案實際需求訂定	數量	單位
1	甲、 功能需求內容說明 1. 獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。 2. 系統日誌接收效能可達 6,000 logs/sec (含)以上。 3. 系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。 4. 系統儲存容量可達 16 TB (含)以上，支援磁碟陣列 RAID 0/1,1s/5,5s/10 規範。 5. 具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。 6. 具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。 7. 具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。 8. 具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。 9. 具備事件監看與告警功能，可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。 10. 具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。 11. 具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。 12. 具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方	2	台

臺北醫學大學採購規格書

便中央監看、顯示資安威脅、深入追蹤與採取行動。

13. 具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服器或 Common Event Format (CEF) 伺服器，以利與既有日誌系統整合。
14. 具備管理區域 (Administrative Domain) 分割功能，並可針對不同管理人員賦予不同的管理權限。
15. 具備 REST API，以利與既有資安環境整合。採購項目說明

乙、 維護標的資訊一覽表

1. 維護等級5x8_設備清單

項次	設備型號	數量	維護期間
1	防火牆日誌紀錄器	1台	驗收日次日起算一年

2. 上述硬體設備得標廠商應提供自驗收次日起 1 年(5*8)人力到場維護保固服務及原廠經銷授權證明。
3. 得標廠商須提供原設備參數轉移與配合網路架構優化相關技術服務。
4. 為確保本案日後維護之保障，廠商須提供網路設備之原廠授權經銷商證明。

1、 履約期限：(請務必設定於預算經費核銷期限前，如需較長測試或試用期間，應視狀況將交貨期提前)

(1) **財物**：

■廠商應於 113 年 12 月 13 日以前，□其他：＿＿＿＿＿＿，將採購標的送達請購單位指定地點，安裝測試完畢，且測試結果符合契約規定；

□廠商應於＿年＿月＿日以前將採購標的送達請購單位指定地點，另於貨到後＿＿年＿＿月＿＿日前，□經請購單位通知＿＿日內完成安裝測試，且測試結果符合契約規定。

(2) **勞務**：廠商應於□＿＿年＿＿月＿＿日以前，□其他：＿＿，完成履行採購標的之供應合約。

※以上計算方式：□以日曆天計，星期例假日、國定假日或其他休息日計入。以□工作天計。

2、保固期限：■提供保固，自驗收合格之日起，保固＿一＿年，□其他：＿＿＿＿＿＿，□不須提供保固。

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

臺北醫學大學採購規格書

3、 **後續擴充：**■無。□後續擴充(請敘明擴充期間、金額或數量，採購金額須含後續擴充項目所需金額)：		
請購單位：資訊處	**請購人：陳暐傑**	**聯絡人/電話：2626**

公開招標公告

公告日：113/11/13　　列印時間：113/11/12 13:53

機關資料	機關代碼	03724606
	機關名稱	臺北醫學大學
	單位名稱	臺北醫學大學
	機關地址	110臺北市信義區吳興街250號
	聯絡人	李清萬
	聯絡電話	(02)27361661#2912
	傳真號碼	(02)27363327
	電子郵件信箱	chingwan@tmu.edu.tw

採購資料	標案案號	TMU113-103
	標案名稱	防火牆日誌紀錄器
	標的分類	財物類 452-計算機及其零件與配件
	財物採購性質	買受,定製
	採購金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
	採購金額級距	公告金額以上未達查核金額
	法人團體辦理適用採購法案件之依據法條	採購法第4條
	辦理方式	補助
	依據法條	採購法第18條、第19條
	是否適用條約或協定之採購	是否適用WTO政府採購協定(GPA)：否 是否適用臺紐經濟合作協定(ANZTEC)：否 是否適用臺星經濟夥伴協定(ASTEP)：否
	本採購是否屬「具敏感性或國安(含資安)疑慮之業務範疇」採購	否
	本採購是否屬「涉及國家安全」採購	否
	預算金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
	預算金額是否公開	否 預算金額不公開理由：機關認為不宜公開
	預計金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
	預計金額是否公開	否
	後續擴充	否
	是否受機關補助	是 補助機關　3.9教育部 補助金額　2,389,800元 貳佰參拾捌萬玖仟捌佰元
	本案是否曾以不同案號辦理招標公告	否
	是否提供英文招標文件	未提供
	是否為政策及業務宣導業務	否

招標資料	招標方式	公開招標
	決標方式	最低標
	是否依政府採購法施行細則第64條之2辦理	否
	新增公告傳輸次數	01
	招標狀態	第一次公開招標
	機關自定公告日	113/11/13
	是否複數決標	否
	是否訂有底價	是
	是否屬特殊採購	否
	是否已辦理公開閱覽	否
	是否屬統包	否
	是否屬共同供應契約採購	否
	是否屬二以上機關之聯合採購(不適用共同供應契約規定)	否
	是否應依公共工程專業技師簽證規則實施技師簽證	否
	是否採行協商措施	否
	是否適用採購法第104條或105條或招標期限標準第10條或第4條之1	否
	是否依據採購法第106條第1項第1款辦理	否

領投開標	是否提供電子領標	是 機關文件費(機關實收) 200元 系統使用費 20元 文件代收費 10元 總計 230元 機關文件費指定收款機關單位： 臺北醫學大學 機關文件費指定收款帳戶： 財團法人臺北醫學大學 是否提供現場領標： 否
	是否提供電子投標	否
	截止投標	113/11/25 17:00
	開標時間	113/11/25 17:00
	開標地點	110臺北市信義區吳興街250號
	是否須繳納押標金	是，尚未提供廠商線上繳納押標金 理由：押標金收款帳戶暫不允許非臨櫃存入 押標金額度：119000
	投標文字	正體中文
	收受投標文件地點	110臺北市信義區吳興街250號

其他	是否依據採購法第99條	否
	履約地點	臺北市(非原住民地區)
	履約期限	詳投標須知及契約書相關規定
	是否刊登公報	是
	是否依據採購法第11條之1，成立採購工作及審查小組	否
	本案採購契約是否採用主管機關訂定之範本	是
	本案採購契約是否採用主管機關訂定之最新版範本	財物類財物採購契約範本最新版之時間為「112.11.23」 是
	契約是否訂有依物價指數調整價金規定	否，招標文件未訂物價指數調整條款 無預算
	廠商資格摘要	1. 廠商登記或設立之證明 投標廠商之基本資格須符合以下任一資格： 1. 具公司登記 2. 具商業登記 2. 廠商納稅之證明，如營業稅或所得稅 3. 除上述外之其他資格 廠商資格登記或設立之證明、公司登記證明文件、商業登記證明文件及最近一期之納稅證明。(廠商須提出資格文件影本；機關得通知廠商提出正本供查驗)
	是否訂有與履約能力有關之基本資格	是 廠商應附具之基本資格證明文件或物品： 【須於招標文件載明者為限】 資格項目 / 附加說明 廠商具有製造、供應或承做能力之證明 / 如曾完成與招標標的類似之製造、供應或承做之文件、招標文件規定之樣品、現有或得標後之可取得履約所需設備、技術、財力、人力或場所之說明或品質管制能力文件等 廠商信用之證明 / 如票據交換機構或受理查詢之金融機構於截止投標日之前半年內所出具之非拒絕往來戶及最近三年內無退票紀錄證明、會計師簽證之財務報表或金融機構或徵信機構出具之信用證明等
	附加說明	1.本案採電子領標方式，請至政府電子採購網電子領標，開標方式採二段式： (1)第一階段開資格標進行資、規格審查，開標時投標廠商得免派員參與。審查後如有需投標廠商另行補充或釋疑部份，投標廠商應於接獲本校通知之日起三個日曆天(含例假日)內提供，如逾期或補充後經本校審查仍不合格，則視同資格不符，不得參加後續第二階段比議價。 (2)第二階段開價格標進行比議價，已通過第一階段資、規格審查之投標廠商，須由負責人或授權代表人攜帶公司大小章、授權書及押標金收據參與第二階段比議價，未派員到場者視同放棄比減價格。比議價日期及地點將視投標及審標狀況另行通知。 2.餘詳投標須知，以上資料若有任何更動，以最新公告日為主。
	是否刊登英文公告	否
	疑義、異議、申訴及檢舉受理單位	疑義、異議受理單位 臺北醫學大學 申訴受理單位 行政院公共工程委員會採購申訴審議委員會-(地址：110臺北市信義區松仁路3號9樓、電話：02-87897530、傳真：02-87897514) 檢舉受理單位 部會署-教育部採購稽核小組-(地址：100臺北市中正區中山南路5號、電話：02-77365529 、傳真：02-23583005) 法務部調查局-(地址：231新北市新店區中華路74號;新店郵政60000號信箱、電話：02-29177777、傳真：02-29188888) 法務部廉政署-(地址：100臺北市中正區博愛路166號;100006國史館郵局第153號信箱、電話：0800286586、傳真：02-23811234)

		中央採購稽核小組-(地址：110臺北市信義區松仁路3號9樓、電話：02-87897548、傳真：02-87897554)
	新增時間	113/11/12 13:53

註：
- 招標公告是否已傳輸成功，可至功能選單「政府採購 > 招標管理 > 查詢招標公告」查詢；招標文件是否已傳輸成功，可至功能選單「政府採購 > 招標管理 > 檢驗上傳標案」確認。

(工程會112.06.30版)

以下各項招標規定內容，由機關填寫，投標廠商不得填寫或塗改。
各項內含選項者，由機關擇符合本採購案者勾填。

一、本採購適用政府採購法(以下簡稱採購法)及其主管機關所訂定之規定，並依本校採購作業辦法及採購作業程序之規範。

二、本標案名稱：防火牆日誌紀錄器。

三、採購標的為：
□(1)工程。
☑ (2)財物；其性質為：☑購買；□租賃；□定製；□兼具兩種以上性質者(請勾選)。
□ (3)勞務。

四、本採購屬：
□(1)公告金額十分之一以下之採購。
□(2)逾公告金額十分之一未達公告金額之採購。
☑(3)公告金額以上未達查核金額之採購。
□(4)查核金額以上未達巨額之採購。
□(5)巨額採購。
□已依「機關提報巨額採購使用情形及效益分析作業規定」第2點第1項，簽准預期使用情形及效益目標。

五、本採購：
□(1)為共同供應契約。
☑(2)非共同供應契約。

六、本採購預算金額(不公告者免填，；但依「投標廠商資格與特殊或巨額採購認定標準」第5條第3項規定辦理者，或屬公告金額以上採購之公開招標、選擇性招標及限制性招標之公開評選，除轉售或供製造加工後轉售之採購、預算金額涉及商業機密或機關認為不宜公開外，應公開預算金額)：

七、本採購預計金額(不公告者免填)：

八、上級機關名稱：教育部。

九、依採購法第4條接受補助辦理採購者，補助機關名稱及地址(非屬此等採購者免填)：教育部，臺北市中正區中山南路五號，電話代表號：(02)7736-6666。國家科學及技術委員會，臺北市大安區和平東路二段106號，電話代表號：(02) 2737-7992。衛生福利部，臺北市南港區忠孝東路六段488號，電話代表號：(02)8590-6666。

十、依採購法第5條由法人或團體代辦採購者，委託機關名稱及地址(非屬此等採購者免填)：

十一、依採購法第40條代辦採購者，洽辦機關名稱及地址(非屬此等採購者免填)：

十二、依採購法第75條，受理廠商異議之機關名稱、地址及電話：同招標機關(不同者請書明機關名稱、地址及電話)。

十三、依採購法第76條及第85條之1，受理廠商申訴(未達公告金額之採購，除屬採購法第31條規定不予發還或追繳押標金之爭議者外，不適用申訴制度)或履約爭議調解(無金額限制)之採購申訴審議委員會名稱、地址及電話：廠商與機關間之招標、審標、決標、訂約、履約及驗收之爭議，得依政府採購法及相關規定向機關提出異議或向行政院公共工程委員會採購申訴審議委員會(地址：110臺北市信義區松仁路3號9樓、電話：02-87897530、傳真：02-87897514)提出申訴或履約爭議調解。

十四、本採購為：
☑(1)未分批辦理。
□(2)依分批辦理公告金額以上之採購，業經上級機關核准(文號：　　)，依總金額核計採購金額，分別按公告金額或查核金額以上之規定辦理。

十五、招標方式為：
☑(1)公開招標
□(1-1)本案為複數決標並採分項決標，廠商各項投標文件無需分項裝封，無需於大外標封標示投標項次，有3家以上廠商投標，且符合政府採購法施行細則第55條規定時，即得開標。
□(2)選擇性招標：符合採購法第20條□第1款；□第2款；□第3款；□第4款；□第5款(請勾選款次)
□(2-1)為特定個案辦理，於廠商資格審查後，邀請所有符合資格廠商投標。
□(2-2)為建立合格廠商名單；後續邀標方式為□個別邀請所有符合資格之廠商投標；□公告邀請所有符合資格之廠商投標；□依審標順序，每次邀請___家符合資格之廠商投標；□以抽籤方式擇定邀請符合資格之廠商投標。
□(3)限制性招標：本案業經需求、使用或承辦採購單位敘明符合採購法第22條第1項第___款之情形，並簽報機關首長或其授權人員核准採限制性招標。
□(3-1)公開評選、公開勘選優勝廠商：
□(3-1-1)依採購法第22條第1項第9款辦理；□委託專業服務；□委託技術服務；□委託資訊服務；□委託社會福利服務。
□(3-1-2)依採購法第22條第1項第10款辦理。
□(3-1-3)依採購法第22條第1項第11款辦理。
□(3-2)比價；□經前次公告招標結果，無廠商投標或無合格標，且符合採購法施行細則第22條第1項規定無廠商異議或申訴在處理中者，依採購法第22條第1項第1款規定，不另公告招標，並依採購法施行細則第23條之1第1項規定，邀請過去表現優良之2家以上廠商以比價方式辦理；□符合採購法第22條第1項第___款(請列明款次，第16款之情形須併填主管機關核准文號)；□符合採購法第104條第1項但書第___款(請列明款次及相關機關核准文號)；□符合採購法第105條第1項第___款(請列明款次及相

關機關核准文號)；□符合中央機關未達公告金額採購招標辦法第___條第___項第___款規定；□符合地方政府依採購法第23條所定未達公告金額採購招標辦法第___條第___項第___款規定。
□(3-3)議價；□符合採購法第22條第1項第___款(請列明款次，其未得以比價方式辦理之原因：_____；第16款之情形須併填主管機關核准文號)；□符合採購法第104條第1項第___款(請列明款次及相關機關核准文號，非填第4款者，其未得以比價方式辦理之原因：_____)；□符合採購法第105條第1項第___款(請列明款次及相關機關核准文號，填第1款或第2款者，其未得以比價方式辦理之原因：_____)；□符合中央機關未達公告金額採購招標辦法第___條第___項第___款規定(其未得以比價方式辦理之原因：_____)；□符合地方政府依採購法第23條所定未達公告金額採購招標辦法第___條第___項第___款規定。
□(3-4)依採購法第22條第1項第___款辦理(請列明款次)，並以公告程序徵求受邀廠商，作為邀請比、議價之用。
□(4)依採購法第49條規定公開取得書面報價或企劃書。(限未達公告金額之採購案始得採行)。
□(4-1)本案業經機關首長或其授權人員核准，本次公告未能取得3家以上廠商之書面報價或企劃書時，將改採限制性招標方式辦理。

十六、本採購：
□(1)適用我國締結之條約或協定；其名稱為：
□世界貿易組織政府採購協定(GPA)。
1.門檻金額：(由機關於招標時擇一勾選；未勾選者，為選項A)
□選項A：依GPA我國承諾開放清單所載門檻金額開放，惟簽署國之門檻金額較我國高者，對該簽署國適用該較高之門檻金額。
□選項B：依GPA我國承諾開放清單所載門檻金額開放。
2.服務及工程服務：(由機關於招標時擇一勾選；未勾選者，為選項A)
□選項A：依GPA我國承諾開放清單之服務及工程服務開放，惟僅開放予對該等服務亦相對開放之簽署國。
□選項B：依GPA我國承諾開放清單之服務及工程服務開放。
□臺紐經濟合作協定。
□臺星經濟夥伴協定。
□其他(請敘明)：
非條約或協定國家之廠商：
□不可參與投標。
□下列外國廠商可以參與投標：
1.國家或地區名稱：_____(未列明者即不允許)
2.是否允許大陸地區廠商參與：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)

□是
□否
□3.給予下列差別待遇(可複選)：
□採購法第43條第1款之措施(招標文件須列明作為採購評選之項目及其比率)：
□採購法第43條第2款之措施：
□採購法第17條第2項處理辦法之措施：
如為工程採購，廠商履約過程中如有使用或供應下列材料或產品，其原產地須屬我國或其他條約或協定國家者(可複選)：
材料：
■水泥
■水泥製品
■鋼筋
■預力鋼絞線
■結構鋼
■陶瓷面磚
■透水性混凝土地磚
□砂石
□木材、竹材
□其他(由招標機關敘明)：
產品：
■升降機
■手扶梯
■阻尼器
■監視設備
■門窗
■櫥櫃
■空調設備
■消防栓
■照明燈具
■避雷針
■電氣設備
■太陽能設備
■衛浴設備
□其他(由招標機關敘明)：
☑(2)不適用我國締結之條約或協定，外國廠商：
□不可參與投標。我國廠商所供應標的(含工程、財物及勞務)之原產地須屬我國者。
□不可參與投標。但我國廠商所供應標的(含工程、財物及勞務)之原產地得為下列外國者：
1.國家或地區名稱：_____(未列明者即不允許)
2.是否允許供應大陸地區標的：(未勾選者即不允許；如允許者

，須符合兩岸進口及貿易往來相關規定)
□是
□否

☑下列外國廠商可以參與投標：
1.國家或地區名稱：均可(未列明者即不允許)
2.是否允許大陸地區廠商參與：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)
□是
☑否
□3.給予下列差別待遇（可複選）：
□採購法第 43 條第 1 款之措施(招標文件須列明作為採購評選之項目及其比率)：
□採購法第 43 條第 2 款之措施：
□採購法第 17 條第 2 項處理辦法之措施：

如為工程採購，廠商履約過程中如有使用或供應下列材料或產品，其原產地須屬我國或其他條約或協定國家者（可複選）：

材料：
■水泥
■水泥製品
■鋼筋
■預力鋼絞線
■結構鋼
■陶瓷面磚
■透水性混凝土地磚
□砂石
□木材、竹材
□其他(由招標機關敘明)：

產品：
■升降機
■手扶梯
■阻尼器
■監視設備
■門窗
■櫥櫃
■空調設備
■消防栓
■照明燈具
■避雷針
■電氣設備
■太陽能設備
■衛浴設備
□其他(由招標機關敘明)：

(3)廠商所供應整體標的之組成項目(例如製成品之特定組件、工程內含之材料與設施)，其不允許使用大陸地區產品之項目：
(4)本採購就取得或使用無人機部分應符合下列條款(與招標文件其他條款有不一致者，本條款優先適用)
(4-1)不允許大陸地區廠商、第三地區含陸資成分廠商、在臺陸資廠商及經濟部投資審議委員會公告之陸資資訊服務業者參與。且符合下列規定：
(4-1-1)屬機關取得財物者，廠商所供應標的，應符合相關目的事業主管機關之規範，整機並不得為大陸廠牌(不及於零組件之廠牌)。
機關有特殊需求者，不允許使用大陸地區製造或大陸廠牌之零組件：_____。[例如軍、警、海巡等機關或關鍵基礎設施、重要人士在場、犯罪偵監等，由機關衡酌個案特性妥適訂定]
(4-1-1-1)廠商履約所供應之無人機，應符合下列要求：
A.依遙控無人機管理規則第 17 條規定於交通部民用航空局登錄。
B.經無人機主管機關(交通部)及資通安全主管機關(數位發展部)認可之專業單位資安檢測通過，並持有該單位核發之資安檢測合格證明[無人機資安檢測需求詳附表]。
C.具射頻功能且屬國家通訊傳播委員會公告「應經核准之電信管制射頻器材」者，應取得該會核發之審驗證明。
(4-1-1-2)其他：_____。
(4-1-2)屬機關取得服務者，廠商履約人員不得為大陸籍人士，使用之無人機不得為大陸廠牌(不及於零組件之廠牌)。
機關有特殊需求者，不允許使用大陸地區製造或大陸廠牌之零組件：_____。[例如軍、警、海巡等機關或關鍵基礎設施、重要人士在場、犯罪偵監等，由機關衡酌個案特性妥適訂定]
(4-1-2-1)廠商履約所使用之無人機，應符合下列要求：
A.依遙控無人機管理規則第 17 條規定於交通部民用航空局登錄。
B.經無人機主管機關(交通部)及資通安全主管機關(數位發展部)認可之專業單位資安檢測通過，並持有該單位核發之資安檢測合格證明[無人機資安檢測需求詳附表]。
C.具射頻功能且屬國家通訊傳播委員會公告「應經核准之電信管制射頻器材」者，應取得該會核發之審驗證明。

(4-1-2-2)無人機操作人，均應具民航局核發之合格專業操作證。
(4-1-2-3)群飛活動應通過無人機飛行場域資通安全防護評估與檢測；飛經紅區者，其飛行計畫須經交通部及(或)活動所在之地方政府審核通過。
(4-1-2-4)法人應訂定作業手冊，經民航局能力審查核准，並經民航局及(或)地方政府同意飛航活動申請。
(4-1-2-5)其他：_____。

無人機資安檢測需求(註1)

適用資安檢測等級	適用情形	排除適用情形
一、無人機產品資安測試**中階**等級(註2)	有下列情形之一者： 1.飛經禁航區、限航區、民航局公告之航空站或飛行場四周或地方政府代中央機關公告之紅區 2.無人機重量 25 公斤以上	經上級機關核轉目的事業主管機關(交通部)及資通安全主管機關(數位發展部) 同意免予適用者。
二、無人機產品資安測試**初階**等級(註2)	飛經地方[直轄市、縣(市)]政府劃設紅區	有下列情形之一者，免予適用: 1.無自主導航且無攝影功能。 2.經地方政府同意免予適用者。 3.紅區所在機關辦理之教育訓練或競賽等低機敏性活動並報經地方政府備查。
三、無人機產品資安測試**初階**等級及群飛系統資安檢測(註2及3)	群飛架數 200 架以上且預計群聚人數達 1,000 人以上(註4)	

註1：本表無人機資安檢測需求係針對一般機關採購取得或使用無人機之基本需求，機關得依個案特性提高檢測安全等級。又因機關使用情境(例如涉軍、警、海巡等機關或關鍵基礎設施、重要人士在場、犯罪偵監等)，請機關衡酌個案特性，以適當資安標準妥適訂定。

註2：本表所稱產品資安檢測等級及檢測項目，係指「無人機資安聯合驗測實驗室」訂定之「無人機資安保障規範」第二部分產品資安測試安全等級及檢測項目(或其他同等級之標準或規範)，並以招標公告或邀標時適用之版本為準，履約期間如有變更資安需求者，得以契約變更方式處理。

註3：本表所稱「群飛系統資安檢測」，係引用台灣資通產業標準協會發布之「物聯網場域資安防護評估指引」安全等級 L1 級(或其他同等級之標準或規範)，針對應用層、網路層及感測設備層所包含設備之一般性安全功能的資安要求及測試評估，並以招

標公告或邀標時適用之版本為準，履約期間如有變更資安需求者，另以契約變更方式處理。

註4：群聚人數門檻係參考內政部「大型群聚活動安全管理要點」對於「大型群聚活動」之定義。

註5：機關應視個案實際情形於採購預算編列資安檢測費用。客製化之財物採購，第1次型式檢測費用由機關預算支應；勞務採購，機關依使用架數、使用頻率等因素評估所需檢測費用。

十七、本採購：
□(1)依採購法第 24 條規定以統包辦理招標。
☑(2)非以統包辦理招標。

十八、本採購：
□(1)依採購法第 25 條規定允許廠商共同投標(招標文件已附共同投標協議書範本)；廠商家數上限為□2 家；□3 家；□4 家；□5 家。
☑(2)不允許廠商共同投標。

十九、廠商得以電子資料傳輸方式於投標截止期限前遞送投標文件，該電子化資料，並視同正式文件，得免另備書面文件。供遞送之電傳號碼/網址為(不允許者免填)：

二十、廠商對招標文件內容有疑義者，應以書面向招標機關請求釋疑之期限：自公告日或邀標日起等標期之四分之一，其尾數不足1日者，以1日計。

二十一、機關以書面答復前條請求釋疑廠商之期限：投標截止期限前1日答覆。

二十二、本採購依採購法第33條第3項：不允許廠商於開標前補正非契約必要之點之文件。

二十三、本採購依採購法第35條：
□(1)允許廠商於在不降低原有功能條件下，可提出可縮減工期、減省經費或提高效率之替代方案（請載明允許項目）：
☑(2)不允許提出替代方案。

二十四、投標文件有效期：自投標時起至開標後30日止。如機關無法於前開有效期內決標，得於必要時洽請廠商延長投標文件之有效期。

二十五、廠商應遞送投標文件份數：
☑(1)1式1份。
□(2)1式2份。
□(3)1式3份。
□(4)1式4份。
□(5)1式5份。
□(6)其他(由招標機關敘明)：

二十六、投標文件使用文字：
□(1)中文(正體字)。

☑(2)中文(正體字)，但特殊技術或材料之圖文資料得使用英文。
☐(3)其他(由招標機關敘明)：

二十七、 公開開標案件之開標時間(依採購法不公開者免填)：
本案採一次投標(資、規格與價格)分段開標。第一階段資、規格標審查未通過者不得參與後續第二階段價格標之開標審查、議(比)價。
第一階段資、規格標開標時間：民國113年11月25日下午05時整(☑廠商得免派員參與，議價時間將另行通知 ☐廠商負責人或被授權人員須出席參與議價)。(截標日或開標日如因應颱風等災變，經臺北市政府宣布停止上班，則順延次一辦公日之同一截標或開標時間為截標日或開標日)
投標廠商提送各項文件資料，應符合本須知所訂條件，且經審查合格者，始得參加下一階段之開標、議(比)價。如審查時對資、規格有疑問時，得要求投標廠商澄清說明，投標廠商應於接獲本機關通知起二個日曆天(含例假日)內提供，廠商不得拒絕回答或藉機要求變動報價。如逾期未回復或補充後仍審查不合格，則視同資、規格不符，不得參加下一階段之開標、議(比)價。

二十八、 公開開標案件之開標地點(依採購法不公開者免填)：臺北市信義區吳興街250號臺北醫學大學醫學綜合大樓後棟一樓總務處會議室。

二十九、 公開開標案件有權參加開標之每一投標廠商人數(依採購法不公開或不限制廠商出席人數者免填)：一人。

三十、 依採購法不公開開標之依據：
☐(1)依採購法第 21 條規定辦理選擇性招標之資格審查，供建立合格廠商名單。
☐(2)依採購法第 42 條規定採分段開標，後續階段開標之時間及地點無法預先標示。
☐(3)依採購法第 57 條第 1 款規定。
☐(4)依採購法第 104 條第 1 項第 2 款規定。
☐(5)其他經主管機關認定者：_____(請載明核准文號)：

三十一、 本採購開標採：
☐(1)不分段開標。所有投標文件置於一標封內，不必按文件屬性分別裝封。
☑(2)分段開標(請勾選項目)；投標廠商應就各段標之標封分別裝封並標示內含資格標、規格標或價格標等：
☑公開招標，資格、規格與價格一次投標分段開標。
☐公開招標，資格與規格合併一段投標、分段開標，再邀符合招標文件規定之廠商投價格標。
☐選擇性招標，邀請廠商就資格、與規格、價格分次投標、分段開標。
☐選擇性招標，邀請符合資格之廠商就規格與價格一次投標、分段開標。

三十二、 押標金金額(無押標金者免填)：
☑(1)一定金額：新台幣 119,000 元整。
☐(2)標價之一定比率：__%。

三十三、 採電子投標之廠商，押標金予以減收金額(無者免填)：

三十四、 為押標金保證金暨其他擔保作業辦法第33條之5第2項所稱優良廠商者(公開於政府電子採購網https://web.pcc.gov.tw/常用查詢/優良廠商名單/有效名單列表)，押標金予以減收金額：
☐行政院公共工程委員會公共工程金質獎之得獎廠商，減收原應繳額度之50%。
☐其他獎項(由招標機關敘明獎項名稱及減收額度，其減收總額度不逾原定應繳總額之 50%)：
為押標金保證金暨其他擔保作業辦法第 33 條之 6 所稱全球化廠商者，押標金予以減收之金額(無者免填)：
為營造業法第 51 條所稱優良營造業，參與案件屬營造業法所稱營繕工程之工程採購者，押標金予以減收金額，其減收金額不併入前 2 項減收總額度計算(無者免填，惟押標金、工程保證金或工程保留款應至少擇一項給予獎勵)

三十五、 押標金有效期(無押標金者免填)：廠商以銀行開發或保兌之不可撤銷擔保信用狀、銀行之書面連帶保證或保險公司之保證保險單繳納押標金者，其有效期應較招標文件規定之報價有效期長三十日。

三十六、 押標金繳納期限：截止投標期限前繳納(無押標金者不適用)。

三十七、 以現金繳納押標金之繳納處所或金融機構帳號(無押標金者免填)：
(1)政府電子採購網線上繳納。(距截止投標期限不足 5 分鐘時，將無法使用本方式繳納押標金，請廠商提早作業)本校暫不接受以線上方式繳納。
(2)未採線上繳納者，其繳納處所或金融機構帳號：本校暫不接受以匯款方式繳納。

三十八、 無押標金之理由為：
☐(1)勞務採購。
☐(2)未達公告金額之工程、財物採購。
☐(3)以議價方式辦理之採購。
☐(4)依市場交易慣例或採購案特性，無收取押標金之必要或可能者。

三十九、 履約保證金金額(無者免填)：☐一定金額：_____；☑契約金額之一定比率：10 %。
☐廠商如以銀行之書面連帶保證或開發或保兌之不可撤銷擔保信用狀繳納履約保證金者，機關得視該銀行之債信、過去履行連帶保證之紀錄等，經機關審核後始予接受。廠商以押標金轉換為履約保證金時，亦同。

四十、 得標廠商提出其他廠商之履約及賠償連帶保證者，履約保證金予以減收之金額(無者免填)：

四十一、 得標廠商為押標金保證金暨其他擔保作業辦法第33條之5第2項所稱優良廠商者(公開於政府電子採購網https://web.pcc.gov.tw/常用查詢/優良

廠商名單/有效名單列表)，履約保證金予以減收金額：
☐行政院公共工程委員會公共工程金質獎之得獎廠商，減收原應繳額度之50%。
☐其他獎項(由招標機關敘明獎項名稱及減收額度，其減收總額度不逾原定應繳總額之 50%)：
得標廠商為押標金保證金暨其他擔保作業辦法第33條之6所稱全球化廠商者，履約保證金予以減收之金額(無者免填)：
得標廠商為營造業法第 51 條所稱優良營造業，且得標案件屬營造業法所稱營繕工程之工程採購者，履約保證金予以減收金額，其減收金額不併入前 2 項減收總額度計算(無者免填，惟押標金、工程保證金或工程保留款應至少擇一項給予獎勵)：

四十二、 履約保證金有效期(無履約保證金者免填)：較契約規定之履約期限長30日。履約事項驗收完成且無待解決事項為止，惟廠商以銀行開發或保兌之不可撤銷擔保信用狀、銀行之書面連帶保證或保險公司之保證保險單繳納履約保證金者，其有效期應較契約約定之最後施工、供應或安裝期限長____日(由機關於招標時自行填列，未填列者，為90日)。但得標廠商以銀行開立之不可撤銷擔保信用狀或銀行之書面連帶保證繳納，有效期未能立即涵蓋上述有效期，須先以較短有效期繳納者，其有效期每次至少__年(由機關於招標時自行填列，未填列者，為3年，末次之有效期得少於3年)。得標廠商應於有效期屆滿前__日(由機關於招標時自行填列，未填列者，為30日)辦理完成繳交符合契約約定額度之保證金。

四十三、 履約保證金繳納期限(無履約保證金者免填)：自決標次日起十四個工作日內。

四十四、 無履約保證金之理由為：
☐(1)勞務採購。
☐(2)未達公告金額之工程、財物採購。
☐(3)依市場交易慣例或採購案特性，無收取履約保證金之必要或可能者。

四十五、 保固保證金金額(無者免填)：契約金額之 3 %。

四十六、 保固保證金有效期(無保固保證金者免填)：較契約規定之保固期限長30日。廠商以銀行開發或保兌之不可撤銷擔保信用狀、銀行之書面連帶保證或保險公司之保證保險單繳納保固保證金者，其有效期應較契約規定之保固期長九十日。

四十七、 保固保證金繳納期限(無保固保證金者免填)：履約標的完成驗收合格後，機關付款前。

四十八、 得標廠商提出其他廠商之履約及賠償連帶保證者，保固保證金予以減收之金額(無者免填)：

四十九、 得標廠商為押標金保證金暨其他擔保作業辦法第33條之5第2項所稱優良廠商者(公開於政府電子採購網https://web.pcc.gov.tw/常用查詢/優良廠商名單/有效名單列表)，保固保證金予以減收金額：
☐行政院公共工程委員會公共工程金質獎之得獎廠商，減收原應繳額度之

50%。
☐其他獎項(由招標機關敘明獎項名稱及減收額度，其減收總額度不逾原定應繳總額之 50%)：
得標廠商為押標金保證金暨其他擔保作業辦法第33條之6所稱全球化廠商者，保固保證金予以減收之金額(無者免填)：
得標廠商為營造業法第 51 條所稱優良營造業，且得標案件屬營造業法所稱營繕工程之工程採購者，保固保證金予以減收金額，其減收金額不併入前 2 項減收總額度計算(無者免填，惟押標金、工程保證金或工程保留款應至少擇一項給予獎勵)：

五十、 預付款還款保證金額(無者免填)：

五十一、 預付款還款保證有效期(無預付款還款保證者免填)：

五十二、 預付款還款保證繳納期限(無預付款還款保證者免填)：

五十二之一、 植栽工程養護期保證金(僅適用於工程驗收合格後給付全部植栽價金之情形)額度為全部植栽價金之__%(由機關於招標時自行填列；未填列者，為25%)，於機關給付全部植栽費用時扣回，作為廠商植栽養護之擔保，無須另行繳納。

五十三、 各種保證金之繳納處所或金融機構帳號(無保證金者免填)：
(一)以金融機構本票、支票、保付支票或郵政匯票(票據請勿加「禁止背書轉讓」，以利作業)繳納者，應為即期且以本機關全銜「財團法人臺北醫學大學」為受款人。
(二)第一次投標前，請先至本校醫學綜合大樓後棟一樓總務處出納組繳納後，將此收據連同投標文件送至本校採購承辦李清蔓先生處，待檢核收據無誤，請將收據影本檢附於資、規格標封內，收據正本得逕行取回留存。
(三)押標金及各種保證金退還時機，均依各階段期限屆滿後，依本機關付款程序，無息退還。

五十四、 押標金及保證金應由廠商以現金、金融機構簽發之本票或支票、保付支票、郵政匯票、政府公債、設定質權之金融機構定期存款單、銀行開發或保兌之不可撤銷擔保信用狀繳納，或取具銀行之書面連帶保證、保險公司之連帶保證保險單繳納，並應符合押標金保證金暨其他擔保作業辦法規定之格式。

五十五、 廠商有下列情形之一者，其所繳納之押標金，不予發還；其未依招標文件規定繳納或已發還者，並予追繳：(無需押標金之案件免列)
(一) 以虛偽不實之文件投標。
(二) 借用他人名義或證件投標，或容許他人借用本人名義或證件參投標。
(三) 冒用他人名義或證件投標。
(四) 得標後拒不簽約。
(五) 得標後未於規定期限內，繳足履約保證金或提供擔保。
(六) 對採購有關人員行求、期約或交付不正利益。
(七) 其他經主管機關認定有影響採購公正之違反法令行為者。

前項追繳押標金之情形，屬廠商未依招標文件規定繳納者，追繳金額依招標文件中規定之額度定之；其為標價之一定比率而無標價可供計算者，以預算金額代之。

附記：主管機關認定之情形如下(行政院公共工程委員會 108 年 9 月 16 日工程企字第 1080100733 號令)：

1. 有採購法第 48 條第 1 項第 2 款之「足以影響採購公正之違法行為者」情形。
2. 有採購法第 50 條第 1 項第 5 款、第 7 款情形之一。
3. 廠商或其代表人、代理人、受雇人或其他從業人員有採購法第 87 條各項構成要件事實之一。

五十六、 廠商依「押標金保證金暨其他擔保作業辦法」規定減收押標金，其有不發還押標金之情形者，應就不發還金額中屬減收之金額補繳之。其經主管機關或相關中央目的事業主管機關取消優良廠商資格或全球化廠商資格，或經各機關依採購法第102條第3項規定刊登政府採購公報，且尚在採購法第103條第1項所定期限內者，亦同。

五十七、 本採購：

☑(1)訂底價，但不公告底價。

☐(2)訂底價，並公告底價。底價為：_____元。

☐(3)不訂底價，理由為：☐訂定底價確有困難之特殊或複雜案件；☐以最有利標決標之採購；☐專業服務、技術服務、資訊服務、社會福利服務或文化創意服務者，以不訂底價之最有利標； ☐小額採購。

五十八、 決標原則：

☑(1)最低標：

☑(1-1)非依採購法施行細則第 64 條之 2 辦理。

A. 第二階段價格標開標(議(比)價)時間：☐同開標日，於資、格標審查後接續辦理；☑另行通知(廠商須到場出席)。

B. 第二階段價格標開標(議(比)價)地點：☐同開標地點；☑另行通知

C. 投標廠商須依照機關所通知開標時間及地點，由負責人攜帶身分證明文件或代理人攜帶授權書及身分證明文件、投標印章(含負責人章)出席開標，依採購法第 51 條、第 53 條或第 54 條辦理時是出說明、減價或當場參加比減價格，非投標廠商之人員不得參與開標。廠商未派員當場者，視同放棄，喪失對投標文件提供說明或價格比減之權利。

D. 減價程序：

a. 開標後，合於招標文件規定之廠商僅有 1 家者，如其投標價逾底價，機關將逕洽該廠商減價，減價次數不得逾 3 次；合於招標文件規定之廠商如有 2 家以上者，其中之最低標超過底價時，得洽最低標廠商優先減價 1 次，減價結果如仍超過底價時，則由所有合於招標文件規定之投標廠商同時比減價格，比減價格次數不得逾 3 次。

b. 如有 2 家以上廠商標價相同，且均得為決標對象時，其比減價格次數已達採購法第 53 條規定之 3 次限制者，逕行抽籤決定之。前述標價相同，其比減價格次數未達 3 次者，應由該等廠商再行比減價格

1 次，以低價者決標。若比減後之標價仍相同者，抽籤決定之。

c. 標價不合理之處理：如最低標廠商之標價顯不合理，有降低品質、不能誠信履約之虞或其他特殊情形，則機關得依採購法第 58 條規定，要求最低標廠商於限期內提出說明或擔保。廠商未於通知期限內提出合理之說明或擔保者，機關得不決標予該廠商，並以次低標廠商為最低標廠商。

d. 投標廠商未到場參與開標者，則視同放棄說明、減價等各項權利，但不影響其為合格廠商，仍得為決標對象。

☐(1-2)依採購法施行細則第 64 條之 2 採評分及格最低標(審查項目、標準及審查方式如附件)。

☐(2)最有利標(評選項目、標準及評定方式如附件)。

☐(2-1)依採購法第 56 條適用最有利標(需報經上級機關核准)。

☐(2-2)依採購法第 22 條第 1 項☐第 9 款；☐第 10 款；☐第 11 款；☐第 14 款準用最有利標。

☐(2-3)未達公告金額之採購參考最有利標精神擇符合需要者辦理議價。

☐達一定分數或序位之未得標廠商，發給一定金額之獎勵金(由機關敘明一定分數或序位及其相對應之獎勵金)

分數(序位)：____；獎勵金：新臺幣____元

分數(序位)：____；獎勵金：新臺幣____元

分數(序位)：____；獎勵金：新臺幣____元

☐(3)最高標。

五十九、 本採購採：

☑(1)非複數決標。

☐(2)複數決標，保留採購項目或數量選擇之組合權利(項目或數量選擇之組合方式如附件。例如得由廠商分項報價之項目，或依不同數量報價之項目及數量之上、下限；投標廠商得標項目或數量之限制、開標順序、願比照得標廠商之價格者得併列為得標廠商、決標廠商家數上限等)。

六十、 本採購：

☐(1)預算未完成立法程序前，得先辦理保留決標，俟預算通過後始決標生效。

(2)決標方式為：

☑(2-1)總價決標。

☐(2-2)分項決標。

☐(2-3)分組決標。

☐(2-4)依數量決標。

☐(2-5)單價決標(以單價乘以預估數量之和決定得標廠商)。

☐(2-6)其他(由招標機關敘明)：

☐(3)屬勞動派遣(指派遣事業單位指派所僱用之勞工至機關提供勞務，接受各該機關指揮監督管理之行為)：派遣勞工(指受派遣事業單位僱用，並向各機關提供勞務者)之薪資(內含勞工依法自行負擔之勞保、健保、就業保險費用)與廠商應負擔之勞保、健保、就業保險費用、積欠工資墊

償基金提繳費及勞工退休金等費用，採固定金額支付，不列入報價範圍。廠商僅需就管理費用(含利潤、相關稅捐及管理所需一切費用等)報價。決標後，廠商報價與前述固定金額合計為契約總價，詳如附件報價明細表【註：報價明細表範例如附件，機關於招標時依案件性質參酌調整後附於投標須知。派遣勞工之加班費及差旅費，不含於契約價金，如發生此等費用，其計算方式依勞動法令規定另行支付】。

六十一、 無法決標時是否得依採購法第56條規定採行協商措施：

☐(1)是；採行協商措施得更改之項目（請敘明）：

☑(2)否。

六十二、 本採購保留未來向得標廠商增購之權利，擬增購之項目及內容(請載明擴充之金額、數量或期間上限，並應將預估選購或擴充項目所需金額計入採購金額。未保留增購權利者免填)：

六十三、 本採購適用採購法：

☑(1)無例外情形。

☐(2)本機關係軍事機關而有採購法第 104 條第 1 項但書之例外情形。

☐(3)有採購法第 105 條第 1 項之例外情形。

☐(4)有採購法第 106 條第 1 項之例外情形。

六十四、 投標廠商之基本資格及應附具之證明文件如下(如允許依法令免申請核發本項基本資格證明文件之廠商參與投標，一併載明該等廠商免繳驗之證明文件；另如允許合作社為投標廠商，且投標廠商為合作社者，應依合作社法之規定，並附具合作社章程，且章程業務項目需涵蓋本採購委託工作項目)：

☑登記或設立之證明：如公司登記或商業登記證明文件、非屬營利事業之法人、機構或團體依法須辦理設立登記之證明文件、工廠登記證明文件、許可登記證明文件、執業執照、開業證明、立案證明或其他由政府機關或其授權機構核發該廠商係合法登記或設立之證明文件。

上開證明，廠商得以列印公開於目的事業主管機關網站之資料代之。(營利事業登記證已不得作為此項證明之用)

☑廠商納稅之證明：廠商最近一期納稅證明文件，廠商不及提出最近一期證明者，得以前一期之納稅證明代之，新設立且未屆第一期營業稅繳納期限者，得以營業稅主管稽徵機關核發之核准設立登記公函代之；經核定使用統一發票者，應一併檢附申領統一發票購票證相關文件。

☑廠商信用之證明：如票據交換機構或受理查詢之金融機構於截止投標日之前半年內所出具之非拒絕往來戶及最近三年內無退票紀錄證明、會計師簽證之財務報表或金融機構或徵信機構出具之信用證明等。

☑廠商具有製造、供應或承做能力之證明：如有效期限內投標物之經銷證明。

☐廠商具有如期履約能力之證明。如迄投標日止正履行中之所有契約尚未完成部分之總量說明、此等契約有逾期履約情形者之清單、逾期情形及逾期責任之說明、律師所出具之迄投標日止廠商涉及賠償責任之訴訟中案件之清單及說明或廠商如得標則是否確可如期履約及如何能如期履約之說明等。

☐廠商或其受雇人、從業人員具有專門技能之證明。如政府機關或其授權機構核發之專業、專技或特許證書、執照、考試及格證書、合格證書、檢定證明或其他類似之文件。

☐廠商須具有維修、維護或售後服務能力之證明：如廠商維修工程師具受訓合格證明(相同機型)，或具有維持本儀器能力之證明。

☐外國廠商直接投標：請提出招標文件規定之資格文件，附經公證(經當地政府機關或公證機關完成公證)或認證(經由中華民國駐該國之代表認證)之中文譯本。外國廠商依該國情形提出有困難者，得於投標文件內敘明其情形或以其所具有之相當資格文件代之。

☐本採購屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，廠商不得為大陸地區廠商、第三地區含陸資成分廠商及經濟部投資審議委員會公告之陸資資訊服務業者。(上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議委員會網站 http://www.moeaic.gov.tw/)。(註：適用條約或協定之採購案，如勾選本項者，請依 GPA 第 3 條規定，妥適考量本須知第 16 點之勾選)。

☐本採購內容涉及國家安全，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與。(註：適用條約或協定之採購案，如勾選本項者，請依 GPA 第 3 條規定，妥適考量本須知第 16 點之勾選)

☐本採購允許合作社參與投標，投標廠商為合作社者，應附具合作社章程，且章程業務項目需涵蓋本採購委託工作項目。

六十五、 本採購採購屬特殊採購；符合「投標廠商資格與特殊或巨額採購認定標準」☐第6條第___款；☐第7條第___款 (請註明款次)。(非特殊採購者免填)

六十六、 投標廠商之特定資格及應附具之證明文件如下(限特殊或巨額之採購方可規定特定資格條件)：無。

六十七、 廠商所提出之資格文件影本，本機關於必要時得通知廠商限期提出正本供查驗，查驗結果如與正本不符，係不實之文件者，依採購法第50條規定辦理。

不同投標廠商參與投標，不得由同一廠商之人員代表出席開標、評審、評選、決標等會議，如有由同一廠商之人員代表出席情形，依採購法第50條第1項第1款或第7款規定辦理。

投標廠商之標價有下列情形之一為投標文件內容不符合招標文件之規定：(預算或底價未公告者免填)

☐(1)高於公告之預算者。

☐(2)高於公告之底價者。

機關辦理採購有下列情形之一者，得依採購法第50條第1項第5款「不同投標廠商間之投標文件內容有重大異常關聯者」之規定及行為事實，判斷認定是否有該款情形後處理：

一、投標文件內容由同一人或同一廠商繕寫或備具者。

二、押標金由同一人或同一廠商繳納或申請退還者。

三、投標標封或通知機關信函號碼連號，顯係同一人或同一廠商所為者。

四、廠商地址、電話號碼、傳真機號碼、聯絡人或電子郵件網址相同者。
五、其他顯係同一人或同一廠商所為之情形者。
機關辦理採購有「廠商投標文件所載負責人為同一人」之情形者，得依採購法第50條第1項第5款「不同投標廠商間之投標文件內容有重大異常關聯者」處理。
機關辦理採購，有3家以上合格廠商投標，開標後有2家以上廠商有下列情形之一，致僅餘1家廠商符合招標文件規定者，得依採購法第48條第1項第2款「發現有足以影響採購公正之違法或不當行為者」或第50條第1項第7款「其他影響採購公正之違反法令行為」之規定及行為事實，判斷認定是否有各該款情形後處理：
一、押標金未附或不符合規定。
二、投標文件為空白文件、無關文件或標封內空無一物。
三、資格、規格或價格文件未附或不符合規定。
四、標價高於公告之預算或公告之底價。
五、其他疑似刻意造成不合格標之情形。

☐工程採購案件，其屬營造業法所定營繕工程者，投標廠商屬營造業，可為決標對象，但決標金額高於營造業法所規定之承攬造價限額時，不決標予該廠商。
☐工程採購案件，其屬營造業法所定營繕工程者，投標之土木包工業須登記於工程所在地區之直轄市、縣(市)或營造業法第 11 條所定毗鄰之直轄市、縣(市)。如有違反，屬投標文件內容不符合招標文件之規定。

六十八、 外國廠商之投標資格及應提出之資格文件，附經公證或認證之中文譯本(不允許外國廠商投標者免填)：
(一)外國廠商直接投標請詳本案投標廠商之基本資格及應附具之證明文件。
(二)經由國內廠商代表外國投標廠商參加投標者，應由該外國廠商出具之「代理授權書」，外國廠商提出廠商登記或設立證明及廠商納稅證明之資格文件得以該國內廠商之資格代之。該國內廠商應另提出投標廠商聲明書，敘明其非屬不得參予採購之廠商。
(三)前項外國廠商參與之採購，有關文件之簽署應以該外國投標廠商之名義為之；其由國內廠商簽署者，應註明係「代理」該外國投標廠商。

六十九、 以選擇性招標方式辦理者，其限制投標廠商資格之理由及其必要性(非選擇性招標者免填)：

七十、 招標標的之功能、效益、規格、標準、數量或場所等說明及得標廠商應履行之契約責任：由招標機關另備如附件。

七十一、 依採購法第65條及採購法施行細則第87條之規定，本採購標的之下列部分及依其他法規規定應由得標廠商自行履約之部分，不得由其他廠商代為履行(視個案情形於招標時勾選；無者免填)：
☑(1)主要部分為：全部。
☐(2)應由得標廠商自行履行之部分為：　　。
☐除前項所列者外，屬營造業法第 3 條第 1 款之營繕工程，且得標廠商為

營造業者，其主要部分尚包括：工地主任、工地負責人、專任工程人員、安全衛生人員均應為廠商僱用之人員。

七十二、 招標文件如有要求或提及特定之商標或商名、專利、設計或型式、特定來源地、生產者或供應者之情形，允許投標廠商提出同等品，其提出同等品之時機為(由機關於招標時擇一勾選；未勾選者，為選項(2))：
☐(1)應於投標文件內預先提出者，廠商應於投標文件內敘明同等品之廠牌、價格及功能、效益、標準或特性等相關資料，以供審查。
☐(2)得標廠商得於使用同等品前，依契約規定向機關提出同等品之廠牌、價格及功能、效益、標準或特性等相關資料，以供審查。

七十三、 投標廠商之標價條件：
☐(1)送達招標機關指定地點(由招標機關敘明地點)：本機關。
☑(2)於招標機關指定地點完工(由招標機關敘明地點)：送達至本機關指定地點及招標文件所規定一切費用。
☐(3)其他(由招標機關敘明)：依標價清單相關規定。

七十四、 投標廠商標價幣別：
☑(1)新臺幣。
☐(2)外幣：_____(指定之外幣由招標機關敘明外幣種類)。
☐(3)新臺幣或外幣：_____(指定之外幣由招標機關敘明外幣種類，該外幣並以決標前一辦公日臺灣銀行外匯交易收盤即期賣出匯率折算總價)

七十五、 採購標的之維護修理(不需維護修理者免填)：
☑ (1)由得標廠商負責一定期間，費用計入標價決標(招標機關敘明其期間)：自正式驗收及試用合格之日起，由廠商全責保固一年，保固期內廠商應免費保養維護及全部零配件更換服務。如發生故障、零件損壞或效果不彰等情形時，廠商應於接獲本校通知日起二個工作天內，免費到場修復或更換。若逾此修復期限，廠商應無償提供同等品或替代方案，俾免影響教學研究之進行。
☐(2)由機關自行負責。
☐(3)另行招標。

七十六、 廠商有下列情形之一者，不得參加投標、作為決標對象或分包廠商或協助投標廠商：
(一)提供規劃、設計服務之廠商，於依該規劃、設計結果辦理之採購。
(二)代擬招標文件之廠商，於依該招標文件辦理之採購。
(三)提供審標服務之廠商，於該服務有關之採購。
(四)因履行機關契約而知悉其他廠商無法知悉或應秘密之資訊之廠商，於使用該等資訊有利於該廠商得標之採購。
(五)提供專案管理服務之廠商，於該服務有關之採購。
☐前項第 1 款及第 2 款之情形，於無利益衝突或無不公平競爭之虞，經機關同意者(本項未勾選者，表示機關不同意)，得不適用於後續辦理之採購。上述無利益衝突或無不公平競爭之虞之情形，於第 1 款指前階段規劃

或設計服務之成果一併於招標文件公開，且經機關認為參與前階段作業之廠商無競爭優勢者。

七十七、 全份招標文件包括：(可複選；刊登於政府電子採購網校內採購招標公告網之本案招標公告為招標文件之一部分，不另檢附)
☐(1)招標投標及契約文件。
☑(2)投標須知。
☑(3)投標標價清單。
☑(4)投標廠商聲明書。(詳附件一)
☐(5)契約條款。
☐(6)招標規範。
☑(7)其他(由招標機關敘明，無者免填)：
☑廠商資格、規格審查表：須檢附相關證件影本。(詳附件二)
☑出席代表授權書：廠商負責人得親自或授權人員參加採購案有關會議(會議當日須帶身份證明文件)，被授權人員應提交「出席代表授權書」(詳附件三)
☑投標標封標籤：請書名投標廠商名稱、地址等資訊，並就各標封分別裝封後張貼標籤，標示內含資、規格標或價格標等(詳附件四)
☑廠商投標文件領回申請書(詳附件五)
☑押標金轉作履約保證金同意書(詳附件六)

七十八、 廠商應送投標文件如下，未依本條規定投標者，審列為不合格標：
☑(1)廠商資格、規格審查表。(應加蓋廠商及負責人章)
☑(2)押標金收據影本。(得於繳交後，現場影印檢附)
☑(3)廠商設立(登記)證明(影本)。
☑(4)納稅(申報)證明影本或免稅證明影本。
☑(5)廠商信用證明影本。
☑(6)投標廠商聲明書。(應加蓋廠商及負責人章)
☑(7)非拒絕往來廠商查詢證明。(於截標日前請至中華民國行政院公共工程委員會全球資訊網 web.pcc.gov.tw 查詢並列印)
☑(8)廠商具有製造、供應或承做能力之證明影本。
☐(9)廠商具有如期履約能力之證明：
☐(10)廠商或其受雇人、從業人員具有專門技能之證明：
☐ (11)廠商須具有維修、維護或售後服務能力之證明影本。
☑(12)出席代表授權書。(應加蓋廠商及負責人章，負責人親自出席者免附)
☑(13)電子領標電子憑據書面明細。
☑(14)型錄或規格說明書。(須依標單規格分別標示清楚，以供請購單位審查)
☑(15)投標標價清單。(應加蓋廠商及負責人章)
投標廠商應依規定填妥(不得使用鉛筆)本招標文件所附招標投標文件、投標標價清單，連同資格文件、規格文件及招標文件所規定之其他文件，密封後投標。惟屬一次投標分段開標者，各階段之投標文件應分別密封後，再以大封套合併裝封。所有內外封套外部皆須張貼標籤(詳附件四)並書明投標廠商名稱、地址及採購案號或招標標的等聯絡資訊。廠商所提供之

投標文件，建議採雙面列印，以節省紙張，愛惜資源。
涉及未得標廠商投標文件著作財產權，機關如欲使用該等文件，應經該廠商同意無償授權機關使用，或由機關給予報酬後，於彼此約定範圍內使用。

七十九、 投標文件須於民國113年11月25日下午05時前，以郵遞、專人送達方式送達至下列收件地點：110臺北市信義區吳興街250號，臺北醫學大學醫學綜合大樓後棟一樓總務處事務組(李清萬先生收)。若逾時、未繳押標金或資格不符規定者，其所投之標單亦視為無效。截止投標日及開標日為辦公日，而該日因故停止辦公，依「因應颱風等災變部分地區停止上班，各機關招標公告之截止收件日或開標日是否延期處理原則」辦理。投標廠商投標後不得以任何理由要求修改標單內容或發還押標金、撤銷其報價單。

八十、 電子領標廠商之投標封附上該標案之領標電子憑據書面明細，或於開標後依機關通知再行提出。

八十一、 本須知未載明之事項，依政府採購相關法令。

八十二、 其他須知(請機關自行訂定。例如：採共同投標、統包、替代方案、國內廠商標價優惠、適用或準用最有利標評選作業或優先採購環保產品等方式辦理者，應注意依相關法規，將應於招標文件載明事項納入。)：
(一) 本案請購單位及聯絡方式：請購單位：資訊處，請購人，陳暐傑先生，聯絡人：陳暐傑先生(聯絡電話：02-2736-1661 #2626)
(二)截止投標日或截止收件日，因故停止上班，以其次一辦公日之同一截止投標或收件時間代之。開標日如遇不可抗力之災害，本機關停止上班，無法如期開標時，開標原則上以次一辦公日同時間同地點舉行代之，如開標時間、地點有一棟則由本機關另行以電話或其他方式通知投標廠商。
(三)本機關優先採購取得環境保護標章使用許可，而其效能相同或相似之產品。產品或其原料之製造、使用過程及廢棄物處理，符合再生材質、可回收、低污染或省能源者，亦同。其他增加社會利益或減少社會成本，而效能相同或相似之產品，準用前項之規定。(請務必於投標時檢附相關證明)
(四)為配合行政院環境保護署推動各機關綠色採購政策，投標廠商所報產品如已取得行政院環境保護署認可之環境保護產品使用許可或證明文件者，請逐項註明並於投標文件內檢附相關證明文件(並附列印公開於行政院環境保護署綠色生活資訊網站之資料佐證)。交貨時立約商須檢附該證明文件以供查核。若在本契約期間提出上項環境保護產品證明文件，亦得據以列入。廠商所報產品如已取得經濟部能源局核發之節能標章證書，亦得比照上述規定辦理。
(五)適逢本校署假期間，每星期三不上班，洽公請務必配合。

八十三、 受理廠商檢舉之採購稽核小組連絡電話、傳真及地址與法務部調查局及機關所在地之調查站處(站、組)檢舉電話及信箱：
(一) 教育部採購稽核小組(地址：100 臺北市中正區中山南路 5 號，電話：

02-77365529 、傳真：02-23583005)
(二) 臺北市調查處(地址：106 臺北市大安區基隆路二段 176 號;臺北市郵政 60000 號信箱、電話：02-27328888)
(三) 法務部調查局(地址:231 新北市新店區中華路 74 號;新店郵政 60000 號信箱、電話：02-29177777、傳真：02-29188888)
(四) 中央採購稽核小組(地址：110 臺北市信義區松仁路 3 號 9 樓、電話：02-87897548、傳真：02-87897554)
~~(五) 教育部政風處(地址：臺北市中正區中山南路 5 號、電話：02-77365837、傳真：02-23976940)~~
~~(六) 國家科學及技術委員會政風處(地址：臺北市和平東路二段 106 號 18 樓、電話：02-27377430、傳真：02-27377814)~~
~~(七) 法務部調查局檢舉電話(02-29188888、檢舉信箱：新店郵政 60000 號信箱)~~
~~(八) 臺北市調查處檢舉電話(02-27328888、檢舉信箱：臺北市郵政 60000 號信箱)~~
~~(九) 衛生福利部採購稽核小組(地址：115 臺北市南港區忠孝東路六段 488 號 5 樓、電話：02-85906579 、傳真：02-85906050)~~
~~(十) 臺北市調查處(地址：106 臺北市大安區基隆路二段 176 號;臺北市郵政 60000 號信箱、電話：02-27328888)~~
~~(十一) 法務部調查局(地址：231 新北市新店區中華路 74 號;新店郵政 60000 號信箱、電話：02-29177777、傳真：02-29188888)~~
~~(十二) 中央採購稽核小組(地址：110 臺北市信義區松仁路 3 號 9 樓、電話：02-87897548、傳真：02-87897554)~~

八十四、 法務部廉政署受理檢舉電話：0800-286-586；檢舉信箱：10099國史館郵局第153號信箱；傳真檢舉專線：02-2381-1234；電子郵件檢舉信箱：gechief-p@mail.moj.gov.tw；24小時檢舉中心地址：10048臺北市中正區博愛路166號。

標價清單

※請列出分項價格

採購名稱：防火牆日誌紀錄器

項目	數量	單價	總價
甲、 功能需求內容說明	2台		
1. 獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。			
2. 系統日誌接收效能可達 6,000 logs/sec (含)以上。			
3. 系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。			
4. 系統儲存容量可達 16 TB (含)以上，支援磁碟陣列 RAID 0/1, 1s/5, 5s/10 規範。			
5. 具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。			
6. 具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。			
7. 具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。			
8. 具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。			
9. 具備事件監看與告警功能，可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。			
10. 具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。			
11. 具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。			
12. 具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。			
13. 具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服			

項目	數量	單價	總價
器或 Common Event Format (CEF) 伺服器，以利與既有日誌系統整合。			
14. 具備管理區域 (Administrative Domain) 分割功能，並可針對不同管理人員賦予不同的管理權限。			
15. 具備 REST API，以利與既有資安環境整合。採購項目說明			

乙、 維護標的資訊一覽表

1. 維護等級5x8_設備清單

項次	設備型號	數量	維護期間
1	防火牆日誌紀錄器	1台	驗收日次日起算一年

2. 上述硬體設備得標廠商應提供自驗收次日起 1 年(5*8)人力到場維護保固服務及原廠經銷授權證明。
3. 得標廠商須提供原設備參數轉移與配合網路架構優化相關技術服務。
4. 為確保本案日後維護之保障，廠商須提供網路設備之原廠授權經銷商證明。

★本招標案件不得使用大陸廠牌資通訊產品(含軟體、硬體及服務)

請購單位：資訊處，請購人：陳曄傑 先生，聯絡電話：2736-1661 轉 2626

合計	新臺幣 佰 拾 萬 仟 佰 拾 元整(含稅)				
型號		原產地		Maker	
交貨期	廠商須於 113 年 12 月 13 日前，將採購標的送達請購單位指定地點，安裝測試完畢，且測試結果符合投標須知及標單、契約等規定。				
備註	※保固期至少為一年(或依原廠保固期較長為主)，請務必列出分項價格及廠牌。				
廠商資料	投標商名稱：			投標廠商及負責人章：	
	投標商統編：				
	投標商地址：				
	投標聯絡人：				
	聯絡人電話：		手機：	投標日： 年 月 日	

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **投標廠商聲明書：(第一次公告)** 標號：TMU113-103

附件一

投標廠商聲明書

本廠商參加(臺北醫學大學)招標採購防火牆日誌紀錄器案之投標，茲聲明如下：

項次	聲明事項	是(打V)	否(打V)
一	本廠商之營業項目不符合公司法或商業登記法規定，無法於得標後作為簽約廠商，合法履行契約。		
二	本廠商有違反政府採購法(以下簡稱採購法)施行細則第 33 條之情形。		
三	本廠商是採購法第 38 條規定之政黨或與政黨具關係企業關係之廠商。		
四	本廠商之負責人或合夥人是採購法第 39 條第 2 項所稱同時為規劃、設計、施工或供應廠商之負責人或合夥人。		
五	本廠商是採購法第 39 條第 3 項所稱與規劃、設計、施工或供應廠商同時為關係企業或同一其他廠商之關係企業。		
六	本廠商已有或將有採購法第 59 條第 1 項所稱支付他人佣金、比例金、仲介費、後謝金或其他不正利益為條件，促成採購契約之成立之情形。		
七	本廠商、共同投標廠商或分包廠商是採購法第 103 條第 1 項、採購法施行細則第 38 條第 1 項、人口販運防制法第 41 條所規定之不得參加投標或作為決標對象或分包廠商之廠商。【投標廠商應於投標當日遞送投標文件前至工程會網站 web.pcc.gov.tw 查詢自己(包括總公司及各分公司)、共同投標廠商、分包廠商是否為採購法第 103 條第 1 項之拒絕往來廠商】		
八	本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人。		
九	本廠商是依法辦理公司或商業登記且合於中小企業發展條例關於中小企業認定標準之中小企業。(依該認定標準第 2 條，所稱中小企業，指依法辦理公司登記或商業登記，實收資本額在新臺幣 1 億元以下，或經常僱用員工數未滿 200 人之事業。) (答「否」者，請於下列空格填寫得標後預計分包予中小企業之項目及金額，可自備附件填寫) 項目＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 項目＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 否計金額＿＿＿＿＿＿＿＿		
十	本廠商目前在中華民國境內員工總人數逾 100 人。(依採購法第 98 條及其施行細則第 107 條、108 條規定，得標廠商其於國內員工總人數逾 100 人者，應於履約期間僱用身心障礙者及原住民各不低於總人數百分之一，僱用不足者，除應繳納代金，並不得僱用外籍勞工取代僱用不足額部分。) (答「是」者，請填目前總人數計＿＿人；其中屬於身心障礙人士計＿＿人，原住民計　　人。)		
十一	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或經濟部投資審議委員會公告之陸資資訊服務業者，不得從事經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」。【上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議委員會網站http://www.moeaic.gov.tw/】【請查察招標文件規定本採購是否屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購】		
十二	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或在臺陸資廠商，不得從事影響國家安全之採購。【請查察招標文件規定本採購是否屬影響國家安全之採購】		

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **投標廠商聲明書：(第一次公告)** 標號：TMU113-103

十三	本廠商是原住民個人或政府立案之原住民團體。 (答「否」者，請於下列空格填寫得標後預計分包予原住民個人或政府立案之原住民團體之項目及金額，可自備附件填寫。如無，得填寫「0」) 項目＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 項目＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 否計金額		

附註	1. 第一項至第七項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象。 2. 本採購如非屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，第八項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象【違反公職人員利益衝突迴避法第 14 條第 1 項規定者，依同法第 18 條第 1 項處罰】。如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，答「是」、「否」或未答者，均可。 3. 第九項、第十項、第十三項未填者，機關得洽廠商澄清。 4. 本採購如屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，第十一項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 5. 本採購如屬影響國家安全之採購，第十二項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 6. 本聲明書填妥後附於投標文件遞送。 7. 本採購如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，且本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人者，請填「公職人員利益衝突迴避法第 14 條第 2 項公職人員及關係人身分關係揭露表」，如未揭露者依公職人員利益衝突迴避法第 18 條第 3 項處罰。
	投標廠商名稱：
	投標廠商章及負責人章： **日期：**

(引用行政院公共工程委員會 113.1.1 版)

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **其他附件：(第一次公告)** 標號：TMU113-103

附件二

投標廠商資、規格審查表

※請依表列順序排放證件影本並將本表置於首頁

廠商所提資格文件影本，本校得通知廠商限期提出正本供查驗，查驗結果如與正本不符，係偽造或變造者，依採購法第 50 條規定辦理。

採購名稱	防火牆日誌紀錄器	**採購案號**	1130203887
廠商名稱		**廠商統編**	
負責人		**廠商印鑑章**	
聯絡人	Email:		
聯絡電話	(市話) (手機)		
廠商地址	□□□：		

	投標廠商資格審查項目		招標機關資格審查
資規格項目	☑ 1.押標金(　119,000 元)繳納憑據 □ 依投標須知規定，免檢附	□符合 □不符合	**採購單位審查(項目1-8項)：** □合格 且開標前已至政採網查詢非拒絕往來廠商詳附件 □不合格，說明：
	☑ 2.廠商登記或設立證明	□符合 □不符合	
	☑ 3.廠商最近一期納稅證明	□符合 □不符合	
	☑ 4.廠商信用證明	□符合 □不符合	**採購單位簽章：**
	☑ 5.非拒絕往來廠商查詢並列印 (請至工程會網站 web.pcc.gov.tw 查詢列印)	□符合 □不符合	
	☑ 6.投標廠商聲明書	□符合 □不符合	
	☑ 7.出席代表授權書 □ 負責人親自出席，免檢附	□符合 □不符合	
	☑ 8.電子領標電子憑據	□符合 □不符合	
	☑ 9.廠商製造、供應或承做能力證明	□符合 □不符合	**請購單位審查(項目 9-11 項)：** □合格 □不合格，說明：
	□ 10.廠商須具有維修、維護或售後服務能力之證明	□符合 □不符合	
	☑ 11.型錄或規格說明書	□符合 □不符合	**請購單位簽章：**

投標廠商審查結果	投標廠商不符事項確認	投標廠商簽章▼
□合　格 □不合格	本廠商所投標及釋疑補充之文件等，經貴機關審核後，不符招標文件規範經本廠商確認無誤後，謹此簽章認同。	

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **其他附件：(第一次公告)** 標號：TMU113-103

附件三

出席代表授權書

茲授權本公司(商號或法人)所屬員工：＿＿＿＿＿＿＿＿先生/小姐代表本公司(商號或法人)出席貴校「**防火牆日誌紀錄器**」之開標/評選/議價會議，該員在開標/評選/議價會議中所做之任何承諾或簽認事項直接對本公司(商號或法人)發生效力，本公司(商號或法人)均予以承受，並經本公司(商號或法人)確認被授權人之下列簽樣真實無誤。

被授權人之簽樣[*註]：　　或

請惠予核備。

此　致

臺北醫學大學

授權人公司(商號)：
負責人姓名：
公司(商號)統一編號：
負責人身分證統一編號：

被授權人：
身分證統一編號：
通訊地址：
聯絡電話：

中　華　民　國　　年　　月　　日

*註：「被授權人簽樣」得為下列形式之1，依民法第 103 條規定，代理人於代理權限內所為之意思表示，直接對投標廠商發生效力：1.公司大小章。2.投標專用章。3.被授權人簽章。

附件四

投標標封標籤 (※請沿實線裁剪並彌貼於標封封面)

資、規格封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本資、規格封內請依投標須知規定裝入相關審核文件(請影印為 A4 尺寸)，並以迴紋針固定於左上角，俾利開標審核作業。

投標廠商		統一編號	
廠商地址		廠商聯絡人	
廠商電話		聯絡人電話	

價格封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本價格封內僅裝入『標價清單』等，其他投標文件請一律裝入資、規格封內。

投標廠商		統一編號	
廠商地址		廠商聯絡人	
廠商電話		聯絡人電話	

附件四

外標封標籤

(※請書寫完整資料並沿實線裁剪並貼於標封封面)

外標封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103 (第一次公告)
截止投標時間：113年11月25日下午05時整　　開標時間：113年11月25日下午05時整

11031 臺北市信義區吳興街 250 號
臺北醫學大學總務處事務組收
事務組採購承辦人：李清萬先生

投標廠商			統一編號	
廠商地址			廠商電話	
廠商聯絡人		聯絡人電話	聯絡人E-mail	

※注意事項：
一、投標文件遞送請注意時效，寄達本校事務組採購承辦人處，如逾時視為無效標。
二、投標文件應以不透明容器(封套)密封，外標封標籤請書寫完整基本資料後貼於標封封面，如未載明本案採購案名、標號及投標廠商、地址、電話或封口處未密封或信封套為透明者，皆視為無效標。

投標文件送達紀錄	遞送請填寫	□郵寄或快遞送達(免簽章及免填送達時間) □專人送達(送件須簽章並註記送達時間) 投標廠商送件人簽章： 送達日期及時間：	本校收件人簽名： 收件日期及時間：

附件五　(※本申請書得於申請退還時另行檢附，不須裝入標封內)

廠商投標文件領回申請書

一、本廠商參加【防火牆日誌紀錄器】案(第一次公告，標號：TMU113-103)之投標，茲因下列原因，請貴校退還本廠商所提送之投標文件：

(一)若本案流標者：
□參加投標廠商或合格廠商未達法定家數而流標。(可領回所有投標文件)

(二)若本標案廢標者：
□本標案開標後因故廢標。(投標文件原則不發還，可領回正本文件，另於影本上加蓋廠商及負責人印章後，由本校留存)

(三)其他：
□本廠商之投標文件，經貴校審查，不符合本案投標須知之形式審查規定。(可領回所有投標文件)
□本廠商之投標文件，經審查不符合本案投標須知之 □資格 □規格文件審查規定。(可領回未開封之文件)
□參與評審/評選作業，但未獲評為符合需要/優勝廠商。(除評審人員未返還及本校保留 3 份外，其餘可領回)
□本標案因有政府採購法第 48 條第 1 項各款情形之一而不予開標。(可領回全部投標文件)
□其他：

二、申請領回投標文件，得由負責人或委任代理人填妥本申請書(加蓋廠商及負責人印章，或與委任授權書相符之授權代理印章)，憑身分證明文件提出申請，並由本校核對後辦理退還。

三、領回清單如下：

文件名稱(□請勾選填寫)	份數	文件名稱(□請勾選填寫)	份數
□全部投標文件	份	□服務建議書或企畫書	份
□未開封之價格封	份	□其他：	份
□未開封之規格封	份		

四、領取人姓名：
(一)姓名：
(二)身分證字號：
(三)聯絡電話：
(四)領取日期：　年　月　日

五、投標廠商及負責人印章(請蓋與投標文件相同之印章)：

與投標文件相同之負責人章

六、領取人簽名：

附件六　(※本同意書得於繳納履約保證金時，另行檢附，不須裝入標封內)

押標金轉作履約保證金同意書

一、本廠商投標臺北醫學大學招標「防火牆日誌紀錄器」採購案(第一次公告，標號：TMU113-103)，經貴校宣布得標，謹此立書同意貴校逕將本廠商所繳押標金總計新臺幣___拾___萬___仟___佰元整。
(_____銀行庫_____分行(部.庫)之票據號碼_____號票據乙紙。)轉作履約保證金之一部分。

二、如本廠商應繳納履約保證金金額超過所繳押標金時，不足部分依本案招標文件及契約相關規定於繳納期限前攜帶押標金收據至貴校一併辦理補足。

此　致

臺北醫學大學

廠商名稱：
統一編號：
負 責 人：
負責人身分證字號：
電　　話：

(公司印鑑章)

(負責人章)

中　華　民　國　　年　　月　　日

密

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

採購案底價單

中華民國113年11月21日

請購單位	資訊處
採購名稱	防火牆日誌紀錄器
底價金額	新台幣：壹佰玖拾捌萬__仟__佰__拾__元整
備　　註	※本案開標後若因故流標，後次之開標如招標文件內容未做變更或補充，且請購單位不重估建議底價分析表時，得以原(本)核定之底價辦理。 ※依臺北醫學大學採購作業程序，底價單應於開標前，依採購分級由會議主席(或指定代理)與三位(含)以上採購委員簽署核定。

事務組經辦人簽章： 李清萬	**事務組組長簽章：**

採購委員簽章

□採購小組會 ■採購委員會	※事務組議價會則免簽。

會議主席(或指定代理)簽章

□事務組議價會	□採購小組會	■採購委員會

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

一一三學年度採購委員

事務組建議價格說明

「防火牆日誌紀錄器」

請購單位：資訊處
採購案號：1130203887
預算來源：教育部獎勵私立大學校院校務發展計畫 113-3600-001-212
預算金額：2,389,800元

請購單位：經自行分析結果，建議價格為 2,150,000 元

採購單位：查詢國外網站價格約台幣 981,694 元(美金 30393*匯率 32.3)，因本案需購置兩台，建議價格為 1,963,388 元

FORTIANALYZER-810G CENTRALIZED LOGANALYSIS APPLIANCE - 4X GE

by: FORTINET **PCN#:** JJ0471 **MFG#:** FAZ-810G

$30,393.36

FORTINET Authorized Dealer

− 1 +

Add to My Favorites

建議價格：1,963,388 元~2,150,000 元

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

採購案底價分析表

請購單位	資訊處網路通訊組	請購人	聯絡電話：2626 陳曄傑（請親簽）	採購案號	1130203887 (無則免填)
採購名稱	防火牆日誌紀錄器			辦理方式	☑公開招標 ☐限制性招標
預算編號 含主、次預算	※請依請購單上預算資料填寫 113-3600-001-212	預算來源	☐校內年度預算 ☑教育部獎補助 ☐研究計畫補助機關：＿＿＿＿ ☐其它經費：＿＿	預算金額	2,400,000

底價分析及理由說明

請就廠商得標歷史資料查詢、網路上之詢報價系統、廠商參考報價等，勾選下列選項(可複選)，並分析說明相同/相似標的之價格，如有相關佐證資料請一併提供。

☐本校過去採購案之決標紀錄
☐政府電子採購網之標案
☐報價廠商過去販售予其他機關單位之紀錄
☑經不同廠商報價比較結果
☐其他(如：自行分析成本後計算、屬寡占/獨占市場經參考廠商報價後計算、廠商提供本校優惠價等)

※**價格分析說明**：(採購品項或商情資料如較多，不敷使用可以續頁或附件方式說明)。

依廠商報價，預估成交金額可打9折，建議成交金額可落在2,150,000

(請以條列或表格敘述，可包括市場上近期同款設備成交價、不同之商業條款、不同廠商報價等。)

建議底價金額	☑新台幣：$2,100,000 ☐外　幣：(幣別)
法令依據	政府採購法施行細則第53條：機關訂定底價，應由規劃、設計、需求或使用單位提出預估金額及其分析後，由承辦採購單位簽報機關首長或其授權人員核定。但重複性採購或未達公告金額之採購，得由承辦採購單位逕行簽報核定。
備註	一、本表連同底價單(或採購案相關附件)依採購分級由會議主席(或其授權人員)與三位(含)以上採購委員簽署，核定底價。 二、本分析表欄位不敷使用時，請自行延伸之。 三、填妥簽章後，請務必於上傳於請採購系統上，正本請於採購立案後送交至事務組。

填表人已詳閱並自我檢核如下：(**請於下方簽章**)

- 應以維護公共利益及公平合理為原則，對廠商不得為無正當理由之差別待遇。(採購法第6條)
- 已將所需標的物依性質、屬性等，併此案統一辦理，並未分批採購。(採購法第14條)
- 所編列之預算符合市場行情。
- 所訂定之規格內容在目的及效果上均未限制競爭。(採購法第26條)
- 所訂定之規格內容，於驗收時不需送第三公證單位檢驗、測試或認證，且其驗收內容、標準或進行方式明確，不會具有爭議性。
- 所建議之底價金額已考量廠商應繳納之稅捐或規費、合理利潤、履約風險、應繳納押標金或保證金之成本、過去採購案例...等因素而提出。

請購人已詳閱，確認簽章：	請購單位主管/計畫主持人簽章：
陳曄傑	陳彥伯

※底價訂定之參考說明：(免附於底價分析表中)

1080102版

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

採購案底價分析表

一、 訂定底價時，宜一併考量下列情形，底價合理且符合實際需要：

(一) 廠商應繳納之稅捐或規費。

(二) 廠商之合理利潤。

(三) 廠商之履約風險。

(四) 參考過去採購案例者，該案例價格之合理性及不同履約時間、環境及條件所可能造成之價格差異。

(五) 相關物價指數或匯率變動情形。

(六) 廠商應繳納押標金或保證金之成本。

(七) 依法令規定應辦事項之費用。

二、 機關訂定底價，得基於技術、品質、功能、履約地、商業條款、評分或使用效益等差異，訂定不同之底價。(政府採購法施行細則第五十二條)

三、 底價之訂定，不能單憑主觀印象和以往的底價或決標紀錄，否則既不客觀也不合理。訂定底價可依二種方式：

(一) **可透過下列管道蒐集價格資料：**

1. 報載行情。
2. 市場調查資料。
3. 各著名工廠廠價。
4. 同業公會牌價。過去採購紀錄。
5. 臨時向有關廠商詢價。
6. 自其他機構調查採購價格。
7. 取得估算底價所須資料後，應經過分析研究，然後參酌採購案的各項條件，加計各項必需費用、利息、稅捐、利潤等計算出價格送至主管核定。

(二) 延聘專業人員估計：有些專業化、技術性程度較高的標的物或工程等，必須延聘專業人員，估算底價、辦理成本分析。

四、 底價定得太低，會造成廠商報價偏高廢標；底價定得太高，則浪費公帑。

五、 成本分析是採購時追求合理的價格手段。進行成本分析時通常最常見：

(一) 底價製作困難。

(二) 無法確定供應商的報價是否合理。

(三) 採購金額鉅大，成本分析有助於將來的議價工作。

六、 決定規格後，就要進行預估底價。**制定底價分析的益處：**

(一) 控制預算：採購案所訂定的底價，依據行情資料，但不能超過預算。

(二) 防止圍標搶標：採購案如不訂定底價，圍標搶標的結果，將使物品品質降低、交貨延期也難以避免。

(三) 提高採購作業效率：有了底價，採購在議、比價時能有所依據。也避免圖利他人，或因此而延宕訂約交貨時程。

臺北醫學大學
TAIPEI MEDICAL UNIVERSITY

☐ 信義校區：110 臺北市信義區吳興街250號
總機電話：02-2736-1661
Xinyi Campus： No.250, Wuxing St., Xinyi Dist.,
Taipei City 110, Taiwan. Tel：02-2736-1661

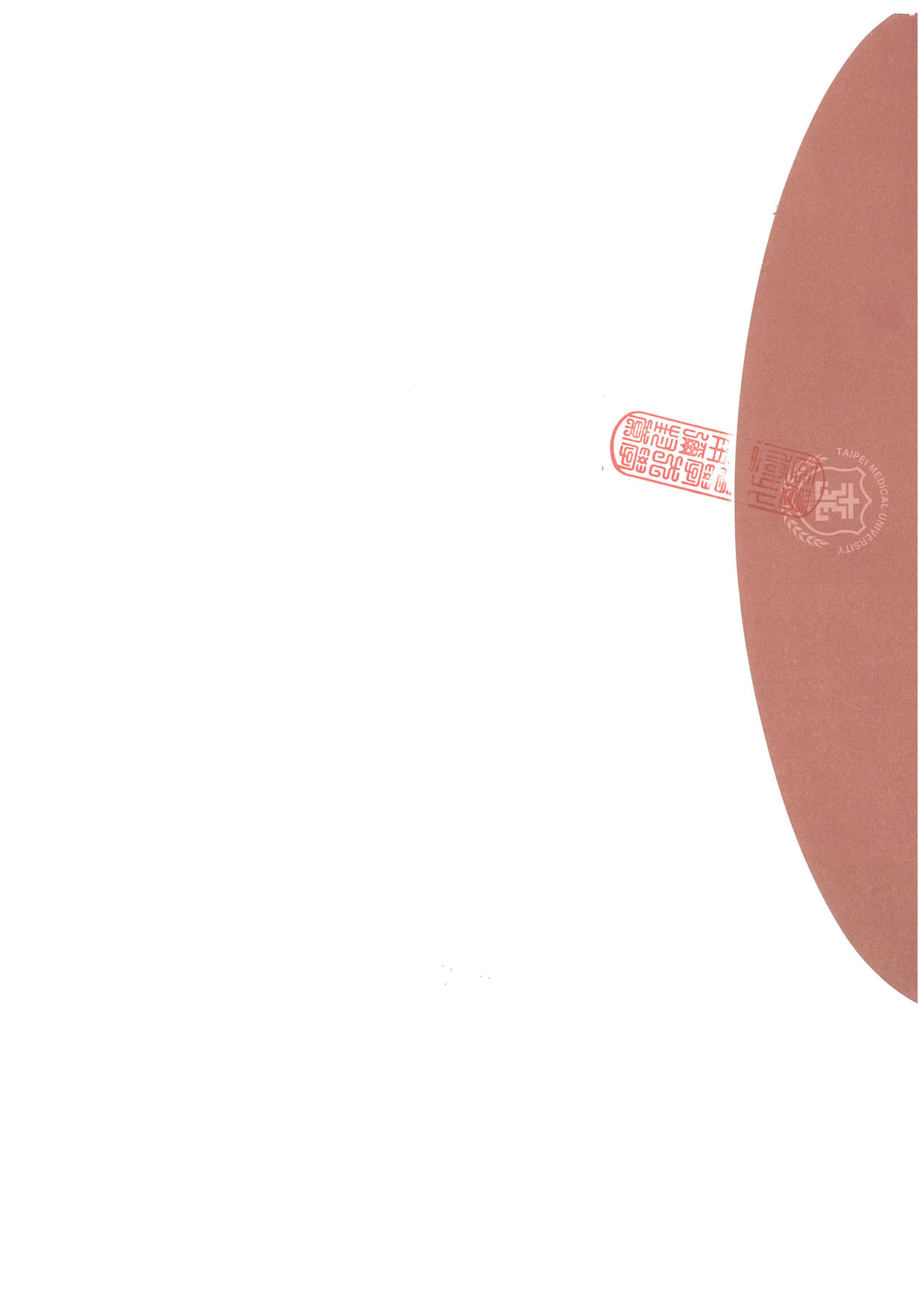
☐ 雙和校區：235 新北市中和區圓通路301號
總機電話：02-6620-2589
Shuangho Campus： No.301, Yuantong Rd., Zhonghe Dist.,
New Taipei City 235, Taiwan. Tel：02-6620-2589

密件

臺北醫學大學採購案底價封

標　　號：TMU113-103
議價日期：中華民國一一三年十一月二十五日
事務組經辦人：李清萬 113.11.21

採購名稱：防火牆日誌紀錄器
開標地點：本校醫學綜合大樓後棟一樓總務處會議室


TAIPEI MEDICAL UNIVERSITY

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

其他附件：(第一次公告) 標號：TMU113-103

附 件 二

投標廠商資、規格審查表

※請依表列順序排放證件影本並將本表置於首頁

廠商所提資格文件影本，本校得通知廠商限期提出正本供查驗，查驗結果如與正本不符，係偽造或變造者，依採購法第 50 條規定辦理。

採購名稱	防火牆日誌紀錄器	採購案號	1130203887
廠商名稱	四海資訊股份有限公司	廠商統編	22644575
負責人	陳松苗	廠商印鑑章	
聯絡人	林高春 Email: arthur@chho.com.tw		
聯絡電話	(市話) 02-2797-9331 (手機) 0919-58-9796		
廠商地址	□□□：台中市北屯區陳平路117巷46號之3		

	投標廠商資格審查項目		招標機關資格審查	
資規格項目	☑	1.押標金(119,000 元)繳納憑據 □ 依投標須知規定，免檢附	☑符合 □不符合	採購單位審查(項目1-8項)： ☑合格 且開標前已至政採網查詢非拒絕往來廠商詳附件 □不合格，說明： 採購單位簽章： 李彥蓉
	☑	2.廠商登記或設立證明	☑符合 □不符合	
	☑	3.廠商最近一期納稅證明	☑符合 □不符合	
	☑	4.廠商信用證明	☑符合 □不符合	
	☑	5.非拒絕往來廠商查詢並列印 (請至工程會網站 web.pcc.gov.tw 查詢列印)	☑符合 □不符合	
	☑	6.投標廠商聲明書	☑符合 □不符合	
	☑	7.出席代表授權書 □ 負責人親自出席，免檢附	☑符合 □不符合	
	☑	8.電子領標電子憑據	☑符合 □不符合	
	☑	9.廠商製造、供應或承做能力證明	☑符合 □不符合	請購單位審查(項目 9-11 項)： ☑合格 □不合格，說明： 請購單位簽章：陳聲傑
	□	10.廠商須具有維修、維護或售後服務能力之證明	□符合 □不符合	
	☑	11.型錄或規格說明書	☑符合 □不符合	

投標廠商審查結果	投標廠商不符事項確認	投標廠商簽章▼
☑合 格 □不合格	本廠商所投標及釋疑補充之文件等，經貴機關審核後，不符招標文件規範經本廠商確認無誤後，謹此簽章認同。	

列印時間 : 113/11/25 16:41

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為
廠商代碼： 22644575 (四海資訊股份有限公司)
廠商現況： 01-核准設立
廠商名稱： 四海資訊股份有限公司

資料取得時間：113/11/25 16:41

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

臺北醫學大學暫收款收據

007891

民國113年11月25日

繳款公司	四海資訊(股)公司		電話:0919789996	
款項名稱	①押標金 2圖說 3	採購案名稱	防火牆日誌紀錄器	
收款票據明細	支票號碼	EH 3733607	支票日期	113年11月18日
	付款銀行	第一商業 銀行庫 新湖	分行(部.庫)	
收款金額	新臺幣(大寫):仟佰壹拾壹萬玖仟佰拾元整			
備註	請妥善保管此收據，得標後憑此暫收據換正式收據。			

經收人:

出納組 113 11 25 許文嘉

112.05.01

第一聯：出納組聯（白）第二聯：暫收據（紅）

經濟部
商工登記公示資料查詢服務

Language

公司基本資料 董監事資料 經理人資料 分公司資料 工廠資料 跨域資料
歷史資料 自行揭露事項 法人董監網絡試用版

列印此頁 Line 複製連結

公司基本資料

統一編號	22644575 訂閱
登記現況	核准設立 「查詢最新營業狀況請至 財政部稅務入口網 」
公司名稱	四海資訊股份有限公司 Google搜尋 「國際貿易署廠商英文名稱查詢(限經營出進口或買賣業務者)」
章程所訂外文公司名稱	
資本總額(元)	12,000,000
實收資本額(元)	12,000,000
每股金額(元)	10
已發行股份總數(股)	1,200,000
代表人姓名	陳松苗
公司所在地	臺中市北屯區陳平路117巷46之3號 電子地圖
登記機關	臺中市政府
核准設立日期	076年09月29日
最後核准變更日期	111年12月28日
複數表決權特別股	無
對於特定事項具否決權特別股	無
特別股股東被選為董事、監察人之禁止或限制或當選一定名額之權利	無

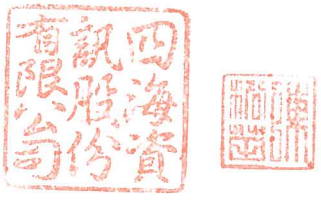
所營事業資料

E601020 電器安裝業
E603050 自動控制設備工程業
E605010 電腦設備安裝業
E701011 電信工程業
E801010 室內裝潢業
EZ99990 其他工程業
F113020 電器批發業
F113050 電腦及事務性機器設備批發業
F113070 電信器材批發業
F118010 資訊軟體批發業
F119010 電子材料批發業
F199990 其他批發業
F399040 無店面零售業
F399990 其他綜合零售業
F401010 國際貿易業
I301010 資訊軟體服務業
I301020 資料處理服務業
I301030 電子資訊供應服務業
ZZ99999 除許可業務外，得經營法令非禁止或限制之業務

(備註)

- 若須查詢該公司是否辦妥營業登記或仍在營業中，因非屬經濟部主管權責，請至財政部稅務入口網「**營業（稅籍）登記資料公示查詢網站**」查詢。謝謝!
- 若須查詢該公司依營造業法許可登記之所營事業項目最近異動情形及記錄，因非屬經濟部主管權責，請至內政部國土管理署-全國建築管理資訊系統入口網「**營造業-登記資料查詢網站**」查詢。謝謝!
- 若須查詢該公司依公寓大廈管理條例許可登記之所營事業項目最近異動情形及記錄，因非屬經濟部主管權責，請至內政部國土管理署-全國建築管理資訊系統入口網「**公寓大廈-管理維護公司資料查詢網站**」查詢。謝謝!
- 按證券投資信託及顧問法第6條規定，非經主管機關金融監督管理委員會核准，不得經營金融特許業務。涉及非法經營金融特許業務經法院判決確定之公司，可至「司法院裁判書系統」查詢：**https://judgment.judicial.gov.tw/FJUD/default.aspx**
- 從事經營「H304011證券投資顧問業」之公司須經金融監督管理委員會核准，公司名稱須標明「證券投資顧問」字樣，且限以「股份有限公司」型態經營。公司登記營業項目「I102010一般投資顧問業」及「I103060管理顧問業」非屬經金融監督管理委員會核准之特許事業或業務，依法不得在國內提供證券(或期貨)投資顧問服務。

諮詢專線：412-1166，直接撥打毋需加撥區碼 (六碼地區請撥 41-1166)，行動電話請加撥 02



第二聯：收執聯

營業人銷售額與稅額申報書(401)

（一般稅額計算----專營應稅營業人使用）

所屬年月份：113 年 09 — 10 月

金額單位:新臺幣元

註記欄	核准按月申報	
	核准合併總繳單位	總機構彙總報繳
		各單位分別申報

統一編號	22644575			使用發票份數	7 份
營業人名稱	四海資訊股份有限公司				
稅籍編號	470211517				
負責人姓名	陳松苗	營業地址	臺中市北屯區忠平里陳平路１１７巷４６－３號		

銷項

區分 / 項目	應稅 銷售額		應稅 稅額		零稅率銷售額	
三聯式發票、電子計算機發票	1	0	2	0	3（非經海關出口應附證明文件者）	
收銀機發票(三聯式)及電子發票	5	0	6	0	7	0
二聯式發票、收銀機發票(二聯式)	9	389,829	10	19,491	11（經海關出口免附證明文件者）	
免用發票	13	0	14	0	15	0
減：退回及折讓	17	0	18	0	19	0
合計	21（1）	389,829	22（2）	19,491	23（3）	0
銷售額總計 (1)+(3)	25（7）	389,829 元	（內含銷售固定資產	27	0 元）	

稅額計算

代號	項目		稅額
1.	本期(月)銷項稅額合計	(2) 101	19,491
7.	得扣抵進項稅額合計	(9)+(10) 107	1,760
8.	上期(月)累積留抵稅額	108	0
10.	小計(7+8)	110	1,760
11.	本期(月)應實繳稅額(1-10)	111	17,731
12.	本期(月)申報留抵稅額(10-1)	112	0
13.	得退稅限額合計	(3)x5%-(10)113	0
14.	本期(月)應退稅額(如 12>13 13>12 則為 13 12)	114	0
15.	本期(月)累積留抵稅額(12-14)	115	0

進項

區分 / 項目		得扣抵進項稅額 金額		稅額	
統一發票扣抵聯（包括一般稅額計算之電子計算機發票扣抵聯）	進貨及費用	28	0	29	0
	固定資產	30	0	31	0
三聯式收銀機發票扣抵聯及一般稅額計算之電子發票	進貨及費用	32	35,226	33	1,760
	固定資產	34	0	35	0
載有稅額之其他憑證（包括二聯式收銀機發票）	進貨及費用	36	0	37	0
	固定資產	38	0	39	0
海關代徵營業稅繳納證扣抵聯	進貨及費用	78	0	79	0
	固定資產	80	0	81	0
減：退出、折讓及海關退還溢繳稅款	進貨及費用	40	0	41	0
	固定資產	42	0	43	0
合計	進貨及費用	44	35,226	45（9）	1,760
	固定資產	46	0	47（10）	0
進項總金額（包括不得扣抵憑證及普通收據）	進貨及費用	48	35,226 元		
	固定資產	49	0 元		

進口免稅貨物	73	0 元	
購買國外勞務	74	0 元	

保稅區營業人按進口報關程序銷售貨物至我國境內課稅區之免開立統一發票銷售額 — 82. 0 元

收件編號：B226445751131036OA8
申報日期：113年11月12日
申報次數：001 次
進銷項筆數：14 筆
法院拍賣進項資料筆數：0 筆
零稅率銷售額筆數：0 筆
營業人申報固定資產退稅清單筆數：0 筆
營業人購買舊乘人小汽車及機車進項憑證明細筆數：0 筆
已納稅額：依實際繳款金額為準
最後異動日期：113年11月12日 19:31:41
製表日期：113年11月12日

財政部 中區國稅局 113.11.12 營業稅網路申報收件章

申辦情形	姓名	身分證統一編號	電話	登錄文(字)號
自行申報	陳松苗	K12090****	02-26589979	
委任申報				

說明

一、本申報書適用專營應稅及零稅率之營業人填報。
二、如營業人申報當期（月）之銷售額包括有免稅、特種稅額計算銷售額者，請改用（403）申報書申報。
三、營業人如有依財政部108年11月15日台財稅字第10804629000號令規定進行一次性移轉訂價調整申報營業稅，除跨境受控交易為進口貨物外，請另填報『營業稅一次性移轉訂價調整聲明書』並檢附相關證明文件，併同會計年度最後一期營業稅申報。
四、納稅者如有依納稅者權利保護法第7條第8項但書規定，為重要事項陳述者，請另填報「營業稅聲明事項表」並檢附相關證明文件。

四海資訊股份有限公司

與正本相符

1131112193141

財政部中區國稅局
營業稅繳款書

國　稅

所屬年月份：　113　年 09－10 月
（401一般稅額計算－專營應稅營業人使用）

收據聯： 本聯經收款蓋章後，交納稅義務人收執作納稅憑證。

營業人名稱：　四海資訊股份有限公司
營業地址：　臺中市北屯區忠平里陳平路１１７巷４６－３號
負責人姓名：　陳松苗

營利事業統一編號：　22644575
稅籍編號：　B470211517
繳納期限：　113年11月15日

項目	本稅		應納稅額合計	便利商店蓋章或收款公庫及經收人員蓋章
	17,731		17,731	
公庫計算	本稅逾期　天 加徵滯納金　%	本稅逾滯納期　天 加計利息	總計（元）	

說明：
一、繳款前請核對各項填報資料，資料如有不符，請修正資料後再重新列印繳款書，不得直接於繳款書上修改，以避免納稅資料條碼讀取內容不符，致生爭議。
二、按月申報之營業人，應於次月15日前繳納本月份應納稅額。按期申報之營業人，應於次期開始15日內繳納本期應納稅額。
三、納稅義務人逾限繳日期（如遇例假日則順延）繳納者，每逾3日按應納本稅加徵1% 滯納金至30日止，逾30日仍未繳納，且未請復查者，依法移送強制執行，應納本稅於滯納期滿(30日)之次日起依各年度1月1日郵政儲金1年期定期儲金固定利率，按日加計利息，一併徵收。對加徵滯納金如有不服，應於滯納期滿(30日)之翌日起30日內，申請復查。對本稅逾滯納期加計利息有不服，應於滯納期滿（30日）次日（處分生效日）之翌日起30日內，申請復查。
四、繳款書之代號應與填報之申報書代號相同。
五、繳納方式：
(一)臨櫃繳納：請至代收稅款金融機構繳納(郵局不代收)，稅額3萬元以下案件，可至統一、全家、萊爾富、來來(OK)等便利商店繳納。
(二)晶片金融卡網際網路轉帳繳納：請至網路繳稅服務網站(網址：https://paytax.nat.gov.tw)進行繳納。
※至便利商店或以晶片金融卡繳納者，繳納截止日開放至繳納期限屆滿後3日24時前，繳納期限屆滿後3日內繳納者，仍屬逾期繳納案件。

1131112193141

財政部中區國稅局
營業稅繳款書

國　稅

所屬年月份：　113　年 09－10 月
（401一般稅額計算－專營應稅營業人使用）

證明聯： 本聯經收款蓋章後，交納稅義務人持向稽徵機關申報。

營業人名稱：　四海資訊股份有限公司
營業地址：　臺中市北屯區忠平里陳平路１１７巷４６－３號
負責人姓名：　陳松苗

營利事業統一編號：22644575
稅籍編號：　B470211517
繳納期限：　113年11月15日

項目	本稅		應納稅額合計	便利商店蓋章或收款公庫及經收人員蓋章
	17,731		17,731	
公庫計算	本稅逾期　天 加徵滯納金　%	本稅逾滯納期　天 加計利息	總計（元）	

四海資訊股份有限公司

與正本相符

查詢者：195936 陳祺睿　查詢日期：2024-11-06 11:08:30

[資料來源：票交所]

第一類票據信用資料查覆單

茲將下列戶號(帳號)票據信用資料查覆如下，請　查照

查詢日：113年11月06日

戶名：四海資訊股份有限公司

開戶行代號：000000000

帳號：000000000

查覆資料截止日：113年10月30日

戶號：0022644575

負責人戶號：K120907537

查　覆　結　果

一、 退票與清償註記總數資訊(未清償註記提供最近三年內之退票未辦理清償註記者；已清償註記提供最近六個月內已辦理退票清償註記者)

退票理由	已清償註記		未清償註記	
	張數	金額	張數	金額
1. 存款不足	0	0	0	0
2. 發票人簽章不符	0	0	0	0
3. 擅自指定金融業者為本票之擔當付款人	0	0	0	0
4. 本票提示期限經過前撤銷付款委託	0	0	0	0

二、 拒絕往來資訊

無拒絕往來紀錄。

三、 經通報終止為其本票擔當付款人資訊

未經通報終止為其本票擔當付款人。

四、 開戶總數資訊

已在台灣地區全體金融業者開立支票存款戶共 003 戶。

五、 其他重大資訊

無。

六、 關係戶資訊

無。

說明：

(1) 查覆單列印之戶號後有(*)註記者，係指該戶號經電腦驗算為不合邏輯之資料。

(2) 查覆單列印之負責人戶號欄位空白者，係指該查詢申請單所填載之負責人，並非本所檔案中所建立該被查詢公司之負責人，如需所填載負責人票信資料者，請以負責人個人名義申請辦理。但查詢者提供被查詢公司之負責人相關資料，並經查證正確更改本所檔案資料後，該欄位即列印查詢申請單所填載之負責人身分證統一編號。

(3) 因建檔及註記作業時差，本查覆單「查覆結果」欄之資料，其中第一、六兩項資訊，除有關清償註記資訊提供至查詢日之前一營業日外，其餘提供至資料截止日，另肆項資訊提供至查詢日。

(4) 不具法人人格之行號、團體，應以其負責人個人名義申請票據信用資料查詢。

(5) 本查覆單「查覆結果」欄之資料，第六項關係戶資訊如有戶名及戶號時，其詳細票信資料請另向本所查詢。

(6) 本查覆單不得為竄改、複製、發布或其他不當使用。

(7) 本查覆單以由票據交換所或受理查詢金融機構出具，始可作為證明之文件。

資料來源：台灣票據交換所

單位章

與正本相符

[查詢條件]:22644575 查詢系統資訊: [Inquiry Task ID: 55063604] [Inquiry ID: 102655586] [ItemCacheInfo ID: 97183544]

列印時間：113/11/14 17:14

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為

廠商代碼： 22644575

（四海資訊股份有限公司）

廠商現況： 01-核准設立

廠商名稱： 四海資訊股份有限公司

資料取得時間：113/11/14 17:14

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

附 件 一

投標廠商聲明書

本廠商參加(臺北醫學大學)招標採購防火牆日誌紀錄器案之投標，茲聲明如下：

項次	聲明事項	是(打V)	否(打V)
一	本廠商之營業項目不符合公司法或商業登記法規定，無法於得標後作為簽約廠商，合法履行契約。		V
二	本廠商有違反政府採購法(以下簡稱採購法)施行細則第 33 條之情形。		V
三	本廠商是採購法第 38 條規定之政黨或與政黨具關係企業關係之廠商。		V
四	本廠商之負責人或合夥人是採購法第 39 條第 2 項所稱同時為規劃、設計、施工或供應廠商之負責人或合夥人。		V
五	本廠商是採購法第 39 條第 3 項所稱與規劃、設計、施工或供應廠商同時為關係企業或同一其他廠商之關係企業。		V
六	本廠商已有或將有採購法第 59 條第 1 項所稱支付他人佣金、比例金、仲介費、後謝金或其他不正利益為條件，促成採購契約之成立之情形。		V
七	本廠商、共同投標廠商或分包廠商是採購法第 103 條第 1 項、採購法施行細則第 38 條第 1 項、人口販運防制法第 41 條所規定之不得參加投標或作為決標對象或分包廠商之廠商。【投標廠商應於投標當日遞送投標文件前至工程會網站 web.pcc.gov.tw 查詢自己(包括總公司及各分公司)、共同投標廠商、分包廠商是否為採購法第 103 條第 1 項之拒絕往來廠商】		V
八	本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人。		V
九	本廠商是依法辦理公司或商業登記且合於中小企業發展條例關於中小企業認定標準之中小企業。(依該認定標準第 2 條，所稱中小企業，指依法辦理公司登記或商業登記，實收資本額在新臺幣 1 億元以下，或經常僱用員工數未滿 200 人之事業。) (答「否」者，請於下列空格填寫得標後預計分包予中小企業之項目及金額，可自備附件填寫) 項目＿＿＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 項目＿＿＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 合計金額＿＿＿＿＿＿＿＿	V	
十	本廠商目前在中華民國境內員工總人數逾 100 人。(依採購法第 98 條及其施行細則第 107 條、108 條規定，得標廠商其於國內員工總人數逾 100 人者，應於履約期間僱用身心障礙者及原住民各不低於總人數百分之一，僱用不足者，除應繳納代金，並不得僱用外籍勞工取代僱用不足額部分。) (答「是」者，請填目前總人數計＿＿人；其中屬於身心障礙人士計＿＿人，原住民計　　人。)		V
十一	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或經濟部投資審議委員會公告之陸資資訊服務業者，不得從事經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」。【上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議委員會網站http://www.moeaic.gov.tw/】【請查察招標文件規定本採購是否屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購】		V
十二	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或在臺陸資廠商，不得從事影響國家安全之採購。【請查察招標文件規定本採購是否屬影響國家安全之採購】		V

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 投標廠商聲明書：(第一次公告) 標號：TMU113-103

十三	本廠商是原住民個人或政府立案之原住民團體。 (答「否」者，請於下列空格填寫得標後預計分包予原住民個人或政府立案之原住民團體之項目及金額，可自備附件填寫。如無，得填寫「0」) 項目 0 金額 0 項目 0 金額 0 合計金額 0		V

附註	1. 第一項至第七項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象。 2. 本採購如非屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，第八項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象【違反公職人員利益衝突迴避法第 14 條第 1 項規定者，依同法第 18 條第 1 項處罰】。如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，答「是」、「否」或未答者，均可。 3. 第九項、第十項、第十三項未填者，機關得洽廠商澄清。 4. 本採購如屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，第十一項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 5. 本採購如屬影響國家安全之採購，第十二項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 6. 本聲明書填妥後附於投標文件遞送。 7. 本採購如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，且本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人者，請填「公職人員利益衝突迴避法第 14 條第 2 項公職人員及關係人身分關係揭露表」，如未揭露者依公職人員利益衝突迴避法第 18 條第 3 項處罰。
	投標廠商名稱： 四海資訊股份有限公司
	投標廠商章及負責人章： **日期：** 113.11.22

(引用行政院公共工程委員會 113.1.1 版)

附 件 三

出席代表授權書

茲授權本公司(商號或法人) 所屬員工：林高春 先生/~~小姐~~代表本公司(商號或法人)出席貴校「**防火牆日誌紀錄器**」之開標/評選/議價會議，該員在開標/評選/議價會議中所做之任何承諾或簽認事項直接對本公司(商號或法人)發生效力，本公司(商號或法人)均予以承受，並經本公司(商號或法人)確認被授權人之下列簽樣真實無誤。

被授權人之簽樣[*註]：林高春 或

請惠予核備。

此　　致

臺北醫學大學

授權人公司(商號)：四海資訊股份有限公司

負責人姓名：陳松苗

公司(商號)統一編號：22644575

負責人身分證統一編號：K120907537

被 授 權 人：林高春

身分證統一編號：A122077855

通訊地址：台北市文山區政大二街171巷40號6樓

聯絡電話：0919-58-9796

中　華　民　國　112　年　11　月　22　日

---

*註：『被授權人簽樣』得為下列形式之1，依民法第103條規定，代理人於代理權限內所為之意思表示，直接對投標廠商發生效力：1.公司大小章。2.投標專用章。3.被授權人簽章。

電子憑據資料	機關代碼	03724606
	機關名稱	臺北醫學大學
	標案案號	TMU113-103
	公告序號	01
	標案名稱	防火牆日誌紀錄器
	領標電子憑證序號	915000000000002330427
	使用者IP	61.220.41.90

力麗科技
LeaLea Technology

經銷授權證明書

茲證明四海資訊股份有限公司為 **Fortinet, Inc.**台灣地區之授權經銷商，可銷售 Fortinet 系列設備並履行產品之技術及保固責任。

案　　名：防火牆日誌記錄器

案　　號：TMU113-103

設備名稱：FAZ-810G*2

此致

臺北醫學大學

立證明書人：

力麗科技股份有限公司

本證明書僅限本採購案專用，若移作其他用途或證明及影本;非經本公司事先書面之認可,本公司一律概不承認。

中　華　民　國　一　一　三　年　十　一　月　十　五　日

設備規格答覆及資料佐證索引

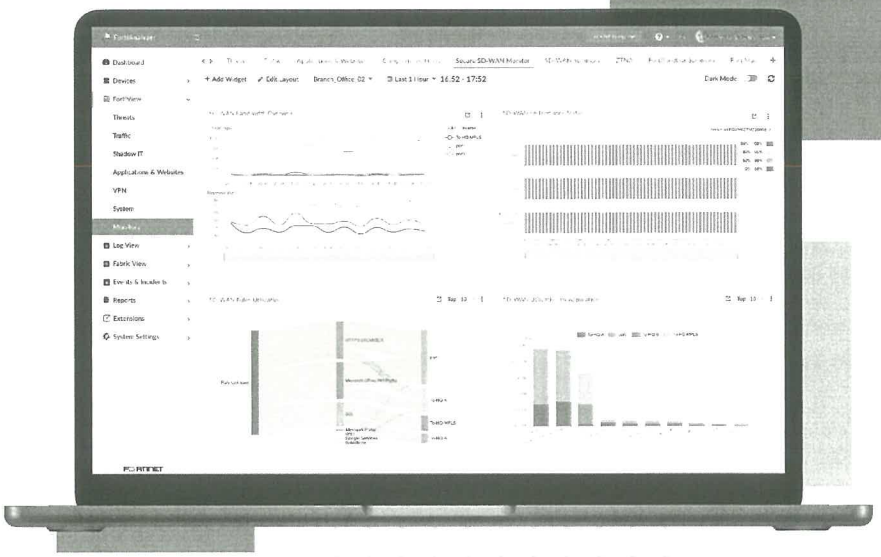
防火牆日誌紀錄器(FortiAnalyzer-810G)

項次	規格	符合	不符合	佐證資料
1	獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。	符合		附件 Page. 5
2.	系統日誌接收效能可達 6,000 logs/sec (含)以上。	符合		附件 Page. 7
3.	系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。	符合		附件 Page. 7
4.	系統儲存容量可達 16 TB (含)以上，支援磁碟陣列 RAID 0/1,1s/5,5s/10 規範。	符合		附件 Page. 7
5.	具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。	符合		附件 Page. 11
6.	具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。	符合		附件 Page. 12
7.	具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。	符合		附件 Page. 13 附件 Page. 14 附件 Page. 15
8.	具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。	符合		附件 Page. 16 附件 Page. 17 附件 Page. 18
9.	具備事件監看與告警功能，可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。	符合		附件 Page. 19 附件 Page. 20
10.	具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。	符合		附件 Page. 21
11.	具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。	符合		附件 Page. 22
12.	具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追	符合		附件 Page. 23

項次	規格	符合	不符合	佐證資料
	蹤與採取行動。			
13	具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服器或 Common Event Format (CEF) 伺服器，以利與既有日誌系統整合。	符合		附件 Page. 24
14	具備管理區域 (Administrative Domain) 分割功能，並可針對不同管理人員賦予不同的管理權限。	符合		附件 Page. 25
15	具備 REST API，以利與既有資安環境整合。	符合		附件 Page. 26

FortiAnalyzer™

Security Fabric Network Analytics



Highlights

- Centralized network monitoring and visibility
- Advanced threat and vulnerability detection with event and log data correlation
- Augmented NOC/SOC operations for real-time response, analytics, and reporting
- Automation to save time, reduce errors, and improve efficiency
- Multi-tenancy solution with quota management
- Administrative domains for operational effectiveness and compliance
- 70+ reports and 2000+ ready-to-use datasets, charts, and macros

Analytics, Reports, and Compliance Across the Security Fabric

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

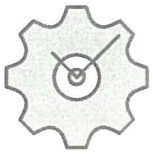
Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

Capabilities

Incident Detection and Response

Centralized NOC/SOC Visibility for the Attack Surface

FortiAnalyzer provides Security Fabric Analytics across all device logs with event correlation and real-time detection of Advanced Persistent Threats (APTs), vulnerabilities and Indicators of Compromise (IOC) for FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail and other Fortinet products, for deep visibility and critical network insights. Simplified orchestration and automated workflows provide Network Security Operations teams with real-time notifications, reports, and dashboards for single-pane visibility and actionable results.

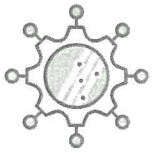


Incidents and Events Management

1-2

Security teams can monitor and manage alerts and event logs from Fortinet devices, with events processed and correlated in a format that analysts can easily understand. Investigate suspicious traffic patterns and search using filters in predefined or custom event handlers to generate real-time notifications and monitoring for NOC and SOC operations, SD-WAN, SSL VPN, wireless, Shadow IT, IPS, network recon, FortiClient, and more.

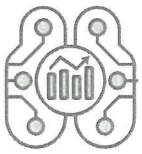
The Incidents component enables analysts to manage incident handling and life cycle, with incidents generated by events that show affected assets, endpoints, users and timelines.



Fabric Automation

FortiAnalyzer Playbooks boost an organization's security team abilities to simplify investigation efforts through automated incident response, freeing up resources and allowing analysts to focus on critical tasks. Out-of-the-box playbook templates enable SOC analysts to quickly customize their use cases, define custom processes, interact with other Security Fabric devices like FortiOS and EMS, edit playbooks and tasks in the visual playbook editor and use the Playbook Monitor for investigation of compromised hosts, infections and critical incidents, data enrichment for Assets and Identity views, blocking malware, C&C IPs, and more.

Security Fabric Analytics



Analytics and Reporting

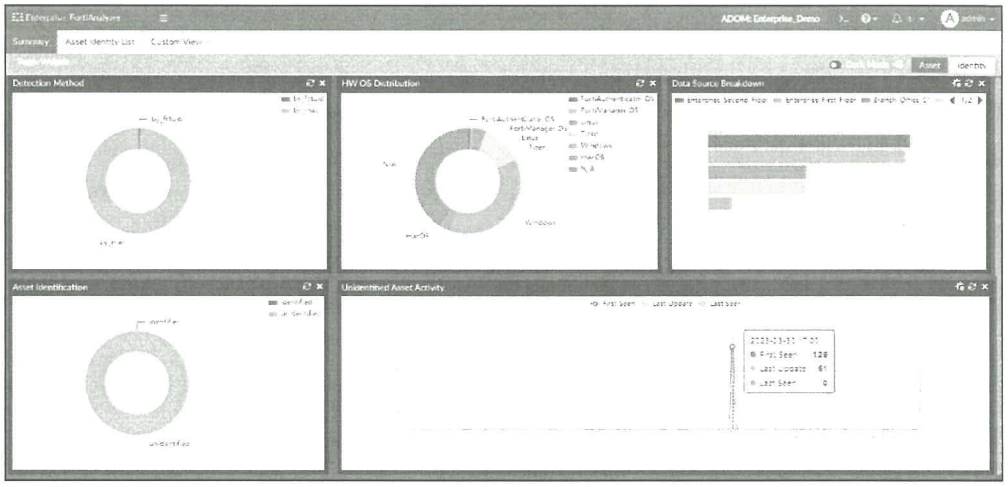
FortiAnalyzer automation driven analytics empowers network security operations teams to complete a fast assessment of network devices, systems, and users, with correlated log data and FortiGuard threat intelligence for analysis of real-time and historical events.

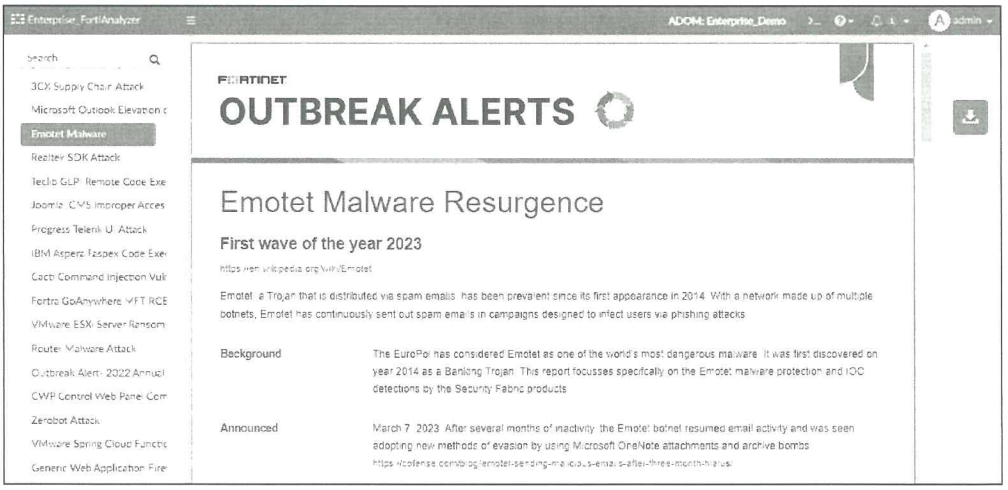
- **FortiView** Monitors and Views provide deep insights with context and meaning of network activity, risks, vulnerabilities, attack attempts, indicators of compromise and anomalies, sanctioned and unsanctioned user activity.
- **Log View** enables analysts to expand their investigation and utilize search filters on managed device logs, drill down on logs, with custom views and log groups, including a SIEM database with normalized logs for Fortinet devices in Fabric ADOMs.
- **Reports** provide comprehensive analysis of your Security Posture, including reports for Operational Technology (OT), security rating, security rating for PCI, Secure SD-WAN, VPN, FortiNDR network anomaly detection, cyber threat assessments, 360 Security Reviews, situational awareness, compliance, auditing, and more.

Capabilities

Assets and Identity

FortiAnalyzer Fabric View with Assets and Identity monitoring provides SOC teams with elevated awareness and visibility into an organization's endpoints and users with dashboards and correlated device and UEBA information, vulnerability detections, EMS tagging, and asset classifications through telemetry with EMS, NAC, Fortinet Fabric Agent, and an OT Dashboard View.





Subscriptions and Extensions

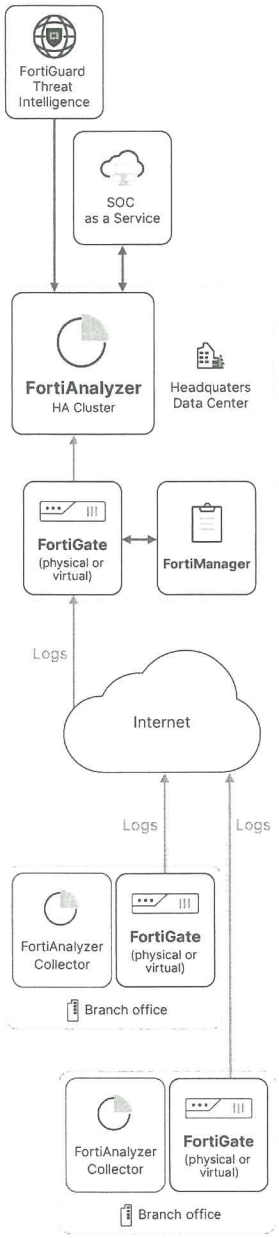
Subscription Licenses and FortiGuard Security Services

- **FortiGuard Outbreak Detection Service** delivers automated content package download for detecting the latest malware, including a summary of outbreaks and kill chain mapping for how the malware works. The package includes a FortiGuard Report for the outbreak, Event Handler, and a Report Template to detect outbreaks.
- **FortiGuard Indicators of Compromise Service** empowers security teams with forensic data from 500 000 IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system, that have been determined with high confidence to be malicious infections or intrusions, and historical rescan of logs for threat hunting.
- **Shadow IT Monitoring Service** provides continuous monitoring of unapproved devices, resources, unsanctioned accounts and unauthorized use of SaaS and IaaS, API integration, and third party apps. The service identifies rogue users using personal accounts for managing company assets, using correlated FortiOS and FortiCASB data with a FortiCASB account subscribed for SaaS features.
- **OT Security Service** provides security teams with advanced OT analytics, risk and compliance reports, OT event handlers, and use-case correlation rules.
- **Security Rating and Compliance Service** helps security teams design, implement, and maintain their security posture, and provides actionable configuration recommendations as well as key performance and risk indicators.
- **Security Automation Service** subscription enables further automation for incident response with enhanced monitoring and escalation, built-in incident management workflows, connectors, playbooks and more.

Management Extension Applications (MEAs)

The Management Extensions pane allows you to enable licensed applications that are released and signed by Fortinet, which can be installed and run on FortiAnalyzer, including the FortiSIEM and FortiSOAR.

Deployments



Deploying FortiAnalyzer

1-1

FortiAnalyzer can be deployed as a physical hardware appliance, virtual machine (VM) and virtual machine subscription (VM-S), as well as private or public cloud instance, with scalability, redundancy and backup, and high availability capabilities.

FortiAnalyzer High Availability (HA)

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

Multi-Tenancy with Flexible Quota Management

FortiAnalyzer provides the ability to manage multiple sub-accounts with each account having its own administrators and users. The time-based archive/analytic log data policy, per Administrative Domain (ADOM), allows automated quota management based on the defined policy, with trending graphs to guide policy configuration and usage monitoring.

Analyzer Collector Modes

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

FortiAnalyzer Fabric

FortiAnalyzer Fabric allows SOC Administrators to configure two operation modes - Supervisor and Member. This allows viewing of member devices, ADOMs and authorized logging devices, as well as incidents and events created on members. Admins get access to Reports and FortiView across all member FortiAnalyzers, and can perform global search in Log View of logs collected across FortiAnalyzer Fabric members with pre-defined device filters and log drill down for each Member and Member ADOMs.

Log Forwarding for Third-Party Integration

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

Cloud Services

FortiAnalyzer Cloud

FortiAnalyzer Cloud offers customers a PaaS-based delivery option for automation-driven, single pane analytics, providing log management, analytics, and reporting for Fortinet NGFW and SD-WAN with an easily accessible cloud-based solution. FortiAnalyzer Cloud delivers reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture. Customers can easily access their FortiAnalyzer Cloud from their FortiCloud single sign-on portal.

Virtual Offerings

FortiAnalyzer VM Subscription

The FortiAnalyzer VM Subscription license model consolidates into one single SKU: VM product SKU, FortiCare Support SKU, FortiGuard IOC and Outbreak Detection Service, Security Automation services, to simplify the product purchase, upgrade, and renewal. FortiAnalyzer-VM S provides organizations with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet and third party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer-VM S series SKUs come in stackable 5, 50, and 500 GB/ day logs licenses, so that multiple units of this SKU can be purchased together providing organizations with the ability and cost-efficiencies to scale and meet their logging needs.

FortiAnalyzer VM

Fortinet offers the FortiAnalyzer-VM licensing in a stackable perpetual license model with a-la-carte technical support and subscription services.

This software-based version of the FortiAnalyzer hardware appliance is designed to run on many virtualization platforms, which allows you to expand your virtual solution as your environment expands.

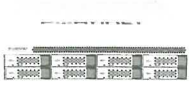
FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity						
GB/ day of Logs *	+1	+5	+25	+100	+500	+2000
Devices/VDOMs Maximum	10 000	10 000	10 000	10 000	10 000	10 000
FortiGuard IOC Service				✓		
Security Automation Service				✓		
Hypervisor Support	Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit https://docs.fortinet.com/product/fortianalyzer/ and find the Release Information at the bottom section Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"					
vCPU Support (Minimum / Maximum)	4 / Unlimited					
Network Interface Support (Min / Max) **	1 / 12					
Memory Support (Minimum / Maximum)	16 GB / Unlimited for 64-bit					

* Unlimited GB/ day when deployed in collector mode

** VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4 3+. Actual consumable numbers vary depending on cloud platforms

Specifications



FORTIANALYZER APPLIANCES	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000G
Capacity and Performance				
GB/ day of Logs	25	100	200	660
Analytic Sustained Rate (logs/ sec)*	500	2000	4000	20 000
Collector Sustained Rate (logs/ sec)*	750	3000	6000	30 000
Devices/VDOMs (Maximum)	50	180	800	2000
Max Number of Days Analytics**	90	50	50	60
Options				
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓	✓
Security Automation Service	✓	✓	✓	✓
Enterprise Bundle	✓	✓	✓	✓
Hardware Bundle	✓	✓	✓	✓
OT Security Service	✓	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓	✓
Hardware Specifications				
Form Factor (supports EIA/non-EIA standards)	Desktop	1 RU Rackmount	1 RU Rackmount	2 RU Rackmount
Total Interfaces	2x RJ45 GE	4x RJ45 GE	4x RJ-45 2x GE SFP	2× 2.5GbE RJ45 + 2× 25GbE SFP28
Storage Capacity	4TB (2× 2TB)	8 TB (2× 4 TB)	16TB (4× 4TB) 3.5 in SAS HDDs	32 TB (8 × 4TB) 3.5 in SAS SED HDD
Usable Storage (After RAID)	2 TB	4 TB	8 TB	24 TB
Removable Hard Drives	No	No	✓	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10	RAID 0/1/5/6/10/50/60
RAID Type	Software	Software	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	1	1	10	50
Redundant Hot Swap Power Supplies	No	Optional	Optional	✓
Trusted Platform Module (TPM) ***	Gen 2	Gen 2	✓	✓
Dimensions				
Height x Width x Length (inches)	9.5 × 3.5 × 8	1.73 × 17.24 × 16.38	1.73 × 17.32 × 21.65	3.46 × 17.24 × 24.41
Height x Width x Length (cm)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	4.4 × 44.0 × 55.0	8.8 × 43.8 × 62.0
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	25.75 lbs (11.68 kg)	49.6 lbs (22.5 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100-240Vac, 50~60Hz, 4A max	100-240Vac, 50~60Hz, 4A max
Power Consumption (Average / Maximum)	36 W / 43 W	90.1 W / 99 W	115W / 150W	251.36W / 302W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	433 BTU/h	857.73 BTU/h
Operating Temperature	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)
Storage Temperature	-4°F to 167° F (-20°C to 75° C)	-13°F to 167° F (-25°C to 75° C)	-4°F to 167° F (-20°C to 75° C)	-40°F to 158° F (-40°C to 70° C)
Humidity	5% to 95% non-condensing	20% to 90% non-condensing	5% to 95% non-condensing	5% to 95% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 16 404 ft (5000 m)
Compliance				
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

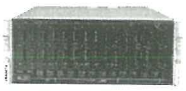
* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation

** The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

Specifications





FORTIANALYZER APPLIANCES	FAZ-3100G	FAZ-3510G	FAZ-3700G
Capacity and Performance			
GB/ day of Logs	3000	5000	8300
Analytic Sustained Rate (logs/sec)*	42 000	60 000	100 000
Collector Sustained Rate (logs/sec)*	60 000	90 000	150 000
Devices/VDOMs (Maximum)	4000	10 000	10 000
Max Number of Days Analytics**	30	35	60
Options			
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓
Security Automation Service	✓	✓	✓
Enterprise Bundle	✓	✓	✓
Hardware Bundle	✓	✓	✓
OT Security Service	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓
Hardware Specifications			
Form Factor (supports EIA/non-EIA standards)	3 RU Rackmount	4 RU Rackmount	4 RU Rackmount
Total Interfaces	2x GE RJ45, 2× 25GE SFP28	2× 10GbE RJ45, 2× 25GbE SFP28	2× 10GE RJ-45 + 2× 25GE SFP28
Storage Capacity	64 TB (16 × 4TB) 3.5" SAS SED HDD + 3.84 (2× 1.92TB) 2.5" NVMe SSD	24× 4TB (96TB) + 2× 3.84TB (7.68TB)	240TB (60× 4TB) 3.5 in HDD + 19.2TB (6× 3.2TB) NVMe SSD
Usable Storage (After RAID)	56 TB	84 TB	224 TB
Removable Hard Drives	✓	✓	✓
RAID Levels Supported	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60
RAID Type	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	50	50	50
Redundant Hot Swap Power Supplies	✓	✓	✓
Trusted Platform Module (TPM) ***	✓	✓	✓
Dimensions			
Height x Width x Length (inches)	5.2 × 17.2 × 25.5	7 × 17.2 × 27.5	7.0 × 17.2 × 30.2
Height x Width x Length (cm)	13.0 × 44.0 × 65.0	17.8 × 43.7 × 69.9	17.8 × 43.7 × 76.7
Weight	69.6 lbs (31.57 kg)	65 lbs (29.5 kg)	118 lbs (53.5 kg)
Environment			
AC Power Supply	100-127V~/10A, 200-240V~/5A	100-127V~/10A, 200-240V~/5A	2000W AC****
Power Consumption (Average/Max)	395 W / 510 W	983 W / 1278 W	850 W / 1423.4 W
Heat Dissipation	1740.19 BTU/h	3424 BTU/h	4858 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	50°F to 95°F (10°C to 35°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)	-4°F to 167°F (-20°C to 75°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	5% to 95% (non-condensing)	5% to 95% (non-condensing)	8% to 90% (non-condensing)
Forced Airflow	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 13 123 ft (4000 m)	Up to 10 000 ft (3048 m)	Up to 7400 ft (2250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release

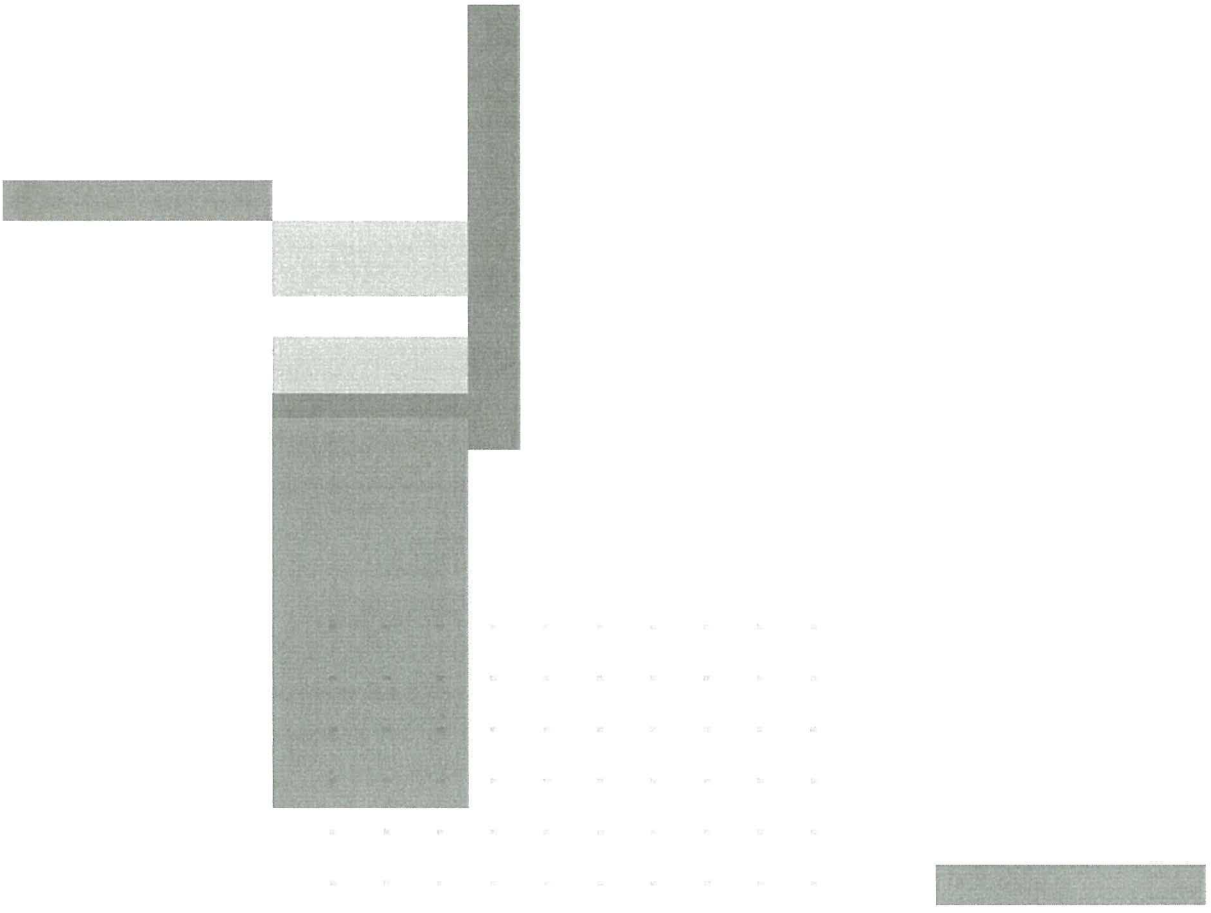
****3700G must connect to a 200V - 240V power source.

Ordering Information

Product	SKU	Description
FortiAnalyzer	FAZ-150G	Centralized log and analysis appliance — 2x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.
	FAZ-300G	Centralized log and analysis appliance — 4x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.
	FAZ-810G	Centralized log and analysis appliance — 4x GE, 2x SFP, 16 TB self-encrypting storage, up to 200 GB/ day of logs
	FAZ-1000G	Centralized logging and analysis appliance - 2× 2.5GbE RJ45 + 2× 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs.
	FAZ-3100G	Centralized log and analysis appliance — 2x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3000 GB/ day of logs.
	FAZ-3510G	Centralized log and analysis appliance — 2× 10GbE RJ45, 2× 25GbE SFP28, 96 TB storage, up to 5000 GB/ day of logs.
	FAZ-3700G	Centralized log and analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 240TB HDD + 19.2TB NVMe SSD storage, up to 8300 GB/ day of Logs
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-465-01-DD	Subscription license for 5 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC2-10-AZVMS-465-01-DD	Subscription license for 50 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC3-10-AZVMS-465-01-DD	Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
FortiAnalyzer-VM	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs
	FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of Logs.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs.
FortiAnalyzer Cloud Storage Subscription	FC1-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service
	FC2-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
	FC3-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
FortiAnalyzer - Backup to Cloud Service	FC-10-FAZ00-286-02-DD	One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud
FortiAnalyzer Cloud with SOCaaS	FC-10-[Model Code]-464-02-DD	FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.
FortiAnalyzer Cloud	FC-10-[Model Code]-585-02-DD	FortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service.
Security Automation Service	FC-10-[Model Code]-335-02-DD	Subscription license for Security Automation Service - Appliance.
	FC[GB Day Code]-10-LV0VM-335-02-DD	Subscription license for Security Automation Service - Virtual Machine
FortiGuard IOC and Outbreak Detection Service	FC-10-[Model Code]-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.
	FC[GB Day Code]-10-LV0VM-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.
OT Security Service	FC-10-[Model Code]-159-02-DD	OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules.
FortiAnalyzer Security Rating and Compliance Service	FC-10-[Model Code]-175-02-DD	Subscription license for FortiAnalyzer Security Rating and Compliance Service.
Enterprise Protection Bundle	FC-10-[Model Code]-466-02-DD	Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).
Hardware Bundle	FAZ-[Hardware Model]-BDL-466-DD	Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

June 4, 2024

FAZ-DAT-REG-20210604

Log View and Log Quota Management

You can view log information by device or by log group.

When rebuilding the SQL database, *Log View* is not available until the rebuild is complete. Click the *Show Progress* link in the message to view the status of the SQL rebuild.

When ADOMs are enabled, each ADOM has its own information displayed in *Log View*.

Log View can display the real-time log or historical (Analytics) logs.

Log Browse can display logs from both the current, active log file and any compressed log files.

For more information, see Analytics and Archive logs on page 42.

Types of logs collected for each device

1-5

FortiAnalyzer can collect logs from the following device types: FortiADC, FortiAnalyzer, FortiAuthenticator, FortiCache, FortiCarrier, FortiCASB, FortiClient, FortiDDoS, FortiDeceptor, FortiEDR, FortiGate, FortiIsolator, FortiMail, FortiManager, FortiNAC, FortiNDR (formerly FortiAI), FortiPAM, FortiProxy, FortiSandbox, FortiSOAR, FortiWeb, and Syslog servers. Following is a description of the types of logs FortiAnalyzer collects from each type of device:

Device Type	Log Type
Fabric	All
FortiADC	Event, Intrusion Prevention, Traffic
FortiAnalyzer	Event, Application
FortiAuthenticator	Event
FortiGate	Traffic Security: Antivirus, Intrusion Prevention, Application Control, Web Filter, File Filter, DNS, Data Loss Prevention, Email Filter, Web Application Firewall, Vulnerability Scan, VoIP, FortiClient Event: Endpoint, HA, Compliance, System, Router, VPN, User, WAN Opt. & Cache, WiFi  File Filter logs are sent when the File Filter sensor is enabled in the FortiOS Web Filter profile. You can enable the File Filter sensor in FortiOS at *Security Profiles* > *Web Filters*.
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiCarrier	Traffic, Event, GTP

To query the log file's MD5 checksum in the CLI:

1. Enter the following command in the FortiAnalyzer CLI:
   ```
   execute log-integrity <device_name> <vdom name> <log_name>
   ```
   For example:
   ```
   execute log-integrity FGVM01TM20000000 root tlog.1608279204.log.gz
      Integrity checking passed:
      MD5 checksum is [82598ec0086319db73bd0f9de2396047]
   ```

Secure Log Transfer

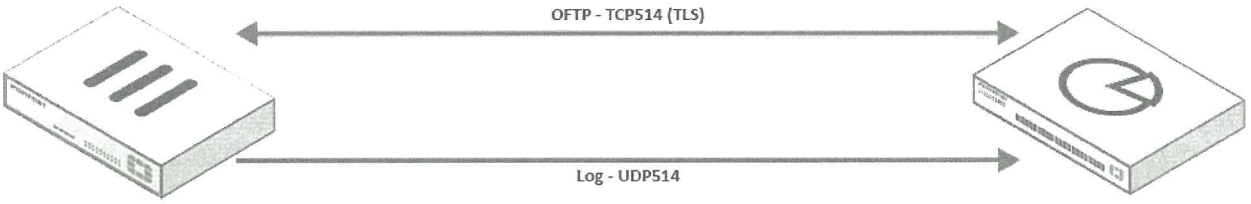
1-6

Optimized Fabric Transfer Protocol (OFTP) is a proprietary Fortinet protocol. It is used for connectivity, performing health checks, file transfers, and log display on FortiGate. OFTP listens on ports TCP514 and UDP514.

In the default configuration, there are two communication streams between FortiGate and FortiAnalyzer. OFTP communication is encrypted and log communication is not.

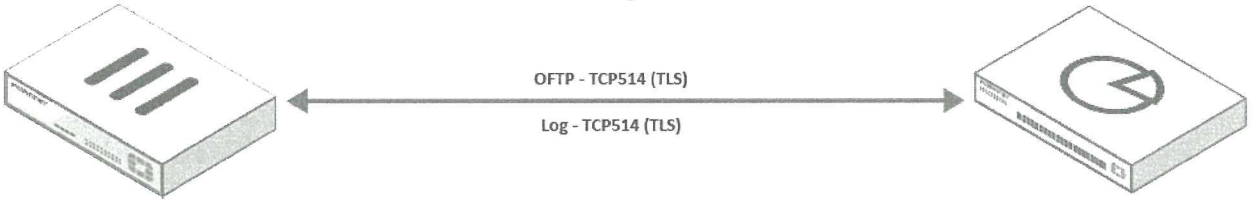
- OFTP communication occurs on TCP514 using TLS.
- Log communication occurs on UDP514 (default setting).

Default FortiGate Settings



To secure log transfer, you can enable TCP and encryption. When enabled, logs are transferred securely between the FortiGate and FortiAnalyzer using TCP514 (TLS).

Secure Log Transfer



Configuring secure log transfer settings

Reliable logging from FortiGate to FortiAnalyzer prevents lost logs when the connection between FortiGate and FortiAnalyzer is disrupted. If connection is lost between the FortiAnalyzer and FortiGate device, logs will be cached and sent to FortiAnalyzer once the connection resumes.

For more information, see *FortiAnalyzer log caching* in the FortiGate / FortiOS Administration Guide.

Reports

1-7

You can generate data reports from logs by using the *Reports* feature. You can do the following:

- Use predefined reports. Predefined report templates, charts, and macros are available to help you create new reports.
- Create custom reports.

Report files are stored in the reserved space for the FortiAnalyzer device. See Automatic deletion on page 150.

When rebuilding the SQL database, *Reports* are not available until the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

For more information on FortiAnalyzer report technology and troubleshooting report performance issues, see the *FortiAnalyzer Report Performance Troubleshooting Guide*.

How ADOMs affect reports

When ADOMs are enabled, each ADOM has its own reports, libraries, and advanced settings. Make sure you are in the correct ADOM before selecting a report. See Switching between ADOMs on page 31.

Some reports are available only when ADOMs are enabled. For example, ADOMs must be enabled to access FortiCarrier, FortiCache, FortiClient, FortiDDoS, FortiMail, FortiSandbox, and FortiWeb reports. In a Security Fabric ADOM, all reports are displayed.

You cannot import reports to ADOMs that do not match the device type used in the charts and datasets for the report. Fabric ADOMs support all reports, regardless of the device type used in the charts and datasets. For example, a FortiGate report cannot be imported to an ADOM for a different device type; it can only be imported to a FortiGate or Fabric ADOM.

You can configure and generate reports for these devices within their respective default ADOM or a Security Fabric ADOM. These devices also have device-specific charts and datasets.

ADOM limits for reports

The following table identifies FortiAnalyzer ADOM limits for reports.

Report object	Per ADOM limit
Chart	5000
Dataset	5000
Macro	5000
Layout	2000

Step 2: Initiate a rebuild of hcache tables

To initiate a rebuild of hcache tables, enter the following CLI command:

```
diagnose sql hcache rebuild-report <start-time> <end-time>
```

Where `<start-time>` and `<end-time>` are in the format: `<yyyy-mm-dd hh:mm:ss>`.

Retrieving report diagnostic logs

Once you start to run a report, FortiAnalyzer creates a log about the report generation status and system performance. Use this diagnostic log to troubleshoot report performance issues. For example, if your report is very slow to generate, you can use this log to check system performance and see which charts take the longest time to generate.

For information on how to interpret the report diagnostic log and troubleshoot report performance issues, see the *FortiAnalyzer Report Performance Troubleshooting Guide*.

To retrieve report generation logs:

1. In *Reports* > *Generated Report*, right-click the report and select *Retrieve Diagnostic* to download the log to your computer.
2. Use a text editor to open the log.

Auto-Generated Reports

The *Cyber Threat Assessment* report is automatically generated. By default, the report will run at 3:00AM every Monday. For more information on report scheduling, see Scheduling reports on page 276.

Schedules can be viewed in the *Report Calendar*. See Report calendar on page 312.

This will only affect newly installed FortiAnalyzer or newly created ADOM. Upgraded ADOM reports, scheduling and calendar will be kept as is.

Scheduling reports 1-7

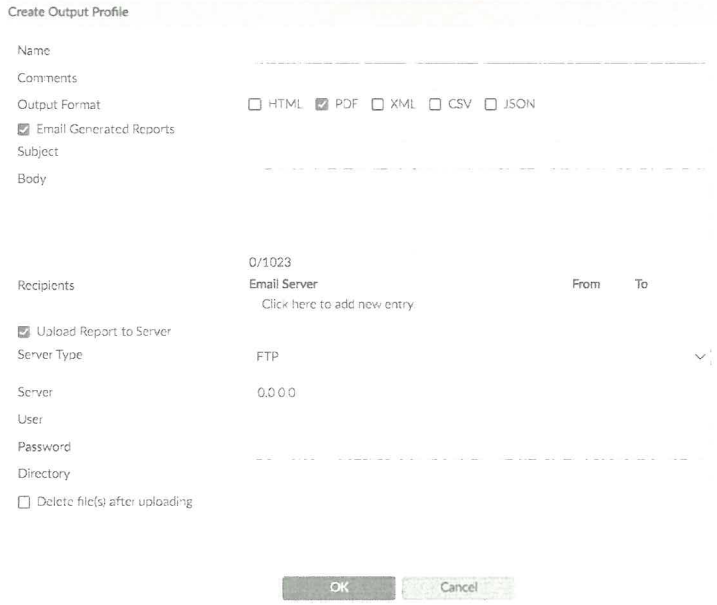
You can configure a report to generate on a regular schedule. Schedules can be viewed in the *Report Calendar*. See Report calendar on page 312.

To schedule a report:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Select a report and click *Edit* in the toolbar.
3. Click *Settings* in the toolbar.
4. Select the *Enable Schedule* checkbox and configure the schedule.
5. Click *Apply*.

To create output profiles:

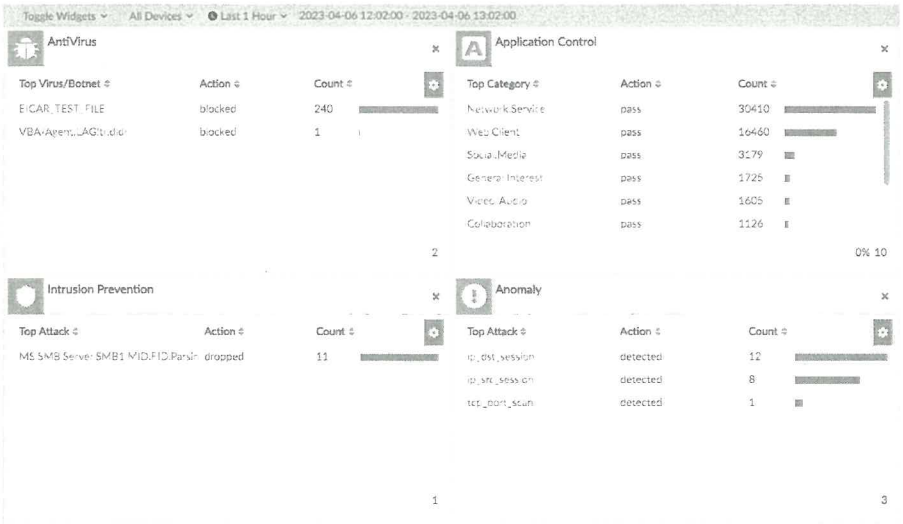
1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Reports* > *Advanced Settings* > *Output Profile*.
3. Click *Create New*. The *Create Output Profile* pane is displayed.



4. Provide the following information, and click *OK*:

Name	Enter a name for the new output profile.
Comments	Enter a comment about the output profile (optional).
Output Format	Select the format or formats for the generated report. You can choose *HTML*, *PDF*, *XML*, *CSV*, or *JSON* format.
Email Generated Reports	Enable emailing of generated reports.
Subject	Enter a subject for the report email.
Body	Enter body text for the report email.
Recipients	Select the email server from the dropdown list and enter to and from email addresses. Click *Add* to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading of generated reports to a server.
Server Type	Select *FTP*, *SFTP*, or *SCP* from the dropdown list.
Server	Enter the server IP address.
User	Enter the username.
Password	Enter the password.
Directory	Specify the directory where the report will be saved.

Security: Summary dashboard:



Event: Summary dashboard:

The summary dashboard for event logs includes a *Total Events* widget, which displays a line chart of the event logs by level. You can hover your cursor over the line chart to display a summary of the count and time at that point. This widget cannot be toggled off.

Viewing historical and real-time logs 1-8

By default, *Log View* displays historical logs. *Custom View* and *Chart Builder* are only available in historical log view.

To view real-time logs, in the log message list view toolbar, click *Tools* > *Real-time Log*.

To switch back to historical log view, click *Tools* > *Historical Log*.

FortiView dashboards for FortiGate and FortiCarrier devices

Category	View	Description
Threats	Top Threats	Lists the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus.
	Threat Map	Displays a map of the world that shows the top traffic destinations starting at the country of origin. Threats are displayed when the threat score is greater than zero and either the source or destination IP is a public IP address. The *Threat Window* below the map, shows the threat, source, destination, severity, and time. The color gradient of the lines indicate the traffic risk. A yellow line indicates a high risk and a red line indicates a critical risk. This view can be filtered by device, time, source, and destination. See also Viewing the threat map on page 90.
	Indicator of Compromise	Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats. To use this feature: 1. UTM logs of the connected FortiGate devices must be enabled. 2. The FortiAnalyzer must subscribe to FortiGuard to keep its threat database up-to-date.
	FortiSandbox Detection	Displays a summary of FortiSandbox related detections. The following information is displayed: Filename, End User and/or IP, Destination IP, Analysis (Clean, Suspicious or Malicious rating), Action (Passthrough, Blocked, etc.), and Service (HTTP, FTP, SMTP, etc.). Select an entry to view additional information in the drilldown menu. Clicking a FortiSandbox action listed in the *Process Flow* displays details about that action, including the *Overview*, *Indicators*, *Behavior Chronology Chart*, *Tree View*, and more. Information included in the *Details* and *Tree View* tab is only available with FortiSandbox 3.1.0 and above.

1-8

Category	View	Description
VPN	SSL & Dialup IPsec	Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec). You can view VPN traffic for a specific user from the top view and drilldown views. In the top view, double-click a user to view the VPN traffic for the specific user. In the drilldown view, click an entry from the table to display the traffic logs that match the VPN user and the destination.
	Site-to-Site IPsec	Displays the names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network.
System	Admin Logins	Displays the users who logged into the managed device.
	System Events	Displays events on the managed device.
	Resource Usage	Displays device CPU, memory, logging, and other performance information for the managed device. Resource Usage includes two widgets: *Resource Usage Average* and *Resource Usage Peak*.
	Failed Authentication Attempts	Displays the IP addresses of the users who failed to log into the managed device.

Using FortiView

When ADOMs are enabled, *FortiView* displays information for each ADOM. Please ensure you are in the correct ADOM. See Switching between ADOMs on page 31.

Viewing FortiView dashboards

When viewing FortiView dashboards, use the controls in the toolbar to select a device, specify a time period, refresh the view, and switch to full-screen mode.

Many widgets on FortiView dashboards let you drill down to view more details. To drill down to view more details, click, double-click, or right-click an element to view details about different dimensions in different tabs. You can continue to drill down by double-clicking an entry. Click the close icon in the widget's toolbar to return to the previous view.

	You can specify a refresh interval of *Every 10 Seconds*, *Every 30 Seconds*, *Every 1 Minute*, or *Every 5 Minutes*.
Export to CSV	Download the events to a CSV file.
Column Settings	Select which columns are displayed in the *All Events* pane. Columns not displayed by default include *Acknowledged*, *Acknowledged By*, *Acknowledged Time*, *Assigned To*, *Comment*, *Commented By*, *Commented Time*, *Device ID*, *Device Type*, *Event ID*, *Group By*, *Group By 2*, *Group By 3*, *Indicators*, *Last Occurence*, and *VDOM Name*.

Default event views

1-9

FortiAnalyzer event handlers apply one or more tags to events, allowing the events to be grouped into views in the *Event Monitor*. These views are visible in the navigation.

Default views are organized into three view categories under *Incidents & Events* > *Event Monitor*:

- *By Endpoint*: Provides security event views from an endpoint perspective.
- *By Threat*: Provides security event views from a threat perspective.
- *System Events*: Provides event views which cover device system events.

In order for events to be displayed in default views, the corresponding event handler(s) must be enabled. Refer to the chart below for a list of the predefined event handlers that must be enabled to support each default view:

View category	Default view	Required predefined event handler
By Endpoint	All Security Events	Displays all events within category with enabled handlers
	Compromised Hosts	Default-Botnet-Communication-Detection-By-Endpoint Default-Compromised Host-Detection-IOC-By-Endpoint
	Sandbox Detections	Default-Sandbox-Detections-By-Endpoint
	Malware Activity	Default-Sandbox-Detections-By-Endpoint Default-Malicious-File-Detection-By-Endpoint
	Ongoing Intrusions	Default-Malicious-Code-Detection-By-Endpoint
	Malicious Domain/URL Access	Default-Risky-Destination-Detection-By-Endpoint
	High Risk App Usage	Default-Risky-App-Detection-By-Endpoint

Creating notification profiles 1-9

Notification profiles are used to send alert notifications when an event is generated by an event handler. You can configure the notification profile to send the alert to an email address, SNMP community, and/or syslog server. You can also configure the notification profile to send the alert through a fabric connector.

You can create, edit, clone, and delete notification profiles in *Incidents & Events* > *Handlers* > *Notification Profiles*.

To assign a notification profile to a basic event handler, see Creating a custom event handler on page 238.

To assign a notification profile to a correlation handler, see Creating a custom correlation handler on page 243.

To create a notification profile:

1. Go to *Incidents & Events* > *Handlers* > *Notification Profiles*.
2. Click *Create New*.
   The *Add New Notification Profile* pane displays.
3. Configure the following options, and click *OK* to save the notification profile.

Option	Description
Name	Enter a name for the notification profile.
Send Alert through Fabric Connectors	Send an alert through one or more fabric connectors selected from the dropdown. Click the plus (+) to add fabric connectors. For more information, see Fabric Connectors on page 173.
Send Alert Email	Send an alert to one or more email addresses. Specify the email parameters, including the mail server. For more information, see Mail Server on page 368.
To	Enter the email address(es) to send the alert to. Use a semicolon (;) to separate multiple email addresses.
From	Enter a from address for the alert email.
Subject	Enter a subject line for the alert email.
Email Server	Select the mail server for the alert email.
Send SNMP(...) Trap	Send an alert to an SNMP community or user selected from the dropdown. For more information, see SNMP on page 321.
Send Alert to Syslog Server	Send an alert to the syslog server selected from the dropdown. For more information, see Syslog Server on page 369.
Send Each Alert Separately	Enable to send each alert individually instead of in a group.

Creating a custom event handler

You can create a custom event handler from scratch or clone a predefined event handler and customize its settings. See Cloning event handlers on page 251.

SD-WAN Performance Status	The SD-WAN performance status comparison with interfaces. Mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check. Click on a scatter chart to view additional details.
SD-WAN Rules Utilization	The SD-WAN rule traffic utilization by interface and application.
SD-WAN Utilization by Application	The share of bandwidth utilization by application for each WAN link.
Top SD-WAN SLA Issues	The top SD-WAN SLA issues. The *Sort By: Speed* option in this widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
SD-WAN Events	This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.
Application Bandwidth Utilization	The total bandwidth from all applications as well as the bandwidth per-SD-WAN interface. This widget can be viewed in a sanky chart or table chart format.
Per-Application Performance	The performance for the selected application based on chosen metric. You can select an application in the widget's *Application* dropdown menu. *Latency*, *Jitter*, *Packet Loss*, and *Bandwidth* metrics are available.
Global-Application Performance	The global application performance for the selected metric. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
SD-WAN Interfaces	The information for SD-WAN interfaces and ADVPN shortcut interfaces. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
Audio MOS Score	The MOS score by interface. Mousing over the chart displays a summary of the MOS score and VoIP quality at that point. The interface must have a performance SLA with MOS enabled to display in the chart.
Speed Test	The upload and download speeds for all tests run on SD-WAN interfaces through a specified time. This widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
Health Check Status	This widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.

1-10

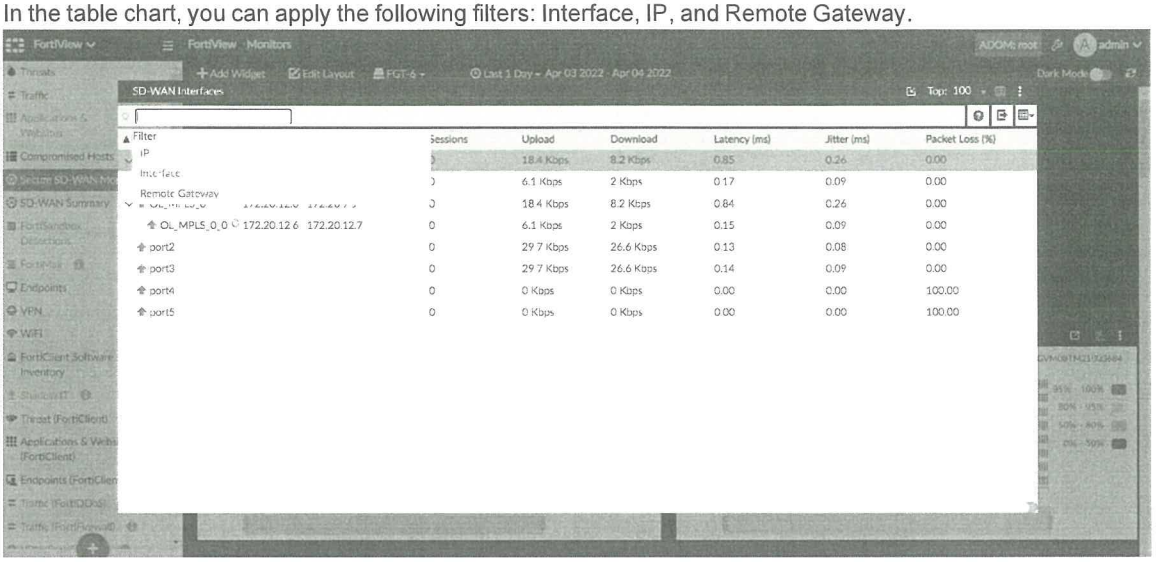
To update the *Refresh Interval*, click the settings icon at the top of the widget, and then select a value from the dropdown.

To filter a chart, click a key in the legend.

SD-WAN Summary

SD-WAN Summary monitor includes the following widgets:

3. In the table chart, you can apply the following filters: Interface, IP, and Remote Gateway.



SD-WAN chart for MOS scoring 1-11

An *Audio MOS Score* widget is added to *FortiView* > *Monitors* > *Secure SD-WAN Monitor* and *FortiView* > *Monitors* > *SD-WAN Summary*. These widgets display logs for the MOS (mean opinion score) of voice and video traffic.

MOS is a method to measure the impact network quality has on the quality of a voice call. It is the industry standard for measuring voice and video quality on a WAN link.

The FortiGate version must be on version 7.2 or later and have the MOS codec and MOS threshold attributes defined for SD-wan health check in order for FortiAnalyzer to display information in the MOS scoring widgets.

To view the Audio MOS Score for individual devices:

1. Go to *FortiView* > *Monitors* > *Secure SD-WAN Monitor*.
2. Click *Add Widget*, and add the *Audio MOS Score* widget.
   The widget includes a line graph of the MOS score for different codecs for the selected device over a specified time period.

Most administrators may need to store between 30 and 60 days in Analytics, however, this should be configured for the amount of time that you would typically need to explore the logs for.

If you need to run analytics for dates outside your Analytics retention, you may perform a database rebuild and load the particular date range. A database rebuild involves purging all logs from Analytics and loading logs for the days of interest from Archive. Once analysis is complete, you can then rebuild once more to load the most current logs into analytics from the archive.

Data policy and automatic deletion

Use a data policy to control how long to keep compressed and indexed logs. When ADOMs are enabled, you can specify settings for each ADOM and the settings apply to all devices in that ADOM. When ADOMs are disabled, settings apply to all managed devices.

A data policy specifies:

- How long to keep Analytics logs indexed in the database
  When the specified length of time in the data policy expires, logs are automatically purged from the database but remain compressed in a log file on the FortiAnalyzer disks.
- How long to keep Archive logs on the FortiAnalyzer disks
  When the specified length of time in the data policy expires, Archive logs are deleted from the FortiAnalyzer disks.

See also Log storage information on page 151.

Disk utilization for Archive and Analytic logs

You can specify how much of the total available FortiAnalyzer disk space to use for log storage. You can specify what ratio of the allotted storage space to use for logs that are indexed in the SQL database and for logs that are stored in a compressed format on the FortiAnalyzer disks. Then you can monitor how quickly device logs are filling up the allotted disk space.

Analytic logs indexed in the SQL database require more disk space than Archive logs (purged from the SQL database but remain compressed on the FortiAnalyzer disks).

An average Analytic log is 600 bytes, and an average Archive log is 80 bytes. By default, after seven days Analytic logs are compressed and are an average of 150 bytes.

Keep this difference in mind when specifying the storage ratio for Analytics and Archive logs.

When ADOMs are enabled, you can specify settings for each ADOM and the settings apply to all devices in that ADOM. When ADOMs are disabled, settings apply to all managed devices. See Log storage information on page 151.

FortiView dashboard

1-12

FortiAnalyzer provides dashboards for Security Operations Center (SOC) administrators. FortiView includes monitors which enhance visualization for real-time activities and historical trends for analysts to effectively monitor network activities and security alerts. See FortiView on page 85.

Deleting a CRL

To delete a CRL or CRLs:

1. Go to *System Settings* > *Certificates*.
2. Select the CRL or CRLs you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

Log Forwarding

1-13

You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server when you use the default forwarding mode in log forwarding. You can also forward logs via an output plugin, connecting to a public cloud service.

The *client* is the FortiAnalyzer unit that forwards logs to another device. The *server* is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs.

In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. See Log storage on page 40 for more information.

To see a graphical view of the log forwarding configuration, and to see details of the devices involved, go to *System Settings* > *Logging Topology*. For more information, see Logging Topology on page 314.

Modes

FortiAnalyzer supports two log forwarding modes: forwarding (default), and aggregation.

Forwarding

Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

This mode can be configured in both the GUI and CLI.

Aggregation

As FortiAnalyzer receives logs from devices, it stores them, and then forwards the collected logs at a specified time every day. To avoid duplication, the client only sends logs that are not already on the server.

FortiAnalyzer supports log forwarding in aggregation mode only between two FortiAnalyzer units. Syslog and CEF servers are not supported.

To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiAnalyzer unit.
   You can also migrate the data to another FortiAnalyzer unit, if you have one. Data migration reduces system down time and the risk of data loss.
3. Install the disks in the FortiAnalyzer unit.
   If your unit supports hot swapping, you can do so while the unit is running. Otherwise the unit must be shut down first. See Unit Operation widget on page 63 for information.
4. Configure the RAID level. See Configuring the RAID level on page 332.
5. If you backed up the log data, restore it.

Administrative Domains (ADOMs)

1-14

Administrative domains (ADOMs) enable administrators to manage only those devices that they are specifically assigned, based on the ADOMs to which they have access. When the ADOM mode is advanced, FortiGate devices with multiple VDOMs can be divided among multiple ADOMs.

Administrator accounts can be tied to one or more ADOMs, or denied access to specific ADOMs. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. Super user administrator accounts, such as the `admin` account, can see and maintain all ADOMs and the devices within them.

Each ADOM specifies how long to store and how much disk space to use for its logs. You can monitor disk utilization for each ADOM and adjust storage settings for logs as needed.

The maximum number of ADOMs you can add depends on the FortiAnalyzer system model. Please refer to the FortiAnalyzer data sheet for more information.

When the maximum number of ADOMs has been reached, you will be unable to create a new ADOM.

When upgrading to FortiAnalyzer 6.2.1 or later, you will continue to have access to any ADOMs exceeding the limit, however, no additional ADOMs can be created, and an alert will be issued in the *Alert Message Console* in *System Settings* > *Dashboard*.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by administrators with the *Super_User* profile. See Administrators on page 384.

The root ADOM and Security Fabric ADOMs are available for visibility into all Fabric devices. See Security Fabric ADOMs on page 195.

Non-FortiGate devices are automatically located in specific ADOMs for their device type. They cannot be moved to other ADOMs, except for FortiClient devices, which can be promoted to Fabric ADOMs if needed.

ADOMs must be enabled to support the logging and reporting of non-FortiGate devices.

To check the IOC package in the CLI:

```
diagnose fmupdate fds-getobject

FAZ object version information
ObjectId                Description             Version         Size    Created Date Time
-------------------------------------------------------------------------------------------
-------
...
00001000TIDB00100       ThreatIntel DB          00000.01052     34 MB   19/04/14 20:10
   ext_desc:ThreatIntel DB
00001000TIDB00100       ThreatIntel DB          00000.01053     37 MB   19/04/16 04:13
<latest> ext_desc:ThreatIntel DB
...
```

FortiAnalyzer periodically syncs its own IOC TIDB files to the version of IOC package downloaded by *fmupdate*. This is performed on a one hour schedule.

To check the license and TIDB version used by FortiAnalyzer in the CLI:

```
diagnose test application sqllogd 204 stats

License of post breach detection installed.
License expiration : 2025-Jan-04
TIDB version : 00000.01017-1902242107
TIDB load time : 2019-02-24 14:11:2
```

Configuring FortiGate to FortiAnalyzer REST API authentication 1-15

FortiGate to FortiAnalyzer REST API authentication allows the FortiAnalyzer to send IOC alerts and trigger configured automation rules, if configured.

To configure REST API authentication:

1. Go to the *Device Manager* in the FortiAnalyzer.
2. Edit the FortiGate device to set the FortiGate super admin username and password.
   This is the only way to configure REST API authentication prior to 6.2.

Alternatively, when configuring logging to FortiAnalyzer on FortiGate, you can go to *Security Fabric* > *Settings* and enable *Allow access to FortiGate REST API* and *Trust FortiAnalyzer by serial number*.

Throttling IOC alerts

To avoid flooding FortiGate with event alerts, you can configure a throttle which allows only one alert to be sent within a set period of time for the same endpoint.
The default time period is one day (1440 minutes).

To set an IOC alert throttle in the CLI:

```
config system log ioc
(ioc)# set
 notification             Disable/Enable Ioc notification.
 notification-throttle    Minute value for throttling the rate of IoC notifications.
```

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

其他附件：(第一次公告) 標號：TMU113-103

附件四

外標封標籤

(※請書寫完整資料並沿實線裁剪並貼於標封封面)

外標封

採購名稱：防火牆日誌紀錄器
截止投標時間：113年11月25日下午05時整

標號：TMU113-103 (第一次公告)
開標時間：113年11月25日下午05時整

11031 臺北市信義區吳興街250號

臺北醫學大學總務處事務組收

事務組採購承辦人：李清萬先生

投標廠商	四海資訊股份有限公司			統一編號	22644575
廠商地址	台中市北屯區陳平路117巷46之3號			廠商電話	02-2797-9331
廠商聯絡人	林高春	聯絡人電話	0919-58-9796	聯絡人E-mail	arthur@chho.com.tw

※注意事項：

一、投標文件遞送請注意時效，寄達本校事務組採購承辦人處，如逾時視為無效標。

二、投標文件應以不透明容器(封套)密封，外標封標籤請書寫完整基本資料後貼於標封封面，如未載明本案採購案名、標號及投標廠商、地址、電話或封口處未密封或信封套為透明者，皆視為無效標。

投標文件送達紀錄	▶廠商請擇一勾選	☐郵寄或快遞送達(免簽章及免填送達時間) ☑專人送達(送件須簽章並註記送達時間) 投標廠商送件人簽章：林高春 送達日期及時間：113.11.25.09:40	本校收件人簽名： 陳婧怡 收件日期及時間：113.11.25.09:40

四海資訊股份有限公司
Whole World Informcition Co., Ltd
總公司：40464台中市北區陝西路33號2F
電　話：(04)-2295-0210　　傳真：(04)-2295-0189
台　北：11473台北市內湖區文德路159號
電　話：(02)-2797-9331　　傳真：(02)-2658-9772

印刷品	
限　時	
掛　號	
平　信	

資、規格封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本資、規格封內請依投標須知規定裝入相關審核文件(請影印為 A4 尺寸)，並以迴紋針固定於左上角，俾利開標審核作業。

投標廠商	四海資訊股份有限公司	統一編號	22644575
廠商地址	台中市北屯區陳平路117巷46之3號	廠商聯絡人	林高春
廠商電話	02-2797-9331	聯絡人電話	0919-58-9796

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **其他附件：(第一次公告)** 標號：TMU113-103

附 件 二

投標廠商資、規格審查表

※請依表列順序排放證件影本並將本表置於首頁

廠商所提資格文件影本，本校得通知廠商限期提出正本供查驗，查驗結果如與正本不符，係偽造或變造者，依採購法第 50 條規定辦理。

採購名稱	防火牆日誌紀錄器	採購案號	1130203887
廠商名稱	威民先科技有限公司	廠商統編	53099614
負責人	陳明朱	廠商印鑑章	
聯絡人	林伯熏 Email: wilson@vltnk.com.tw		
聯絡電話	(市話) 02-86603168 (手機) 0930-275-966		
廠商地址	公司：新北市永和區中山路1段267號3F		

	投標廠商資格審查項目		招標機關資格審查	
資規格項目	☑	1.押標金(119,000 元)繳納憑據 ☐ 依投標須知規定，免檢附	☑符合 ☐不符合	採購單位審查(項目1-8項)： ☑合格 且開標前已至政採網查詢非拒絕往來廠商詳附件 ☐不合格，說明：
	☑	2.廠商登記或設立證明	☑符合 ☐不符合	
	☑	3.廠商最近一期納稅證明	☑符合 ☐不符合	
	☑	4.廠商信用證明	☑符合 ☐不符合	採購單位簽章：李彥蓉
	☑	5.非拒絕往來廠商查詢並列印 (請至工程會網站 web.pcc.gov.tw 查詢列印)	☑符合 ☐不符合	
	☑	6.投標廠商聲明書	☑符合 ☐不符合	
	☑	7.出席代表授權書 ☐ 負責人親自出席，免檢附	☑符合 ☐不符合	
	☑	8.電子領標電子憑據	☑符合 ☐不符合	
	☑	9.廠商製造、供應或承做能力證明	☑符合 ☐不符合	請購單位審查(項目 9-11 項)： ☑合格 ☐不合格，說明：
	☐	10.廠商須具有維修、維護或售後服務能力之證明	☐符合 ☐不符合	
	☑	11.型錄或規格說明書	☑符合 ☐不符合	請購單位簽章：陳曉慶

投標廠商審查結果	投標廠商不符事項確認	投標廠商簽章▼
☑合 格 ☐不合格	本廠商所投標及釋疑補充之文件等，經貴機關審核後，不符招標文件規範經本廠商確認無誤後，謹此簽章認同。	

列印時間：113/11/25 16:39

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為
廠商代碼： 53099614 (威尼克科技有限公司)
廠商現況： 01-核准設立
廠商名稱： 威尼克科技有限公司

資料取得時間：113/11/25 16:39

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

臺北醫學大學暫收款收據

007886

民國 113 年 11 月 21 日

繳款公司	合宏天科技有限公司			電話:093027566
款項名稱	1押標金 2圖說 3	採購案名稱	防火卷門基礎修繕	
收款票據明細	支票號碼	KNB077599	支票日期	113 年 11 月 20 日
	付款銀行	台北富邦 銀行庫	存	分行(部.庫)
收款金額	新臺幣(大寫): ~~仟~~ 佰壹拾壹萬玖仟零佰零拾零元整			
備註	請妥善保管此收據，得標後憑此暫收據換正式收據。			

出納組 113.11.21 許文嘉

經收人:

112.05.01

第一聯：出納組聯（白）第二聯：暫收據（紅）

自領
2

正本

新北市政府　　函

機關地址：22001新北市板橋區中山路1段161號3樓
承辦人：柯佩利（509）
電　話：(02)29603456轉5295
傳　真：(02)29568030
電子郵件：AE8390@ntpc.gov.tw

234
新北市永和區中山路1段267號3樓
受文者：威尼克科技有限公司

發文日期：中華民國105年11月04日
發文字號：新北府經司字第1055322207號
速別：普通件
密等及解密條件：普通
附件：規費收據暨變更登記表1份

裝

主旨：貴公司（統一編號：53099614）申請公司遷址、修正章程變更登記，經核符合規定，准予登記。

說明：

一、依公司法辦理兼復貴公司105年11月4日（收文日）申請書。

二、處分相對人名稱：威尼克科技有限公司（代表人姓名：陳明朱、身分證照號碼：N20181****）、公司所在地：新北市永和區中山路1段267號3樓。

訂

三、公司登記之核准，與土地及建物是否合法使用係屬二事，貴公司實際經營業務之營業場所應符合都計、建管、消防等法令規定，違反者，應受上開法令之處罰。貴公司可向營業場所所在地直轄市、縣（市）政府之都計、建管單位或『營業場所預查服務櫃檯』，填載內政部訂定之『營業場所土地使用分區管制與建築管理規定查詢表』（表格下載：http://www.economic.ntpc.gov.tw/upload/cht/article/營業場所土地使用分區管制與建築管理規定查詢表(9).doc，或向直轄市、縣（市）政府之都計、建管單位、『營業場所預查服務櫃檯』索取），申請查詢實際營業之場所是否符合土地使用分區管制與建築管理之規定。

線

四、檢附規費收據暨變更登記表1份，請查收。

五、如涉及稅籍登記部分，請於開始營業前檢送負責人身分證明文件、公司章程、許可業務之核准文件等影本洽營業所在地稽徵機關辦理；詳細文件請逕洽各地區國稅局。

六、依據「新北市火災預防自治條例」，如實際營業場所為樓地板面積超過3000平方公尺之商場、百貨商場或超級市場，請於營業前辦妥自衛消防編組驗證事項，違反者，將處管理權人新臺幣1萬元以上5萬元以下罰鍰，相關資訊可至本府消防局官網下載，網址：http://www.fire.ntpc.gov.tw/_file/1143/SG/31583/D.html（洽詢專線8951-9119）。

七、原公司地址：110臺北市信義區忠孝東路5段19號3樓之1。

八、對本行政處分如有不服，請依訴願法第14條及第58條規定，自行政處分書到達之次日起30日內，繕具訴願書，向本府遞送（以實際收受訴願書之日期為準，而非投郵日），並將副本抄送經濟部（地址

統一編號：53099614

：臺北市中正區福州街15號）。

九、公司營業項目：C601020紙製造業、C601030紙容器製造業、C601040加工紙製造業、C701010印刷業、C702010製版業、C703010印刷品裝訂及加工業、CB01010機械設備製造業、CB01020事務機器製造業、CC01060有線通信機械器材製造業、CC01070無線通信機械器材製造業、CC01080電子零組件製造業、CC01110電腦及其週邊設備製造業、CC01120資料儲存媒體製造及複製業、F109070文教、樂器、育樂用品批發業、F113010機械批發業、F113030精密儀器批發業、F113050電腦及事務性機器設備批發業、F113070電信器材批發業、F118010資訊軟體批發業、F119010電子材料批發業、F401010國際貿易業、ZZ99999除許可業務外，得經營法令非禁止或限制之業務。

裝

※104年5月20日公布修正公司法第235條，因應員工分紅費用化並使公司法與商業會計法規範一致，爰刪除現行條文第2項至第4項有關員工分配紅利規定，並增訂公司法第235條之1「公司應於章程訂明以當年度獲利狀況之定額或比率，分派員工酬勞。但公司尚有累積虧損時，應予彌補。」，倘貴公司章程尚未符合上開修正後公司法第235條之1規定，貴公司應儘速依上開規定修正章程，至遲應於105年6月底前依新法完成章程之修正。(章程範例請參考：http://gcis.nat.gov.tw/main/subclassNewAction.do?method=getFile&pk=413)

訂

※有關全民健康保險部分，請檢送相關表件自行向衛生福利部中央健康保險署各分區業務組，辦理有關投保單位變更事宜，相關規定請至該署全球資訊網(http://www.nhi.gov.tw)參閱。

※提醒貴公司，「商業會計法」與「商業會計處理準則」已於103年修正，並自105年1月1日施行。

※經濟部於104年10月30日新建置「工作規則線上填報自動檢核系統」，凡雇用勞工30人以上之企業首次申報工作規則，歡迎多加利用該系統進行線上申報，網址為：https://onestop.nat.gov.tw/oss/ossWeb/WorkRuleOnline/workRuleOnline.do。

線

正本：威尼克科技有限公司

副本：財政部臺北國稅局信義分局、財政部北區國稅局中和稽徵所

市長 朱立倫

本案依分層負責規定授權業務主管決行

裝

訂

線

第二聯：收執聯

營業人銷售額與稅額申報書(401)

（一般稅額計算----專營應稅營業人使用）

所屬年月份：113 年 09 － 10 月

金額單位:新臺幣元

註記欄	核准按月申報	
	核准合併總繳單位	總機構彙總報繳
		各單位分別申報

統一編號	53099614
營業人名稱	威尼克科技有限公司
稅籍編號	351911714
負責人姓名	陳明朱
營業地址	新北市永和區中山路1段267號3樓
使用發票份數	67 份

銷項

區分 / 項目	應稅 銷售額		應稅 稅額		零稅率銷售額
三聯式發票、電子計算機發票	1	4,190,360	2	209,519	3（非經海關出口應附證明文件者）
收銀機發票(三聯式)及電子發票	5	0	6	0	7 0
二聯式發票、收銀機發票(二聯式)	9	0	10	0	11（經海關出口免附證明文件者）
免用發票	13	0	14	0	15 0
減：退回及折讓	17	0	18	0	19 0
合計	21 (1)	4,190,360	22 (2)	209,519	23 (3) 0
銷售額總計 (1)+(3)	25 (7)	4,190,360 元	（內含銷售固定資產	27	0 元）

稅額計算

代號	項目		稅額
1.	本期(月)銷項稅額合計	(2) 101	209,519
7.	得扣抵進項稅額合計	(9)-(10) 107	37,994
8.	上期(月)累積留抵稅額	108	0
10.	小計(7+8)	110	37,994
11.	本期(月)應實繳稅額(1-10)	111	171,525
12.	本期(月)申報留抵稅額(10-1)	112	0
13.	得退稅限額合計	(3)x5%+(10)113	0
14.	本期(月)應退稅額(如 12>13 13>12 則為 13 12)	114	0
15.	本期(月)累積留抵稅額(12-14)	115	0

進項

區分 / 項目		得扣抵進項稅額 金額		稅額
統一發票扣抵聯（包括一般稅額計算之電子計算機發票扣抵聯）	進貨及費用	28	750,794	29 37,542
	固定資產	30	0	31 0
三聯式收銀機發票扣抵聯及一般稅額計算之電子發票	進貨及費用	32	9,045	33 452
	固定資產	34	0	35 0
載有稅額之其他憑證（包括二聯式收銀機發票）	進貨及費用	36	0	37 0
	固定資產	38	0	39 0
海關代徵營業稅繳納證扣抵聯	進貨及費用	78	0	79 0
	固定資產	80	0	81 0
減：退出、折讓及海關退還溢繳稅款	進貨及費用	10	0	11 0
	固定資產	12	0	13 0
合計	進貨及費用	14	759,839	15 (9) 37,994
	固定資產	16	0	17 (10) 0
進項總金額（包括不得扣抵憑證及普通收據）	進貨及費用	18		759,839 元
	固定資產	19		0 元

進口免稅貨物	73	0 元
購買國外勞務	74	0 元

保稅區營業人按進口報關程序銷售貨物至我國境內課稅區之免開立統一發票銷售額 元 0 82.

收件編號：F53099614113100E665
申報日期：113年11月13日
申報次數：001 次
進銷項筆數：82 筆
法院拍賣進項資料筆數：0 筆
零稅率銷售額筆數：0 筆
營業人申報固定資產退稅清單筆數：0 筆
營業人購買舊乘人小汽車及機車進項憑證明細筆數：0 筆
已納稅額：0 元
最後異動日期：113年11月13日 10:55:53
製表日期：113年11月14日

財政部 北區國稅局 113.11.13 營業稅網路申報收件章

申辦情形	姓名	身分證統一編號	電話	登錄文(字)號
自行申報				
委任申報	施美珍		02-29266691	(95)台財稅證字第0*號

說明

一、本申報書適用專營應稅及零稅率之營業人填報。
二、如營業人申報當期（月）之銷售額包括有免稅、特種稅額計算銷售額者，請改用（403）申報書申報。
三、營業人如有依財政部108年11月15日台財稅字第10804629000號令規定進行一次性移轉訂價調整申報營業稅，除跨境受控交易為進口貨物外，請另填報『營業稅一次性移轉訂價調整聲明書』並檢附相關證明文件，併同會計年度最後一期營業稅申報。
四、納稅者如有依納稅者權利保護法第7條第8項但書規定，為重要事項陳述者，請另填報「營業稅聲明事項表」並檢附相關證明文件。

查詢序號：20241119021092000001

第一類票據信用資料查覆單

茲將下列戶號(帳號)票據信用資料查覆如下，請查照

查詢日：113年11月19日　　查覆資料截止日：113年11月13日

戶名：威尼克科技有限公司　　戶號：0053099614

開戶行代號：000000000　　負責人戶號：N201811734

帳號：000000000

查覆結果

一、退票與清償註記總數資訊(未清償註記提供最近三年內之退票未辦理清償註記者；已清償註記提供最近六個月內已辦理退票清償註記者)

退票理由	已清償註記		未清償註記	
	張數	金額	張數	金額
1. 存款不足	0	0	0	0
2. 發票人簽章不符	0	0	0	0
3. 擅自指定金融業者為本票之擔當付款人	0	0	0	0
4. 本票提示期限經過前撤銷付款委託	0	0	0	0

二、拒絕往來資訊

無拒絕往來紀錄。

三、經通報終止為其本票擔當付款人資訊

未經通報終止為其本票擔當付款人。

四、開戶總數資訊

已在台灣地區全體金融業者開立支票存款戶共 001 戶。

五、其他重大資訊

無。

六、關係戶資訊

無。

說明：

(1) 查覆單列印之戶號後有 (*) 註記者，係指該戶號經電腦驗算為不合邏輯之資料。

(2) 查覆單列印之負責人戶號欄位空白者，係指該查詢申請單所填載之負責人，並非本所檔案中所建立該被查詢公司之負責人，如需所填載負責人票信資料者，請以負責人個人名義申請辦理。但查詢者提供被查詢公司之負責人相關資料，並經查證正確更改本所檔案資料後，該欄位即列印查詢申請單所填載之負責人身分證統一編號。

(3) 因建檔及註記作業時差， 本查覆單「查覆結果」欄之資料，其中第一、六兩項資訊，除有關清償註記資訊提供至查詢日之前一營業日外，其餘提供至資料截止日，另肆項資訊提供至查詢日。

(4) 不具法人人格之行號、 團體，應以其負責人個人名義申請票據信用資料查詢。

(5) 本查覆單「查覆結果」欄之資料，第六項關係戶資訊如有戶名及戶號時，其詳細票信資料請另向本所查詢。

(6) 本查覆單不得為竄改、複製、發布或其他不當使用。

(7) 本查覆單以由票據交換所或受理查詢金融機構出具， 始可作為證明之文件。

資料來源： 台灣票據交換所

單位章

臺北區銀行業票據交換所 (2) 113. 11. 19 (2) 保生分行

列印時間：113/11/14 16:38

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為

廠商代碼： 威尼克科技有限公司

廠商名稱： 威尼克科技有限公司

資料取得時間：113/11/14 16:38

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

附 件 一

投標廠商聲明書

本廠商參加(臺北醫學大學)招標採購防火牆日誌紀錄器案之投標，茲聲明如下：

項次	聲明事項	是(打V)	否(打V)
一	本廠商之營業項目不符合公司法或商業登記法規定，無法於得標後作為簽約廠商，合法履行契約。		V
二	本廠商有違反政府採購法(以下簡稱採購法)施行細則第 33 條之情形。		V
三	本廠商是採購法第 38 條規定之政黨或與政黨具關係企業關係之廠商。		V
四	本廠商之負責人或合夥人是採購法第 39 條第 2 項所稱同時為規劃、設計、施工或供應廠商之負責人或合夥人。		V
五	本廠商是採購法第 39 條第 3 項所稱與規劃、設計、施工或供應廠商同時為關係企業或同一其他廠商之關係企業。		V
六	本廠商已有或將有採購法第 59 條第 1 項所稱支付他人佣金、比例金、仲介費、後謝金或其他不正利益為條件，促成採購契約之成立之情形。		V
七	本廠商、共同投標廠商或分包廠商是採購法第 103 條第 1 項、採購法施行細則第 38 條第 1 項、人口販運防制法第 41 條所規定之不得參加投標或作為決標對象或分包廠商之廠商。【投標廠商應於投標當日遞送投標文件前至工程會網站 web.pcc.gov.tw 查詢自己(包括總公司及各分公司)、共同投標廠商、分包廠商是否為採購法第 103 條第 1 項之拒絕往來廠商】		V
八	本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人。		V
九	本廠商是依法辦理公司或商業登記且合於中小企業發展條例關於中小企業認定標準之中小企業。(依該認定標準第 2 條，所稱中小企業，指依法辦理公司登記或商業登記，實收資本額在新臺幣 1 億元以下，或經常僱用員工數未滿 200 人之事業。) (答「否」者，請於下列空格填寫得標後預計分包予中小企業之項目及金額，可自備附件填寫) 項目＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 項目＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 合計金額＿＿＿＿＿＿＿＿	V	
十	本廠商目前在中華民國境內員工總人數逾 100 人。(依採購法第 98 條及其施行細則第 107 條、108 條規定，得標廠商其於國內員工總人數逾 100 人者，應於履約期間僱用身心障礙者及原住民各不低於總人數百分之一，僱用不足者，除應繳納代金，並不得僱用外籍勞工取代僱用不足額部分。) (答「是」者，請填目前總人數計＿＿人；其中屬於身心障礙人士計＿＿人，原住民計　　人。)		V
十一	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或經濟部投資審議委員會公告之陸資資訊服務業者，不得從事經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」。【上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議委員會網站http://www.moeaic.gov.tw/】【請查察招標文件規定本採購是否屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購】		V
十二	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或在臺陸資廠商，不得從事影響國家安全之採購。【請查察招標文件規定本採購是否屬影響國家安全之採購】		V

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 投標廠商聲明書：(第一次公告) 標號：TMU113-103

十三	本廠商是原住民個人或政府立案之原住民團體。 (答「否」者，請於下列空格填寫得標後預計分包予原住民個人或政府立案之原住民團體之項目及金額，可自備附件填寫。如無，得填寫「0」) 項目＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ 金額 0 項目＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ 金額 0 合計金額 0		

附註	1. 第一項至第七項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象。 2. 本採購如非屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，第八項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象【違反公職人員利益衝突迴避法第 14 條第 1 項規定者，依同法第 18 條第 1 項處罰】。如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，答「是」、「否」或未答者，均可。 3. 第九項、第十項、第十三項未填者，機關得洽廠商澄清。 4. 本採購如屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，第十一項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 5. 本採購如屬影響國家安全之採購，第十二項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 6. 本聲明書填妥後附於投標文件遞送。 7. 本採購如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，且本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人者，請填「公職人員利益衝突迴避法第 14 條第 2 項公職人員及關係人身分關係揭露表」，如未揭露者依公職人員利益衝突迴避法第 18 條第 3 項處罰。
	投標廠商名稱： 威尼克科技有限公司
	投標廠商章及負責人章： 陳明生 **日期：** 113.11.21

(引用行政院公共工程委員會 113.1.1 版)

附 件 三

出席代表授權書

茲授權本公司(商號或法人) 所屬員工：林伯熏 先生/小姐代表本公司(商號或法人)出席貴校「**防火牆日誌紀錄器**」之開標/評選/議價會議，該員在開標/評選/議價會議中所做之任何承諾或簽認事項直接對本公司(商號或法人)發生效力，本公司(商號或法人)均予以承受，並經本公司(商號或法人)確認被授權人之下列簽樣真實無誤。

被授權人之簽樣[*註]：　　或

請惠予核備。

此　　致

臺北醫學大學

授權人公司(商號)：威尼克科技有限公司

負責人姓名：陳明朱

公司(商號)統一編號：53099614

負責人身分證統一編號：N120811734

被 授 權 人：林伯熏

身分證統一編號：A121901423

通訊地址：新北市永和區中山路1段269號3F

聯絡電話：0930-275-766

中　華　民　國　113　年　11　月　21　日

---

*註：『被授權人簽樣』得為下列形式之1，依民法第103條規定，代理人於代理權限內所為之意思表示，直接對投標廠商發生效力：1.公司大小章。2.投標專用章。3.被授權人簽章。

電子憑據資料		
	機關代碼	03724606
	機關名稱	臺北醫學大學
	標案案號	TMU113-103
	公告序號	01
	標案名稱	防火牆日誌紀錄器
	領標電子憑證序號	915000000000002330708
	使用者IP	101.10.62.107

力麗科技
LeaLea Technology

經銷授權證明書

茲證明威尼克科技有限公司為 **Fortinet, Inc.**台灣地區之授權經銷商，可銷售 Fortinet 系列設備並履行產品之技術及保固責任。

案　　名：防火牆日誌記錄器

案　　號：TMU113-103

設備名稱：FAZ-810G*2

此致

臺北醫學大學

立證明書人：

力麗科技股份有限公司

本證明書僅限本採購案專用，若移作其他用途或證明及影本;非經本公司事先書面之認可,本公司一律概不承認。

中　華　民　國　一　一　三　年　十　一　月　十　五　日

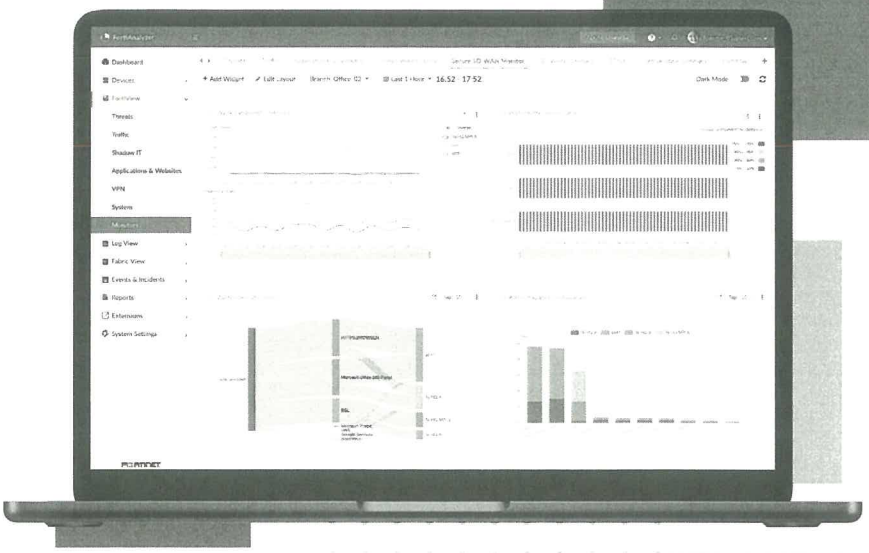
防火牆日誌紀錄器

項次	規格	佐證
	防火牆日誌紀錄器 : FAZ-810G	
1.	獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。	page 3
2.	系統日誌接收效能可達 6,000 logs/sec (含)以上。	page 2
3.	系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。	page 2
4.	系統儲存容量可達 16 TB (含)以上，支援磁碟陣列 RAID 0/1,1s/5,5s/10 規範。	page 2
5.	具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。	page 1 page 7
6.	具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。	page 4
7.	具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。	page 5 page 6
8.	具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。	page 7 page 8 page 9
9.	具備事件監看與告警功能，可從日誌中擷取	page 10

項次	規格	佐證
	過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。	
10.	具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。	page 11
11.	具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。	page 12 page 13
12.	具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。	page 14
13.	具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服器或 Common Event Format (CEF) 伺服器，以利與既有日誌系統整合。	page 15
14.	具備管理區域 (Administrative Domain) 分割功能，並可針對不同管理人員賦予不同的管理權限。	page 16
15.	具備 REST API，以利與既有資安環境整合。	page 17

FortiAnalyzer™

Security Fabric Network Analytics



Highlights

- Centralized network monitoring and visibility
- Advanced threat and vulnerability detection with event and log data correlation
- Augmented NOC/SOC operations for real-time response, analytics, and reporting
- Automation to save time, reduce errors, and improve efficiency
- Multi-tenancy solution with quota management
- Administrative domains for operational effectiveness and compliance
- 70+ reports and 2000+ ready-to-use datasets, charts, and macros

1–5

Analytics, Reports, and Compliance Across the Security Fabric

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

Specifications




FORTIANALYZER APPLIANCES	FAZ-150G	FAZ-300G	FAZ-800G	FAZ-810G
Capacity and Performance				
GB/ day of Logs	25	100	200	200
Analytic Sustained Rate (logs/ sec)*	500	2000	4000	4000
Collector Sustained Rate (logs/ sec)*	750	3000	6000	6000 1–2
Devices/VDOMs (Maximum)	50	180	800	800
Max Number of Days Analytics**	90	50	50	50
Options				
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓	✓
Security Automation Service	✓	✓	✓	✓
Enterprise Bundle	✓	✓	✓	✓
Hardware Bundle	✓	✓	✓	✓
OT Security Service	✓	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓	✓
Hardware Specifications				
Form Factor (supports EIA/non-EIA standards)	Desktop	1 RU Rackmount	1 RU Rackmount	1 RU Rackmount 1–3
Total Interfaces	2 x RJ45 GE	4 x RJ45 GE	4 x RJ45 GE, 2 x SFP	4x RJ-45 2x GE SFP
Storage Capacity	4TB (2× 2TB)	8 TB (2 × 4 TB)	16 TB (4 × 4 TB) 1–4	16TB (4× 4TB) 3.5 in SAS HDDs
Usable Storage (After RAID)	2 TB	4 TB	8 TB	8 TB
Removable Hard Drives	No	No	✓	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10	RAID 0/1,1s/5,5s/10 1–4
RAID Type	Software	Software	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	1	1	10	10
Redundant Hot Swap Power Supplies	No	Optional	Optional	Optional
Trusted Platform Module (TPM) ***	Gen 2	Gen 2	✓	✓
Dimensions				
Height x Width x Length (inches)	9.5 × 3.5 × 8	1.73 × 17.24 × 16.38	1.73 × 17.32 × 21.65	1.73 × 17.32 × 21.65
Height x Width x Length (cm)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	4.4 × 44.0 × 55.0	4.4 × 44.0 × 55.0
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	25.75 lbs (11.68 kg)	25.75 lbs (11.68 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100–240V AC, 50–60 Hz	100-240Vac, 50~60Hz, 4A max
Power Consumption (Average / Maximum)	36 W / 43 W	90.1 W / 99 W	134 W / 174.2 W	115W / 150W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	594.4 BTU/h	433 BTU/h
Operating Temperature	32°–104° F (0°–40° C)	32°–104° F (0°–40° C)	32°–104° F (0°–40° C)	32°–104° F (0°–40° C)
Storage Temperature	-4°–167° F (-20°–75° C)	-13°–167° F (-25°–75° C)	-4°–167° F (-20°–75° C)	-4°–167° F (-20°–75° C)
Humidity	5% to 95% non-condensing	20% to 90% non-condensing	5% to 95% non-condensing	5% to 95% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)
Compliance				
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

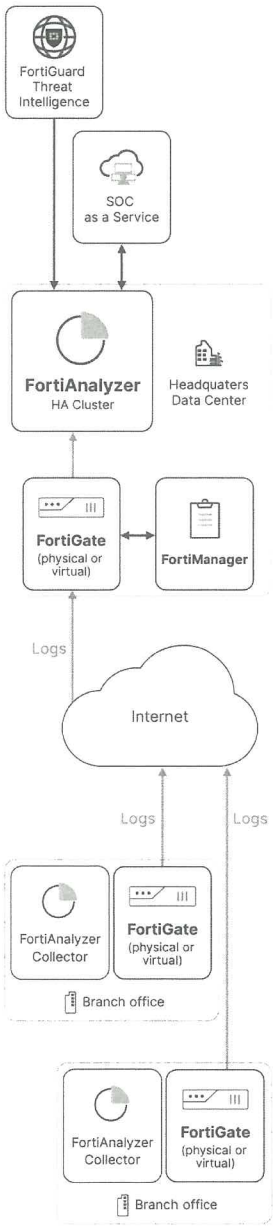
Capabilities

Deployments

1 –1

Deploying FortiAnalyzer

FortiAnalyzer can be deployed as a physical hardware appliance, virtual machine (VM) and virtual machine subscription (VM-S), as well as private or public cloud instance, with scalability, redundancy and backup, and high availability capabilities.



FortiAnalyzer High Availability (HA)

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

Multi-Tenancy with Flexible Quota Management

FortiAnalyzer provides the ability to manage multiple sub-accounts with each account having its own administrators and users. The time-based archive/analytic log data policy, per Administrative Domain (ADOM), allows automated quota management based on the defined policy, with trending graphs to guide policy configuration and usage monitoring.

Analyzer Collector Modes

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

FortiAnalyzer Fabric

FortiAnalyzer Fabric allows SOC Administrators to configure two operation modes - Supervisor and Member. This allows viewing of member devices, ADOMs and authorized logging devices, as well as incidents and events created on members. Admins get access to Reports and FortiView across all member FortiAnalyzers, and can perform global search in Log View of logs collected across FortiAnalyzer Fabric members with pre-defined device filters and log drill down for each Member and Member ADOMs and support for .

Log Forwarding for Third-Party Integration

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

	SHA256
fips enabled	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:AES256-SHA:AES256-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES256-GCM-SHA384:AES128-SHA:AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES128-GCM-SHA256

The following ciphers are *not available* when using forward secrecy (`ssl-static-key-ciphers` is disabled).

ssl-static-key-ciphers disabled

enc-algorithm

Low	AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:AES256-SHA:CAMELLIA256-SHA:AES128-GCM-SHA256:AES128-CCM:AES128-SHA256:CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:AES256-CCM8:AES128-CCM8
Medium	AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:AES256-SHA:CAMELLIA256-SHA:AES128-GCM-SHA256:AES128-CCM:AES128-SHA256:CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:AES256-CCM8:AES128-CCM8
High	AES256-GCM-SHA384:AES256-CCM:ARIA256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA256:AES256-SHA:CAMELLIA256-SHA:AES128-GCM-SHA256:AES128-CCM:AES128-SHA256:CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA
fips enabled	AES256-SHA:AES256-SHA256:AES128-SHA:AES128-SHA256

1–6

Maximum TLS/SSL version compatibility

The tables below indicate the maximum supported TLS version that you can configure for communication between a FortiGate and FortiAnalyzer, as well as FortiAnalyzer's configured with log forwarding when the type is *FortiAnalyzer*.

For more information on secure log transfer and log integrity settings between FortiGate and FortiAnalyzer, see Appendix B - Log Integrity and Secure Log Transfer on page 471.

Maximum configurable TLS version for FortiGate to FortiAnalyzer communication:

	FAZ 6.4.0+	FAZ 6.2.0+	FAZ 6.0.0+
FGT 6.4.0+	tlsv1.3	tlsv1.2	tlsv1.2
FGT 6.2.3 – 6.2.8	tlsv1.3	tlsv1.2	tlsv1.2

How auto-cache works

When you generate a report, it can take days to assemble the required dataset and produce the report, depending on the required datasets. Instead of assembling datasets at the time of report generation, you can enable the *auto-cache* feature for the report. *Auto-cache* is a setting that tells the system to automatically generate *hcache*.

hcache is a proprietary FortiAnalyzer caching system that stays on the disk in the form of a database table. Unlike other caches, *hcache* tables are persistent and are not removed based on a set period of time.

When a database table is rolled, it becomes "mature", meaning the table will not grow any more. Because the tables will not grow, it is unnecessary to query the database table each time for the same SQL query. *hcache* runs queries on these matured database tables in advance and caches the interim results of each query. When it is time to generate the report, much of the datasets are already assembled, and the system only needs to merge the results from *hcaches*. This reduces report generation time significantly.

The *auto-cache* process uses system resources to assemble and cache the datasets and it takes extra space to save the query results. You should only enable *auto-cache* for reports that require a long time to assemble datasets.

1–7

Generating reports

You can generate reports by using one of the predefined reports or by using a custom report that you created. You can find all the predefined reports and custom reports listed in *Reports* > *Report Definitions* > *All Reports*.

Click the icon in the *Config Recommendation* column to determine if the appropriate Analytics logs are available for the report. For more information, see Report guidance on page 300.

To generate a report:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. In the content pane, select a report from the list.
3. (Optional) Click *Edit* in the toolbar and edit settings on the *Settings* and *Layout* tabs. For a description of the fields in the *Settings* and *Layout* tabs, see Reports Settings tab on page 306 and Creating charts on page 324 and Macro library on page 327.
4. In the toolbar, click *Run Report*.

Generated reports can be attached to incidents. See Adding reports to an incident on page 186.

Report guidance

You can use the *Report Guidance* feature to determine if FortiAnalyzer has the appropriate Analytics logs available for a report.

If Analytics logs are not available for a chart or macro used in the report, it will display `No Data` in the report output. For example, the Analytics logs may not be available if;

- logging is not enabled correctly on the device,
- the log requires a FortiGuard license and you do not have one,

Viewing imported event handlers and reports

1–7 With a valid license, the FortiAnalyzer Outbreak Detection Service automatically downloads event handlers and reports created by Fortinet in response to known outbreaks. Handlers and reports are downloaded from FortiGuard as part of the FOAS package. This section includes information on how to view downloaded outbreak event handlers and reports.

To view outbreak event handlers and reports:

1. To view the event handlers, go to *Incidents & Events* > *Handlers* > *Basic Handlers*.
   Event handlers created by the FortiAnalyzer Outbreak Detection Service are displayed with the Outbreak Alert prefix. See Event handlers on page 197.

   In FortiAnalyzer 7.6.0 and later, these event handlers will also have the *Automatically Create Incident* option enabled. The incidents generated by these event handlers can be found in *Incidents & Events* > *Incidents* > *Incidents*.

2. To view the reports, go to *Reports* > *Report Definitions* > *All Reports*.

1–7
- The *Outbreak Alert Reports* folder includes available reports from the FortiAnalyzer Outbreak Detection Service. Reports can be run in HTML, PDF, XML, CSV, and JSON output formats. See Generating reports on page 300.
- In FortiAnalyzer 7.4.2 and later, new reports included in the FOAS package are displayed in the global *Outbreak Alert Reports* folder. Outbreak Alert reports released prior to this release remain at the ADOM level. The global folder and global reports are identified with the system theme's color applied to the icon.

Log View and Log Quota Management

You can view log information by device or by log group.

When rebuilding the SQL database, *Log View* is not available until the rebuild is complete. Click the *Show Progress* link in the message to view the status of the SQL rebuild.

1–8

When ADOMs are enabled, each ADOM has its own information displayed in *Log View*.

Log View > *Logs* > *All / Fortinet Logs* can display the real-time log or historical (Analytics) logs.

Log View > *Logs* > *Log Browse* can display logs from both the current, active log file and any compressed log files.

For more information, see Analytics and Archive logs on page 42.

Types of logs collected for each device

1–5

FortiAnalyzer can collect logs from the following device types: FortiADC, FortiAnalyzer, FortiAuthenticator, FortiCache, FortiCarrier, FortiCASB, FortiClient, FortiDDoS, FortiDeceptor, FortiEDR, FortiGate, FortiIsolator, FortiMail, FortiManager, FortiNAC, FortiNDR, FortiPAM, FortiProxy, FortiSandbox, FortiSOAR, FortiWeb, and Syslog servers. Following is a description of the types of logs FortiAnalyzer collects from each type of device:

Device Type	Log Type
Fabric	Normalized
FortiADC	Event, Intrusion Prevention, Traffic
FortiAnalyzer	Event, Application 1–8
FortiAuthenticator	Event
FortiGate	Traffic Security: Antivirus, Intrusion Prevention, Application Control, Web Filter, File Filter, DNS, Data Loss Prevention, Email Filter, Web Application Firewall, Vulnerability Scan, VoIP, FortiClient Event: Endpoint, HA, Compliance, System, Router, VPN, User, WAN Opt. & Cache, WiFi
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiCarrier	Traffic, Event, GTP

File Filter logs are sent when the File Filter sensor is enabled in the FortiOS Web Filter profile. You can enable the File Filter sensor in FortiOS at *Security Profiles* > *Web Filters*.

Category	View	Description
Traffic	Top Sources	Displays the highest network traffic by source IP address and interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Source Addresses 1–8	Displays the top source addresses by source object, interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Destinations	Displays the highest network traffic by destination IP addresses, the applications used to access the destination, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Destination Addresses	Displays the top destination addresses by destination objects, applications, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Country/Region	Displays the highest network traffic by country in terms of traffic sessions, including the destination, threat score, sessions, and bytes.
	Policy Hits	Lists the policy sessions by policy, device name, VDOM, number of hits, bytes, and last used time and date.
	DNS Logs	Summarizes the DNS activity on the network. Double click an entry to drill down to the specific details about that domain.
	ZTNA Servers	ZTNA servers by bytes.
Shadow IT	Top Cloud Applications	Displays the top cloud applications used on the network. When viewing information about an application, FortiAnalyzer will first check the Shadow IT database, and if no results are found, it will use the metadata.
	Top Cloud Users	Displays the top cloud users on the network.
Applications & Websites 1–8	Top Applications	Displays the top applications used on the network including the application name, category, risk level, and sessions blocked and allowed. Bytes sent and received can also be enabled through the widget settings. Top Applications can be viewed as a stackbar, bar, table, or bubble chart. For a usage example, see Finding application and user information on page 111.
	Top Website Domains	Displays the top allowed and blocked website domains on the network.
	Top Website Categories	Displays the top website categories.
	Top Browsing Users	Displays the top web-browsing users, including source, group, number of sites visited, browsing time, and number of bytes sent and received.

FortiView dashboards for FortiGate and FortiCarrier devices

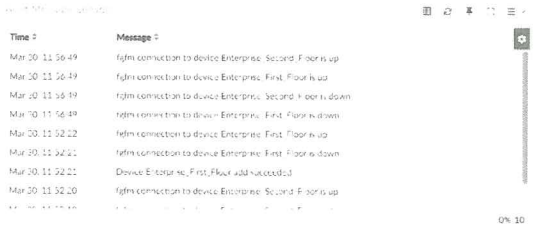
Category	View	Description
Threats	Top Threats	Lists the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus.
	Threat Map	Displays a map of the world that shows the top traffic destinations starting at the country of origin. Threats are displayed when the threat score is greater than zero and either the source or destination IP is a public IP address. The *Threat Window* below the map, shows the threat, source, destination, severity, and time. The color gradient of the lines indicate the traffic risk. A yellow line indicates a high risk and a red line indicates a critical risk. This view can be filtered by device, time, source, and destination. See also Viewing the threat map on page 94.
	Indicator of Compromise	Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats. To use this feature: 1. UTM logs of the connected FortiGate devices must be enabled. 2. The FortiAnalyzer must subscribe to FortiGuard to keep its threat database up-to-date.
	FortiSandbox Detection	Displays a summary of FortiSandbox related detections. The following information is displayed: Filename, End User and/or IP, Destination IP, Analysis (Clean, Suspicious or Malicious rating), Action (Passthrough, Blocked, etc.), and Service (HTTP, FTP, SMTP, etc.). Select an entry to view additional information in the drilldown menu. Clicking a FortiSandbox action listed in the *Process Flow* displays details about that action, including the *Overview*, *Indicators*, *Behavior Chronology Chart*, *Tree View*, and more. Information included in the *Details* and *Tree View* tab is only available with FortiSandbox 3.1.0 and above.

Alert Messages Console widget

The *Alert Message Console* widget displays log-based alert messages for both the FortiAnalyzer unit itself and connected devices.

Alert messages help you track system events on your FortiAnalyzer unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time the event occurred.

Alert messages can also be delivered by email, syslog, or SNMP.



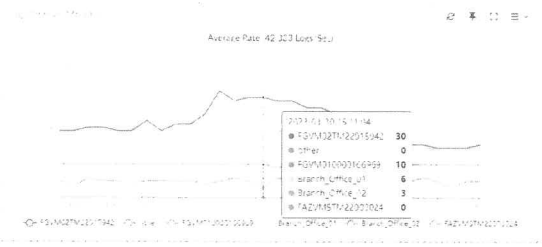
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

To view a complete list of alert messages, click *Show More* from the widget toolbar. The widget will show the complete list of alerts. To clear the list, click *Delete All Messages*. Click *Show Less* to return to the previous view.

Log Receive Monitor widget

The *Log Receive Monitor* widget displays the rate at which the FortiAnalyzer unit receives logs over time. Log data can be displayed by either log type or device.

Hover the cursor over a point on the graph to see the exact number of logs that were received at a specific time. Click the name of a device or log type to add or remove it from the graph. Click *Edit* in the widget toolbar to modify the widget's settings.



Event Handler	Description
1–10	Rule 7: Device phase2-up or phase2-down detected • Event Severity: Medium • Log Type: Event > VPN • Log Field: Device Name, Message • Log messages that match all of the following filters: • *logid=="0101037139"* and (*action=="phase2-up"* OR *action=="phase2-down"*) • Tags: NOC, VPN • Custom message: ${logdesc} due to: ${action}

Default-NOC-SD-WAN-Events	Event handler for FortiGate device type logs to generate events for SD-WAN status, alerts, and health check events including SLA targets/SLA met or not met for jitter, latency, packetloss, Health-check server status (alive or dead), status (up or down), and member status change.
	Disabled by default
	Rule 1: SLA failed for jitter
	• Event Severity: High
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match all of the following filters:
	  • *subtype=="sdwan"* AND *metric=="jitter"* AND *msg~"SLA failed"*
	• Tags: NOC, SD-WAN
	• Custom message: On ${devname} the SLA for the ${healthcheck} failed for ${metric} with the current value of ${jitter} which violates the target ID ${slatargetid}.
	Rule 2: SLA failed for latency
	• Event Severity: High
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match all of the following filters:
	  • *subtype=="sdwan"* AND *metric=="latency"* AND *msg~"SLA failed"*
	• Tags: NOC, SD-WAN
	• Custom message: On ${devname} the SLA for the ${healthcheck} failed for ${metric} with the current value of ${latency} which violates the target ID ${slatargetid}.
	Rule 3: SLA failed for packetloss
	• Event Severity: High
	• Log Type: Event > SD-WAN
	• Log Field: Device Name, Health Check
	• Log messages that match all of the following filters:
	  • *subtype=="sdwan"* AND *metric=="packetloss"* AND *msg~"SLA failed"*
	• Tags: NOC, SD-WAN

	Place your mouse over a bar in the graph to view a tooltip which includes the date/time, classifier, and count. This widget may be viewed by *Count* and *Size*. This widget can be also be displayed as a donut chart which includes charts for total mail, virus mail, and spam mail.
Mail Statistics	The summary of email messages where the FortiMail detected viruses, spam, or neither in the selected time period. Place your mouse over a bar in the graph to view a tooltip which includes the date/time, classifier, and count. This widget may be viewed by *Count*, *Size*, *Scan Speed*, and *Transfer Speed*.
Outbreak Statistics (FortiSandbox)	The summary of the number of email messages that the FortiSandbox unit is scanning in the selected time period. Email messages are tracked as either clean, containing a malicious file, or containing a malicious URL. Place your mouse over a bar in the graph to view a tooltip which includes the date/time, clean, malicious file, and malicious URL. This widget requires a FortiSandbox.
Statistics Summary	The summary of spam, viruses, and not spam in the selected time period, including the classifier details per category, the corresponding total number of every classifier, the subtotal number, the subtotal percentage of every category, and the total number of all emails.

FortiProxy

FortiProxy includes the following widgets:

Top Proxy Sources	Top proxy sources by number of sessions.
Top Proxy Destinations	Top proxy destinations by number of sessions.
Top Website Domains	Top website domains by number of sessions.
Top Threats Destinations	Top threat destinations by threat level.
Top Threats	Top threats by threat level.
Top Applications	Top applications by risk.
Top DLP Events	Top DLP events by number of incidents.

Secure SD-WAN Monitor

1–11

Secure SD-WAN Monitor includes the following widgets:

SD-WAN Bandwidth Overview	The bandwidth of the SD-WAN network over time. This widget displays a line chart of the sent/received rate (bps) in the selected time period for SD-WAN members interfaces.

SD-WAN Performance Status	The SD-WAN performance status comparison with interfaces. Mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check. Click on a scatter chart to view additional details.
SD-WAN Rules Utilization	The SD-WAN rule traffic utilization by interface and application.
SD-WAN Utilization by Application	The share of bandwidth utilization by application for each WAN link.
Top SD-WAN SLA Issues	The top SD-WAN SLA issues. The *Sort By: Speed* option in this widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
SD-WAN Events	This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.
Application Bandwidth Utilization	The total bandwidth from all applications as well as the bandwidth per-SD-WAN interface. This widget can be viewed in a sanky chart or table chart format.
Per-Application Performance	The performance for the selected application based on chosen metric. You can select an application in the widget's *Application* dropdown menu. *Latency*, *Jitter*, *Packet Loss*, and *Bandwidth* metrics are available.
Global-Application Performance	The global application performance for the selected metric. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
SD-WAN Interfaces	The information for SD-WAN interfaces and ADVPN shortcut interfaces. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
Audio MOS Score	The MOS score by interface. Mousing over the chart displays a summary of the MOS score and VoIP quality at that point. The interface must have a performance SLA with MOS enabled to display in the chart.
Speed Test	The upload and download speeds for all tests run on SD-WAN interfaces through a specified time. This widget requires event logs generated by speed tests from FortiOS 7.4.0 or higher.
Health Check Status	This widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.

1–11

To update the *Refresh Interval*, click the settings icon at the top of the widget, and then select a value from the dropdown.

To filter a chart, click a key in the legend.

SD-WAN Summary

SD-WAN Summary monitor includes the following widgets:

Widget	Description
	• *Known or Suspected URL-based Attack* • *Known or Suspected Impersonation-based Threats*
Email Bandwidth	An area chart that displays the amount of bandwidth used by email traffic, which includes data for inbound emails and spam emails over time. Mouse over the chart to display a tooltip of values for inbound and spam emails at that time.
Email Count	A stacked bar chart that displays the number of emails over time by inbound emails and spam emails. Mouse over the chart to display a tooltip of values for inbound or spam emails at that sample time.
Top Senders by Email Size	A pie chart that displays the email accounts which have sent the largest emails by size. Mouse over the chart to display a tooltip of the email account and the amount of emails sent by size and percentage.
Top Recipients by Email Size	A pie chart that displays the email accounts which have received the largest emails by size. Mouse over the chart to display a tooltip of the email account and the amount of emails received by size and percentage.
Top Recipients by Count	A race bar chart that displays the top email accounts with highest number of emails received. The chart is animated to show the number of emails for each account over time.
Top Senders by Count	A race bar chart that displays the top email accounts with highest number of emails sent. The chart is animated to show the number of emails for each account over time.
Top Malware Senders	Displays email accounts that have sent the highest number of malwares using email.
Top Phishing Senders	Displays email accounts with the highest number of attempts to send phishing emails.
Top Spam Senders	Displays spammer email accounts sorted by email count.

1–12

SOC dashboard

The *SOC Dashboard* provides an overview of incidents, events, and alerts. By clicking on widgets in the dashboard, you can open the detailed information in the *Incidents & Events* pane, as well as other panes in the FortiAnalyzer GUI.

Use the time range dropdown to filter all widgets in the *SOC Dashboard*. You can customize which widgets appear in the dashboard. After clicking *Edit*, select which widgets should appear using the *Toggle Widget* dropdown. You can also resize and move widgets in this display. Once the changes are complete, click *Save*.

By default, the *Statistics* widget displays at the top of the dashboard. The following is available in the *Statistics* widget in the *SOC Dashboard*:

Deleting a CRL

To delete a CRL or CRLs:

1. Go to *System Settings* > *Certificates*.
2. Select the CRL or CRLs you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

1-13

Log Forwarding

You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server when you use the default forwarding mode in log forwarding. You can also forward logs via an output plugin, connecting to a public cloud service.

The *client* is the FortiAnalyzer unit that forwards logs to another device. The *server* is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs.

In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. See Log storage on page 40 for more information.

To see a graphical view of the log forwarding configuration, and to see details of the devices involved, go to *System Settings* > *Logging Topology*. For more information, see Logging Topology on page 341.

Modes

FortiAnalyzer supports two log forwarding modes: forwarding (default), and aggregation.

Forwarding

Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

This mode can be configured in both the GUI and CLI.

Aggregation

As FortiAnalyzer receives logs from devices, it stores them, and then forwards the collected logs at a specified time every day. To avoid duplication, the client only sends logs that are not already on the server.

FortiAnalyzer supports log forwarding in aggregation mode only between two FortiAnalyzer units. Syslog and CEF servers are not supported.

To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiAnalyzer unit.
   You can also migrate the data to another FortiAnalyzer unit, if you have one. Data migration reduces system down time and the risk of data loss.
3. Install the disks in the FortiAnalyzer unit.
   If your unit supports hot swapping, you can do so while the unit is running. Otherwise the unit must be shut down first. See Unit Operation widget on page 64 for information.
4. Configure the RAID level. See Configuring the RAID level on page 359.
5. If you backed up the log data, restore it.

1-14

Administrative Domains (ADOMs)

Administrative domains (ADOMs) enable administrators to manage only those devices that they are specifically assigned, based on the ADOMs to which they have access. When the ADOM mode is advanced, FortiGate devices with multiple VDOMs can be divided among multiple ADOMs.

Administrator accounts can be tied to one or more ADOMs, or denied access to specific ADOMs. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. Super user administrator accounts, such as the `admin` account, can see and maintain all ADOMs and the devices within them.

Each ADOM specifies how long to store and how much disk space to use for its logs. You can monitor disk utilization for each ADOM and adjust storage settings for logs as needed.

The maximum number of ADOMs you can add depends on the FortiAnalyzer system model. Please refer to the FortiAnalyzer data sheet for more information.

When the maximum number of ADOMs has been reached, you will be unable to create a new ADOM.

When upgrading to FortiAnalyzer 6.2.1 or later, you will continue to have access to any ADOMs exceeding the limit, however, no additional ADOMs can be created, and an alert will be issued in the *Alert Message Console* in *Dashboards* > *Status*.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by administrators with the *Super_User* profile. See Administrators on page 411.

The root ADOM and Security Fabric ADOMs are available for visibility into all Fabric devices. See Security Fabric ADOMs on page 176.

Non-FortiGate devices are automatically located in specific ADOMs for their device type. They cannot be moved to other ADOMs, except for FortiClient devices, which can be promoted to Fabric ADOMs if needed.

ADOMs must be enabled to support the logging and reporting of non-FortiGate devices.

To check the IOC package in the CLI:

```
diagnose fmupdate fds-getobject

FAZ object version information
ObjectId                Description             Version         Size    Created Date Time
-------------------------------------------------------------------------------------------
-------
...
00001000TIDB00100       ThreatIntel DB          00000.01052     34 MB   19/04/14 20:10
   ext_desc:ThreatIntel DB
00001000TIDB00100       ThreatIntel DB          00000.01053     37 MB   19/04/16 04:13
<latest> ext_desc:ThreatIntel DB
...
```

FortiAnalyzer periodically syncs its own IOC TIDB files to the version of IOC package downloaded by *fmupdate*. This is performed on a one hour schedule.

To check the license and TIDB version used by FortiAnalyzer in the CLI:

```
diagnose test application sqllogd 204 stats

License of post breach detection installed.
License expiration : 2025-Jan-04
TIDB version : 00000.01017-1902242107
TIDB load time : 2019-02-24 14:11:2
```

1-15

Configuring FortiGate to FortiAnalyzer REST API authentication

FortiGate to FortiAnalyzer REST API authentication allows the FortiAnalyzer to send IOC alerts and trigger configured automation rules, if configured.

To configure REST API authentication:

1. Go to the *Device Manager* in the FortiAnalyzer.
2. Edit the FortiGate device to set the FortiGate super admin username and password.
   This is the only way to configure REST API authentication prior to 6.2.

Alternatively, when configuring logging to FortiAnalyzer on FortiGate, you can go to *Security Fabric* > *Settings* and enable *Allow access to FortiGate REST API* and *Trust FortiAnalyzer by serial number*.

Throttling IOC alerts

To avoid flooding FortiGate with event alerts, you can configure a throttle which allows only one alert to be sent within a set period of time for the same endpoint.
The default time period is one day (1440 minutes).

To set an IOC alert throttle in the CLI:

```
config system log ioc
(ioc)# set
 notification             Disable/Enable Ioc notification.
 notification-throttle    Minute value for throttling the rate of IoC notifications.
```

外 標 封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103 (第一次公告)
截止投標時間：113年11月25日下午05時整　　開標時間：113年11月25日下午05時整

11031 臺北市信義區吳興街 250 號

臺北醫學大學總務處事務組收

事務組採購承辦人：李清萬先生

投標廠商	威尼克科技有限公司	統一編號	53099614
廠商地址	新北市永和區中山路一段269號3樓	廠商電話	0930-275-766
廠商聯絡人	林伯勳 聯絡人電話 0930-275-766	聯絡人E-mail	wilson@vink.com.tw

※注意事項：

一、投標文件遞送請注意時效，寄達本校事務組採購承辦人處，如逾時視為無效標。

二、投標文件應以不透明容器(封套)密封，外標封標籤請書寫完整基本資料後貼於標封封面，如未載明本案採購案名、標號及投標廠商、地址、電話或封口處未密封或信封套為透明者，皆視為無效標。

投標文件送達紀錄

▶廠商請擇一勾選

☐郵寄或快遞送達(免簽章及免填送達時間)

☑專人送達(送件須簽章並註記送達時間)

投標廠商送件人簽章：林伯勳

送達日期及時間：113.11.4 10:30

本校收件人簽名：

收件日期及時間：113.11.4 10:30

資、規格封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本資、規格封內請依投標須知規定裝入相關審核文件(請影印為 A4 尺寸)，並以迴紋針固定於左上角，俾利開標審核作業。

投標廠商	威尼克科技有限公司	統一編號	53099614
廠商地址	新北市永和區中山路1段269號3樓	廠商聯絡人	林佰勳
廠商電話	0930-275-766	聯絡人電話	0930-275-766

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **其他附件：(第一次公告)** 標號：TMU113-103

附 件 二

投標廠商資、規格審查表

※請依表列順序排放證件影本並將本表置於首頁

廠商所提資格文件影本，本校得通知廠商限期提出正本供查驗，查驗結果如與正本不符，係偽造或變造者，依採購法第 50 條規定辦理。

採購名稱	防火牆日誌紀錄器	採購案號	1130203887
廠商名稱	秦譽科技股份有限公司	廠商統編	28208184
負責人	賴銘德	廠商印鑑章	
聯絡人	陳妤嘉 Email: yoga.chen@tai-win.com.tw		
聯絡電話	(市話)0225781133 (手機)0908590611		
廠商地址	105：台北市南京東路四段130號4F		

	投標廠商資格審查項目		招標機關資格審查
資規格項目	☑ 1.押標金(119,000 元)繳納憑據 ☐ 依投標須知規定，免檢附	☑符合 ☐不符合	採購單位審查(項目1-8項)： ☑合格 且開標前已至政採網查詢非拒絕往來廠商詳附件 ☐不合格，說明：
	☑ 2.廠商登記或設立證明	☑符合 ☐不符合	
	☑ 3.廠商最近一期納稅證明	☑符合 ☐不符合	
	☑ 4.廠商信用證明	☑符合 ☐不符合	採購單位簽章：李彥蓉 11/5
	☑ 5.非拒絕往來廠商查詢並列印 (請至工程會網站 web.pcc.gov.tw 查詢列印)	☑符合 ☐不符合	
	☑ 6.投標廠商聲明書	☑符合 ☐不符合	
	☑ 7.出席代表授權書 ☐ 負責人親自出席，免檢附	☑符合 ☐不符合	
	☑ 8.電子領標電子憑據	☑符合 ☐不符合	
	☑ 9.廠商製造、供應或承做能力證明	☑符合 ☐不符合	請購單位審查(項目 9-11 項)： ☑合格 ☐不合格，說明：
	☐ 10.廠商須具有維修、維護或售後服務能力之證明	☐符合 ☐不符合	
	☑ 11.型錄或規格說明書	☑符合 ☐不符合	請購單位簽章：陳曉傑

投標廠商審查結果	投標廠商不符事項確認	投標廠商簽章▼
☑合 格 ☐不合格	本廠商所投標及釋疑補充之文件等，經貴機關審核後，不符招標文件規範經本廠商確認無誤後，謹此簽章認同。	

附 件 三

出席代表授權書

茲授權本公司(商號或法人) 所屬員工：陳妤嘉 先生/小姐代表本公司(商號或法人)出席貴校「**防火牆日誌紀錄器**」之開標/評選/議價會議，該員在開標/評選/議價會議中所做之任何承諾或簽認事項直接對本公司(商號或法人)發生效力，本公司(商號或法人)均予以承受，並經本公司(商號或法人)確認被授權人之下列簽樣真實無誤。

被授權人之簽樣[*註]：陳妤嘉 或

請惠予核備。

此　　致

臺北醫學大學

授權人公司(商號)：泰譽科技股份有限公司
負責人姓名：賴銘德
公司(商號)統一編號：28208184
負責人身分證統一編號：A122368691

被 授 權 人：陳妤嘉
身分證統一編號：N226047187
通訊地址：台北市南京東路四段130號4F
聯絡電話：0908590611

中　華　民　國 113 年 11 月 25 日

*註：『被授權人簽樣』得為**下列形式之1**，依民法第103條規定，代理人於代理權限內所為之意思表示，直接對投標廠商發生效力：1.公司大小章。2.投標專用章。3.被授權人簽章。

列印時間：113/11/25 16:40

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為
廠商代碼： 28208184 (泰瑩科技股份有限公司)
廠商現況： 01-核准設立
廠商名稱： 泰瑩科技股份有限公司

資料取得時間：113/11/25 16:40

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

李清萬

臺北醫學大學暫收款收據

007892

民國 113 年 11 月 25 日

繳款公司	泰瑩科技股份有限公司			電話：0908590611
款項名稱	1押標金 2圖說 3	採購案名稱	防火牆日誌紀錄器	
收款票據明細	支票號碼	KB2232917	支票日期	113年 11 月 18 日
	付款銀行	彰化商業銀行庫 東台北	分行(部.庫)	
收款金額	新臺幣(大寫)：仟 佰 壹拾 壹萬 玖仟 佰 拾 元整			
備註	請妥善保管此收據，得標後憑此暫收據換正式收據。			

出納組 113 11 25 許文嘉

經收人：

112.05.01

第一聯：出納組聯（白） 第二聯：暫收據（紅）

正本

自領

2

臺北市政府　　函

機關地址：110臺北市市府路1號北區1樓
承辦人：楊光遠（307）
電　話：02-27208889/1999轉6530
傳　真：02-27228444

100

臺北市中正區北平東路30號12樓之3

受文者：泰瑩科技股份有限公司代理人：胡碩勻會計師

發文日期：中華民國113年09月20日
發文字號：府產業商字第11353405100號
速別：普通件
密等及解密條件：普通
附件：規費收據暨變更登記表1份

主旨：貴公司（統一編號：28208184）申請發行新股、修正章程變更登記，准予登記。另申請董事、監察人持有股份變動報備，准予備查，並請詳閱說明欄相關事項，以保障公司權益，請查照。

說明：

一、依公司法辦理兼復貴公司委託信達聯合會計師事務所胡碩勻會計師113年9月18日申請書。

二、處分相對人名稱：泰瑩科技股份有限公司（代表人姓名：賴銘德、身分證照號碼：A12236****）、公司所在地：臺北市松山區南京東路4段130號4樓。

三、檢附規費收據暨變更登記表1份，請查收。

四、對本行政處分如有不服，請依訴願法第14條及第58條規定，自行政處分書達到之次日起30日內，繕具訴願書，向本府遞送（以實際收受訴願書之日期為準，而非投郵日），並將副本抄送經濟部（地址：臺北市中正區福州街15號）。

正本：泰瑩科技股份有限公司代理人：胡碩勻會計師
副本：

市長 蔣萬安

本案依分層負責規定授權人員決行

統一編號：28208184

宣導事項:

※營業地點涉有室內裝修時，應依「建築物室內裝修管理辦法」申請室內裝修審查許可；並應依「建築物公共安全檢查簽證及申報辦法」規定定期辦理申報，如有違反規定，將依建築法裁罰6萬至30萬元。

※公司登記之核准，與土地及建物是否合法使用係屬二事，貴公司實際經營業務之營業場所應符合都計、建管、消防等法令規定，違反者，應受上開法令之處罰。貴公司可向營業場所所在地直轄市、縣（市）政府之都計、建管單位，如營業場所位於臺北市者，可利用營業場所預先查詢系統(https://reurl.cc/yyGaRO)，查詢實際營業之場所是否符合土地使用分區管制與建築管理之規定。

※有關都市計畫法及建築法等相關規定，請洽本府都市發展局，電話：02-27208889/1999轉6737(都市計畫便民資訊查詢系統網址：http://www.zonemap.taipei.gov.tw/)及本市建築管理工程處，電話：02-27208889/1999轉8387(臺北市網際網路執照存根影像查詢系統網址：http://163.29.37.131/)。

※依公司法第9條規定，公司應收之股款，股東並未實際繳納，而以申請文件表明收足，或股東雖已繳納而於登記後將股款發還股東，或任由股東收回者，公司負責人各處5年以下有期徒刑、拘役或科或併科新臺幣50萬元以上250萬元以下罰金。如經法院判決有罪確定，由中央主管機關撤銷或廢止公司登記。敬請留意避免觸法。

※依臺北市自助選物販賣事業管理自治條例規定，自助選物販賣事業及非自助選物販賣事業於其營業場所內自行或提供他人設置自助選物販賣機者，應依法辦妥公司或商業登記、營業場所應距離國民中小學50公尺以上，違反規定者，將限期命其停止營業，屆期未改善者，處新臺幣2萬元以上10萬元以下罰鍰，並得按次處罰。

※聘僱外籍人士前，應確實核對應徵者身分文件正本或依法向勞動部申請聘僱外國人工作許可，切勿僱用不明身分之外籍人士，如違反相關規定，最高可罰75萬元。

※公司登記業務除臨櫃或郵寄方式辦理外，亦提供線上申請之管道（網址：https://onestop.nat.gov.tw），公司登記線上辦理登記費減收300元，又不必出門或郵寄即可完成送件，省時省錢又省力，敬請多加利用。經濟部商工行政諮詢專線:(行動電話請加撥02)412-1166，(六碼地區請撥 41-1166)

※有關全民健康保險部分，請檢送相關表件自行向衛生福利部中央健康保險署各分區業務組，辦理有關投保單位變更事宜，相關規定請至該署全球資訊網(http://www.nhi.gov.tw)參閱。

※經營餐館業者，請於營業場所裝設油脂截留器，以免違反《建築物給水排水設備設計技術規範》、《廢棄物清理法》等法令規定。[相關事項請洽本府環境保護局，電話：02-27208889/1999轉7261及本府工務局

衛生下水道工程處，電話：02-25973183轉188〕。

※公司嗣後若有臺北市房屋、土地及車輛，可透過長期約定轉帳代繳地方稅款，請至臺北市稅捐稽徵處網站／納稅資訊／申辦與書表下載／稅務管理及其他／8.申請委託轉帳代繳（領）各項稅款項下，填寫委託轉帳代繳稅款約定書並同時申辦以電子方式傳送轉帳繳納通知及證明。

※使用牌照稅繳款書112年7月1日起開放歸戶囉!多張繳款書可申請整合為1張，每張繳款書以5筆車籍號碼為限，可至『地方稅網路申報作業入口網』點選『使用牌照稅歸戶申請』（網址：https：//net.tax.nat.gov.tw）線上申請，或填寫申請書，以郵寄、傳真、電子檔傳送或臨櫃等方式，向車籍所在地之稅捐稽徵機關申請。

※經營西藥、中藥或醫療器材之業者，如有停、解散或公司名稱、地址、負責人、管理人/監製人、技術人員、營業項目變更，請於法定限期內（經營西藥、中藥業者 應於15日內、經營醫療器材業者應於30日內），向本府衛生局（電話：02-27208889/1999轉7073）辦理變更登記，以免違反藥事法、醫療器材管理法之規定。

※為保護個人資料安全，業者提供消費明細所揭露之資訊，應依個人資料保護法規定辦理

※為平等保障身心障礙者之生命安全及緊急逃生時機，建議逃生避難設施應具備無障礙通用性，例如設有點字、觸摸引導、語音播放等措施。

※1. 為提供友善通行環境 ，若民眾有設置需求，建管處將委派建築師提供現場無障礙專業諮詢服務，並定期召開改善諮詢審查會議。詳情可聯繫建管處無障礙專案諮詢電話：1999轉8394。相關建築物無障礙資訊，也可至建管處建築物無障礙專區參考（網址：https://reur1.cc/dD7daD，或可直接查詢：建管處網站首頁-宣導專區-建築物無障礙專區），歡迎本市店家與市府一同打造無障礙友善環境，提供行動不便者、攜帶嬰兒車者及年長者一個安全暢行的便利生活。2.另本市店家營運場域內可供輪椅通行，且具有服務熱忱者，可備妥相關文件自行申請加入本市友善店家，有機會參與導客活動等行銷推廣，提升店家知名度及形象，相關訊息可至台北友善店家官網（網址：https://friendlystore.taipei/）；相關建築物無障礙資訊，可至建管處建築物無障礙專區參考（網址：https://reur1.cc/dD7daD，或可直接查詢：建管處網站首頁-宣導專區-建築物無障礙專區）。

※身心障礙者權益保障法第60條略以，視覺、聽覺、肢體功能障礙者由合格導盲犬、導聾犬、肢體輔助犬陪同或導盲犬、導聾犬、肢體輔助犬專業訓練人員於執行訓練時帶同幼犬，得自由出入公共場所、公共建築物、營業場所、大眾運輸工具及其他公共設施，不得收取額外費用，且不得拒絕其自由出入或附加其他出入條件。違者依同法第100條令限期改善；屆期未改善者，處新臺幣1萬元以上5萬元以下罰鍰，並接受4小時之講習。

※依公司法第22條-1規定，除外商公司、公開發行股票公司及國營事業

外，公司應於設立後十五日內前往「公司負責人及主要股東資訊申報平臺」(網址：https://ctp.tdcc.com.tw)完成首次申報，並依規定進行後續變動申報及年度申報。應申報資料包括董事、監察人、經理人及持有已發行股份總數或資本總額超過百分之十之股東之姓名或名稱、國籍、出生年月日或設立登記之年月日、身分證明文件號碼、持股數或出資額。未依規定完成申報或申報不實之公司，經限期通知改正仍未改正者，可處新臺幣5~500萬元罰鍰，最重將可廢止公司登記。申報方式及相關規定可前往申報平臺瀏覽(網址:https://ctp.tdcc.com.tw)。

※依「臺北市消費者保護自治條例」規定，設址本市之公司、分公司其營業場所若屬「臺北市消費場所強制投保公共意外責任保險實施辦法」規範應投保公共意外責任保險範疇，應即依規定投保。

經衛生福利部公告類別及規模之食品業者，應依食品安全衛生管理法第13條第1項規定事先完成產品責任保險之投保，並保存該保險文件，維持保單有效性，以免違反食品安全衛生管 理法之規定。若有相關疑問，請聯繫臺北市政府衛生局諮詢窗口（02-27208889／1999轉7088）

※為促進高齡者的職場連結，企業可應用智慧科技與輔具，進行職務再設計，提供更為友善中高齡工作者的工作設備、條件、方法，減輕其工作負荷，增加其繼續就業的可能；另鼓勵企業運用智慧科技以發展多元就業模式，包括部分工時、彈性工時、遠距辦公、在家工作等，讓需彈性工時工作者，亦能持續參與勞動市場。

※毒品不來亂-人生才燦爛，為避免特定營業場所淪為毒品施用者取得及施用毒品之管道，請業者應善盡場所管理責任。

※涉及稅籍登記部分，請於開始營業前檢送負責人身分證明文件、公司章程、許可業務之核准文件等影本洽營業所在地稽徵機關辦理；詳細文件請逕洽各地區國稅局。

※臺灣地區位於環太平洋地震帶，除平時應預防之火災、豪雨、颱風等，仍需預防大規模災害導致交通運輸停擺，衍生之混亂、意外事故及影響救災等情形，建議貴公司視業務性質制定災害應變計畫，於平時儲備糧食、飲用水、隨身包等防災用品，並考量與供應商、物流業者等簽訂開口契約或協議，於災時可供應員工足夠之生活必需品（如飲用水及食物），以因應災時緊急需求，降低災害損失，並快速重返營運，達成企業永續經營之目標。另應購買經認證之消防機具器材或防災產品，以維權益。

※經濟部已建置公司登記函復電子送達平台，只要申請人於公司登記申請書勾選領取方式為「電子送達」，並留下聯絡人姓名、電子信箱及手機號碼，申請人就可直接在該平台下載登記機關電子函復公文，與紙本公文送達有同一效力，可縮短取得公文之時間，敬請多加利用。

貴公司如經營自助選物販賣事業，請依111年1月29日修訂「臺北市自助選物販賣事業防疫營運指引」規範，檢附復業申請書等文件，向本市商業處復業申請，並經同意後始得營業。

※為維護企業經營者信譽，惠請貴公司於生產、製造、進口或販賣商品時落實商品標示，若欲瞭解商品標示法及相關標示基準詳盡規定，請上臺北市商業處網站（http://www.tcooc.taipei.gov.tw/）查詢。

※勞動部辦理免費創業課程及諮詢輔導，另提供符合資格者微型創業貸款利息補貼，申辦簡便，不需委託他人代辦，請洽詢0800-092-957免付費服務專線。

※有關勞動條件及職業安全衛生法規定辦理事項可參考臺北市政府勞動局首頁https://bola.gov.taipei/>業務服務>勞動服務>勞動條件／職業安全衛生服務專>百寶箱

裝

訂

線

（公司印章）　　（代表公司負責人印章）

變更時請打V		變更時請打V	

印章請用油性印泥蓋章，並勿超出框格。

股份有限公司變更登記表

變更預查編號
公司統一編號 28208184
公司聯絡電話 (02)25787890
僑外投資事業 □是 V否　公開發行 □是 V否
陸資 □是 V否
閉鎖性股份有限公司股東人數＿＿人
複數表決權特別股 □有 V無
對於特定事項具否決權特別股 □有 V無
特別股股東被選為董事、監察人之禁止或限制或當選一定名額之權利 □有 V無

原名稱　　股份有限公司

	一、公司名稱（變更後）	中文	泰瑩科技			股份有限公司
		（章程所訂）外文				
	二、（郵遞區號）公司所在地（含鄉鎮市區村里）		（ 105 ）台北市松山區南京東路4段130號4樓			
	三、代表公司負責人		賴銘德	四、每股金額（阿拉伯數字）		10 元
	五、資本總額（阿拉伯數字）					60,000,000 元
V	六、實收資本總額（阿拉伯數字）					60,000,000 元
	七、股份總數		6,000,000 股	V	八、已發行股份總數 1.普通股	6,000,000 股
					2.特別股	0 股
	九、董事人數任期		5 人　自 111 年 8 月 23 日　至　114 年 8 月 22 日 （含獨立董事 0 人）			
	十、■監察人人數任期 或 □審計委員會		1 人　自 111 年 8 月 23 日　至　114 年 8 月 22 日			
			本公司設置審計委員會由全體獨立董事組成替代監察人			
V	十一、公司章程修正（訂定）日期		113 年 06 月 26 日			

※變更登記日期文號 11353405100　※檔號

公務記載蓋章欄

臺北市政府 113 9 20 公司登記表 專用章(20)

（一）申請表一式二份，於核辦後一份存核辦單位，一份送還申請公司收執。
（二）為配合電腦作業，請打字或電腦以黑色列印填寫清楚，數字部份請採用阿拉伯數字，並請勿折疊、挖補、浮貼或塗改。
（三）※各欄如變更登記日期文號、檔號等，申請人請勿填寫。
（四）違反公司法代作資金導致公司資本不實，公司負責人最高可處五年以下有期徒刑。
（五）為配合郵政作業，請於所在地加填郵遞區號。
（六）第十欄位請依公司章程內容，於「監察人人數任期」前註記■，並填寫人數任期；或於「審計委員會」前註記■，監察人之人數任期免填。
（七）閉鎖性股份有限公司應填列股東人數、以技術或勞務出資者應填列章程載明之核給股數與抵充金額（勞務出資僅適用閉鎖性股份有限公司）。

泰瑩科技

股份有限公司變更登記表

註:欄位不足請自行複製，未使用之欄位可自行刪除，若本頁不足使用，請複製全頁後自行增減欄位。

更變時請打V						
V	十二、本次股本增加明細 (股本若為9、10、11、12之併購者，請加填第十四欄)	資產增加	1. 現金	0股、	0元	
			2. 財產	0股、	0元	
			3. 技術	0股、	0元	
			4. 股份交換	0股、	0元	
			5. 認股權憑證轉換股份	0股、	0元	
		權益科目調整	6. 資本公積	0股、	0元	
			7. 法定盈餘公積	0股、	0元	
			8. 股息及紅利	800,000股、	8,000,000元	
		併購	9. 合併	0股、	0元	
			10. 分割受讓	0股、	0元	
			11. 股份轉換	0股、	0元	
			12. 收購	0股、	0元	
		其他	13. 債權抵繳股款	0股、	0元	
			14. 公司債轉換股份	0股、	0元	
			15. 勞務	0股、	0元	
				股、	元	
				股、	元	

	十三、本次股本減少明細	1. 彌補虧損	0股、	0元	2. 退還股款	0股、 0元
		3. 註銷庫藏股	0股、	0元	4. 合併銷除股份	0股、 0元
		5. 分割減資	0股、	0元	6. 收回特別股	0股、 0元

十四、被併購公司資料明細

	併購種類	併購基準日	被併購公司	
			統一編號	公司名稱
		年 月 日		
		年 月 日		

臺北市政府 113. 4. 20 公司登記表 專用章(20)

公務記載蓋章欄

11353405100

泰瑩科技

股份有限公司變更登記表

註:欄位不足請自行複製，未使用之欄位可自行刪除，若本頁不足使用，請複製全頁後自行增減欄位。

更請V變時打	所營事業		
	編號	代碼	營業項目說明
	1	E605010	電腦設備安裝業
	2	E801010	室內裝潢業
	3	F108040	化粧品批發業
	4	F109070	文教、樂器、育樂用品批發業
	5	F113020	電器批發業
	6	F113030	精密儀器批發業
	7	F113050	電腦及事務性機器設備批發業
	8	F113070	電信器材批發業
	9	F118010	資訊軟體批發業
	10	F119010	電子材料批發業
	11	F208040	化粧品零售業
	12	F209060	文教、樂器、育樂用品零售業
	13	F213010	電器零售業
	14	F213030	電腦及事務性機器設備零售業
	15	F213040	精密儀器零售業
	16	F213060	電信器材零售業
	17	F218010	資訊軟體零售業
	18	F219010	電子材料零售業
	19	F399990	其他綜合零售業
	20	F401010	國際貿易業
	21	F601010	智慧財產權業
	22	I102010	投資顧問業
	23	I103060	管理顧問業
	24	I199990	其他顧問服務業
	25	I301010	資訊軟體服務業
	26	I301020	資料處理服務業

臺北市政府 113.9.20 公司登記表專用章(20)

公務記載蓋章欄

11353405100

泰瑩科技　　股份有限公司變更登記表

註:欄位不足請自行複製，未使用之欄位可自行刪除，若本頁不足使用，請複製全頁後自行增減欄位。

更請變時打V	所營事業		
	編號	代　碼	營業項目說明
	27	I301030	電子資訊供應服務業
	28	I401010	一般廣告服務業
	29	I503010	景觀、室內設計業
	30	IE01010	電信業務門號代辦業
	31	IZ12010	人力派遣業
	32	IZ13010	網路認證服務業
	33	IZ15010	市場研究及民意調查業
	34	IZ99990	其他工商服務業
	35	E599010	配管工程業
	36	E601010	電器承裝業
	37	E601020	電器安裝業
	38	E603010	電纜安裝工程業
	39	ZZ99999	除許可業務外，得經營法令非禁止或限制之業務

更請變時打V	董事、監察人 或 其他負責人 名單				
	編號	職　稱	姓名(或法人名稱)	身分證號(或法人統一編號)	持有股份(股)
		(郵遞區號)	住　所　或　居　所　(或　法　人　所　在　地)		
V	1	董事長	賴銘德	A1223*****	1,342,317
		*****			
V	2	董事	賴金德	A1292*****	903,741
		*****			
	3	董事	錢均義	A1701*****	0
		*****			
V	4	董事	黃志剛	A1235*****	52,721
		*****			

臺北市政府 113.11.21 公司登記表 專用章(20)

公務記載蓋章欄

11353405100

泰瑩科技　　股份有限公司變更登記表

註:欄位不足請自行複製，未使用之欄位可自行刪除，若本頁不足使用，請複製全頁後自行增減欄位。

更請V變時打	董事、監察人 或 其他負責人 名單				
	編號	職　稱	姓名(或法人名稱)	身分證號(或法人統一編號)	持有股份(股)
		(郵遞區號)	住　所　或　居　所　(或　法　人　所　在　地)		
V	5	董事	費立平	A1213*****	128,769
		*****			
V	6	監察人	石鈺涵	J1216*****	209,880
		*****			

更請V變時打	所　代　表　法　人			
	編號	董監事編號	所代表法人名稱	法人統一編號
		(郵遞區號)	法　人　所　在　地	
	1	6　～　6	泰倡企業股份有限公司	30898615
		(　105　)台北市松山區南京東路4段130號4樓之1		

臺北市政府 113.9.20 公司登記表專用章(20)

公務記載蓋章欄
11353405100

營業人銷售額與稅額申報書(401)

（一般稅額計算----專營應稅營業人使用）

第二聯：收執聯

統一編號 28208184
營業人名稱 泰鑒科技股份有限公司
稅籍編號 111307732

所屬年月份：113 年 09 — 10 月

金額單位:新臺幣元

核准按月申報
註記欄 核准合併總繳 總機構彙總報繳
單位 各單位分別申報

負責人姓名 賴銘德　營業地址 臺北市松山區南京東路４段１３０號４樓　使用發票份數 218 份

區分	項目		銷售額		稅額	零稅率銷售額
銷項	三聯式發票、電子計算機發票	1	0	2	0	3（非經海關出口應附證明文件者）
	收銀機發票(三聯式)及電子發票	5	40,855,698	6	2,042,787	7 0
	二聯式發票、收銀機發票(二聯式)	9	0	10	0	11（經海關出口免附證明文件者）
	免用發票	13	0	14	0	15 0
	減：退回及折讓	17	0	18	0	19 0
	合計	21 (1)	40,855,698	22 (2)	2,042,787	23 (3) 0
	銷售額總計 (1)+(3)	25 (7)	40,855,698 元	內含銷售固定資產	27	0 元

區分	項目		得扣抵進項稅額 金額		稅額
進項	統一發票扣抵聯（包括一般稅額計算之電子計算機發票扣抵聯）	進貨及費用	28 9,310,980	29	465,555
		固定資產	30 0	31	0
	三聯式收銀機發票扣抵聯及一般稅額計算之電子發票	進貨及費用	32 32,336,574	33	1,616,847
		固定資產	34 0	35	0
	載有稅額之其他憑證（包括二聯式收銀機發票）	進貨及費用	36 79,293	37	3,965
		固定資產	38 0	39	0
	海關代徵營業稅繳納證扣抵聯	進貨及費用	78 0	79	0
		固定資產	80 0	81	0
	減：退出、折讓及海關退還溢繳稅款	進貨及費用	40 0	41	0
		固定資產	42 0	43	0
	合計	進貨及費用	44 41,726,847	45 (9)	2,086,367
		固定資產	46 0	47 (10)	0
	進項總金額（包括不得扣抵憑證及普通收據）	進貨及費用	48		41,726,847 元
		固定資產	49		0 元
	進口免稅貨物		73		0 元
	購買國外勞務		74		0 元

代號	項目		稅額
1.	本期(月)銷項稅額合計	(2) 101	2,042,787
7.	得扣抵進項稅額合計	(9)-(10) 107	2,086,367
8.	上期(月)累積留抵稅額	108	2,753,816
10.	小計(7+8)	110	4,840,183
11.	本期(月)應實繳稅額(1-10)	111	0
12.	本期(月)申報留抵稅額(10-1)	112	2,797,396
13.	得退稅限額合計	(3)x5%-(10) 113	0
14.	本期(月)應退稅額(如 12>13 13>12 則為 13 12)	114	0
15.	本期(月)累積留抵稅額(12-14)	115	2,797,396

稅額計算

保稅區營業人按進口報關程序銷售貨物至我國境內課稅區之免開立統一發票銷售額 元 0

82.

收件編號：A282081841131084574
申報日期：113年11月13日
申報次數：001 次
進銷項筆數：427 筆
法院拍賣進項資料筆數：0 筆
零稅率銷售額筆數：0 筆
營業人申報固定資產退稅清單筆數：0 筆
營業人購買舊乘人小汽車及機車進項憑證明細筆數：0 筆
已納稅額：0 元
最後異動日期：113年11月13日 12:30:11
製表日期：113年11月13日

財政部 臺北國稅局 113.11.13 營業稅網路申報收件章

申辦情形	姓名	身分證統一編號	電話	登錄文(字)號
自行申報	陳麗卿	C22067****	02-25781133 #103	
委任申報				

說明

一、本申報書適用專營應稅及零稅率之營業人填報。
二、如營業人申報當期（月）之銷售額包括有免稅、特種稅額計算銷售額者，請改用（403）申報書申報。
三、營業人如有依財政部108年11月15日台財稅字第10804629000號令規定進行一次性移轉訂價調整申報營業稅，除跨境受控交易為進口貨物外，請另填報『營業稅一次性移轉訂價調整聲明書』並檢附相關證明文件，併同會計年度最後一期營業稅申報。
四、納稅者如有依納稅者權利保護法第7條第8項但書規定，為重要事項陳述者，請另填報「營業稅聲明事項表」並檢附相關證明文件。

查詢者：191101 戴振宸　查詢日期：2024-11-07 10:43:33

[遠端查詢]

第一類票據信用資料查覆單

茲將下列戶號 (帳號) 票據信用資料查覆如下，請　查照

查詢日：113年11月07日　　查覆資料截止日：113年11月01日

戶名：泰瑩科技股份有限公司　　戶號：0028208184

開戶行代號：000000000　　負責人戶號：A122368691

帳號：000000000

查　覆　結　果

一、退票與清償註記總數資訊(未清償註記提供最近三年內之退票未辦理清償註記者；已清償註記提供最近六個月內已辦理退票清償註記者)

退票理由	已清償註記		未清償註記	
	張數	金額	張數	金額
1. 存款不足	0	0	0	0
2. 發票人簽章不符	0	0	0	0
3. 擅自指定金融業者為本票之擔當付款人	0	0	0	0
4. 本票提示期限經過前撤銷付款委託	0	0	0	0

二、拒絕往來資訊

無拒絕往來紀錄。

三、經通報終止為其本票擔當付款人資訊

未經通報終止為其本票擔當付款人。

四、開戶總數資訊

已在台灣地區全體金融業者開立支票存款戶共 004 戶。

五、其他重大資訊

無。

六、關係戶資訊

無。

說明：

（1）查覆單列印之戶號後有 (*) 註記者，係指該戶號經電腦驗算為不合邏輯之資料。

（2）查覆單列印之負責人戶號欄位空白者，係指該查詢申請單所填載之負責人，並非本所檔案中所建立該被查詢公司之負責人，如需所填載負責人票信資料者，請以負責人個人名義申請辦理。但查詢者提供被查詢公司之負責人相關資料，並經查證正確更改本所檔案資料後，該欄位即列印查詢申請單所填載之負責人身分證統一編號。

（3） 因建檔及註記作業時差，本查覆單「查覆結果」欄之資料，其中第一、六兩項資訊，除有關清償註記資訊提供至查詢日之前一營業日外，其餘提供至資料截止日，另肆項資訊提供至查詢日。

（4） 不具法人人格之行號、團體，應以其負責人個人名義申請票據信用資料查詢。

（5） 本查覆單「查覆結果」欄之資料，第六項關係戶資訊如有戶名及戶號時，其詳細票信資料請另向本所查詢。

（6） 本查覆單不得為竄改、複製、發布或其他不當使用。

（7） 本查覆單以由票據交換所或受理查詢金融機構出具，始可作為證明之文件。

資料來源： 台灣票據交換所

單位章

009-5227 簽章
彰銀
東台北
(7/31)

[查詢條件]:28208184 查詢系統資訊: [InquiryTask ID: 22363466] [Inquiry ID: 44078486] [ItemCacheInfo ID: 42209042]

列印時間：113/11/14 12:54

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為

廠商代碼： 28208184
（泰鐿科技股份有限公司）

廠商現況： 01-核准設立

廠商名稱： 泰鐿科技股份有限公司

資料取得時間：113/11/14 12:54

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

附 件 一

投標廠商聲明書

本廠商參加(臺北醫學大學)招標採購防火牆日誌紀錄器案之投標，茲聲明如下：

項次	聲明事項	是(打V)	否(打V)
一	本廠商之營業項目不符合公司法或商業登記法規定，無法於得標後作為簽約廠商，合法履行契約。		V
二	本廠商有違反政府採購法(以下簡稱採購法)施行細則第 33 條之情形。		V
三	本廠商是採購法第 38 條規定之政黨或與政黨具關係企業關係之廠商。		V
四	本廠商之負責人或合夥人是採購法第 39 條第 2 項所稱同時為規劃、設計、施工或供應廠商之負責人或合夥人。		V
五	本廠商是採購法第 39 條第 3 項所稱與規劃、設計、施工或供應廠商同時為關係企業或同一其他廠商之關係企業。		V
六	本廠商已有或將有採購法第 59 條第 1 項所稱支付他人佣金、比例金、仲介費、後謝金或其他不正利益為條件，促成採購契約之成立之情形。		V
七	本廠商、共同投標廠商或分包廠商是採購法第 103 條第 1 項、採購法施行細則第 38 條第 1 項、人口販運防制法第 41 條所規定之不得參加投標或作為決標對象或分包廠商之廠商。【投標廠商應於投標當日遞送投標文件前至工程會網站 web.pcc.gov.tw 查詢自己(包括總公司及各分公司)、共同投標廠商、分包廠商是否為採購法第 103 條第 1 項之拒絕往來廠商】		V
八	本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人。		V
九	本廠商是依法辦理公司或商業登記且合於中小企業發展條例關於中小企業認定標準之中小企業。(依該認定標準第 2 條，所稱中小企業，指依法辦理公司登記或商業登記，實收資本額在新臺幣 1 億元以下，或經常僱用員工數未滿 200 人之事業。) (答「否」者，請於下列空格填寫得標後預計分包予中小企業之項目及金額，可自備附件填寫) 項目＿＿＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 項目＿＿＿＿＿＿＿＿＿＿＿＿ 金額＿＿＿＿＿＿＿＿ 合計金額＿＿＿＿＿＿＿＿	V	
十	本廠商目前在中華民國境內員工總人數逾 100 人。(依採購法第 98 條及其施行細則第 107 條、108 條規定，得標廠商其於國內員工總人數逾 100 人者，應於履約期間僱用身心障礙者及原住民各不低於總人數百分之一，僱用不足者，除應繳納代金，並不得僱用外籍勞工取代僱用不足額部分。) (答「是」者，請填目前總人數計＿＿人；其中屬於身心障礙人士計＿＿人，原住民計　　人。)		V
十一	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或經濟部投資審議委員會公告之陸資資訊服務業者，不得從事經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」。【上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議委員會網站http://www.moeaic.gov.tw/】【請查察招標文件規定本採購是否屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購】		V
十二	本廠商屬大陸地區廠商、第三地區含陸資成分廠商或在臺陸資廠商，不得從事影響國家安全之採購。【請查察招標文件規定本採購是否屬影響國家安全之採購】		V

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 投標廠商聲明書：(第一次公告) 標號：TMU113-103

十三	本廠商是原住民個人或政府立案之原住民團體。 (答「否」者，請於下列空格填寫得標後預計分包予原住民個人或政府立案之原住民團體之項目及金額，可自備附件填寫。如無，得填寫「0」) 項目＿＿＿＿＿＿＿＿＿＿＿＿ 金額 0 項目＿＿＿＿＿＿＿＿＿＿＿＿ 金額 0 合計金額 0		V

附註	1. 第一項至第七項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象。 2. 本採購如非屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，第八項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；聲明書內容有誤者，不得作為決標對象【違反公職人員利益衝突迴避法第 14 條第 1 項規定者，依同法第 18 條第 1 項處罰】。如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，答「是」、「否」或未答者，均可。 3. 第九項、第十項、第十三項未填者，機關得洽廠商澄清。 4. 本採購如屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，第十一項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 5. 本採購如屬影響國家安全之採購，第十二項答「是」或未答者，不得參加投標；其投標者，不得作為決標對象；如非屬上開採購，答「是」、「否」或未答者，均可。 6. 本聲明書填妥後附於投標文件遞送。 7. 本採購如屬依採購法以公告程序辦理或同法第 105 條辦理之情形者，且本廠商就本採購案，係屬公職人員利益衝突迴避法第 2 條及第 3 條所稱公職人員或其關係人者，請填「公職人員利益衝突迴避法第 14 條第 2 項公職人員及關係人身分關係揭露表」，如未揭露者依公職人員利益衝突迴避法第 18 條第 3 項處罰。
	投標廠商名稱： 泰聲科技股份有限公司
	投標廠商章及負責人章： **日期：** 113, 11, 25

(引用行政院公共工程委員會 113.1.1 版)

電子憑據資料	機關代碼	03724606
	機關名稱	臺北醫學大學
	標案案號	TMU113-103
	公告序號	01
	標案名稱	防火牆日誌紀錄器
	領標電子憑證序號	915000000000002329708
	使用者IP	61.220.23.205

力麗科技
LeaLea Technology

經銷授權證明書

茲證明泰瑩科技股份有限公司為 **Fortinet, Inc.**台灣地區之授權經銷商，可銷售Fortinet系列設備並履行產品之技術及保固責任。

案　　名：防火牆日誌記錄器

案　　號：TMU113-103

設備名稱：FAZ-810G*2

此致

臺北醫學大學

立證明書人：

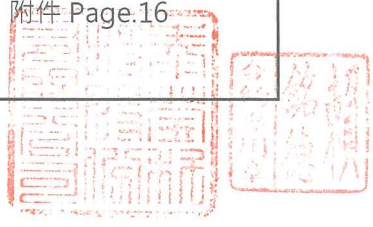
力麗科技股份有限公司

本證明書僅限本採購案專用，若移作其他用途或證明及影本;非經本公司事先書面之認可,本公司一律概不承認。

中　華　民　國　一　一　三　年　十　一　月　十　五　日

設備規格答覆及資料佐證索引

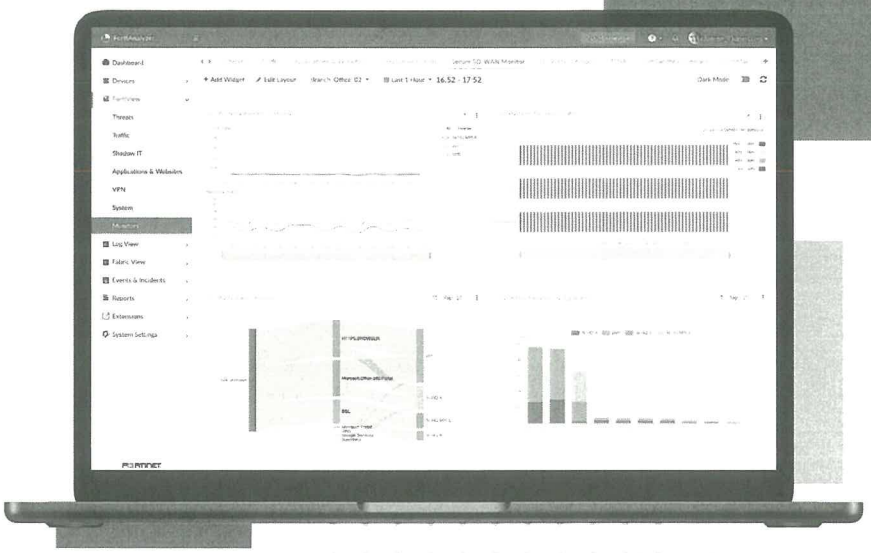
防火牆日誌紀錄器 (FortiAnalyzer-810G)		符合	不符合	佐證資料
1.	獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。	符合		附件 Page.5
2.	系統日誌接收效能可達 6,000 logs/sec (含)以上。	符合		附件 Page.7
3.	系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。	符合		附件 Page.7
4.	系統儲存容量可達 16 TB (含)以上，支援磁碟陣列 RAID 0/1,1s/5,5s/10 規範。	符合		附件 Page.7
5.	具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。	符合		附件 Page.5
6.	具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。	符合		附件 Page.12
7.	具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。	符合		附件 Page.22 附件 Page.23
8.	具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。	符合		附件 Page.13 附件 Page.14 附件 Page.15 附件 Page.17
9.	具備事件監看與告警功能，可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。	符合		附件 Page.18
10	具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。	符合		附件 Page.16
11.	具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。	符合		附件 Page.16



12.	具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。	符合		附件 Page.15 附件 Page.19 附件 Page.20 附件 Page.21
13.	具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服器或 Common Event Format (CEF) 伺服器，以利與既有日誌系統整合。	符合		附件 Page.24
14.	具備管理區域 (Administrative Domain) 分割功能，並可針對不同管理人員賦予不同的管理權限。	符合		附件 Page.25
15.	具備 REST API，以利與既有資安環境整合。	符合		附件 Page.11

FortiAnalyzer™

Security Fabric Network Analytics



Highlights

- Centralized network monitoring and visibility
- Advanced threat and vulnerability detection with event and log data correlation
- Augmented NOC/SOC operations for real-time response, analytics, and reporting
- Automation to save time, reduce errors, and improve efficiency
- Multi-tenancy solution with quota management
- Administrative domains for operational effectiveness and compliance
- 70+ reports and 2000+ ready-to-use datasets, charts, and macros

Analytics, Reports, and Compliance Across the Security Fabric

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

Capabilities

Incident Detection and Response

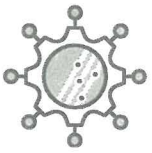
Centralized NOC/SOC Visibility for the Attack Surface

FortiAnalyzer provides Security Fabric Analytics across all device logs with event correlation and real-time detection of Advanced Persistent Threats (APTs), vulnerabilities and Indicators of Compromise (IOC) for FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail and other Fortinet products, for deep visibility and critical network insights. Simplified orchestration and automated workflows provide Network Security Operations teams with real-time notifications, reports, and dashboards for single-pane visibility and actionable results.

Incidents and Events Management

Security teams can monitor and manage alerts and event logs from Fortinet devices, with events processed and correlated in a format that analysts can easily understand. Investigate suspicious traffic patterns and search using filters in predefined or custom event handlers to generate real-time notifications and monitoring for NOC and SOC operations, SD-WAN, SSL VPN, wireless, Shadow IT, IPS, network recon, FortiClient, and more.

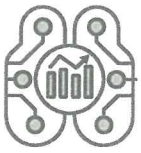
The Incidents component enables analysts to manage incident handling and life cycle, with incidents generated by events that show affected assets, endpoints, users and timelines.



Fabric Automation

FortiAnalyzer Playbooks boost an organization's security team abilities to simplify investigation efforts through automated incident response, freeing up resources and allowing analysts to focus on critical tasks. Out-of-the-box playbook templates enable SOC analysts to quickly customize their use cases, define custom processes, interact with other Security Fabric devices like FortiOS and EMS, edit playbooks and tasks in the visual playbook editor and use the Playbook Monitor for investigation of compromised hosts, infections and critical incidents, data enrichment for Assets and Identity views, blocking malware, C&C IPs, and more.

Security Fabric Analytics



Analytics and Reporting

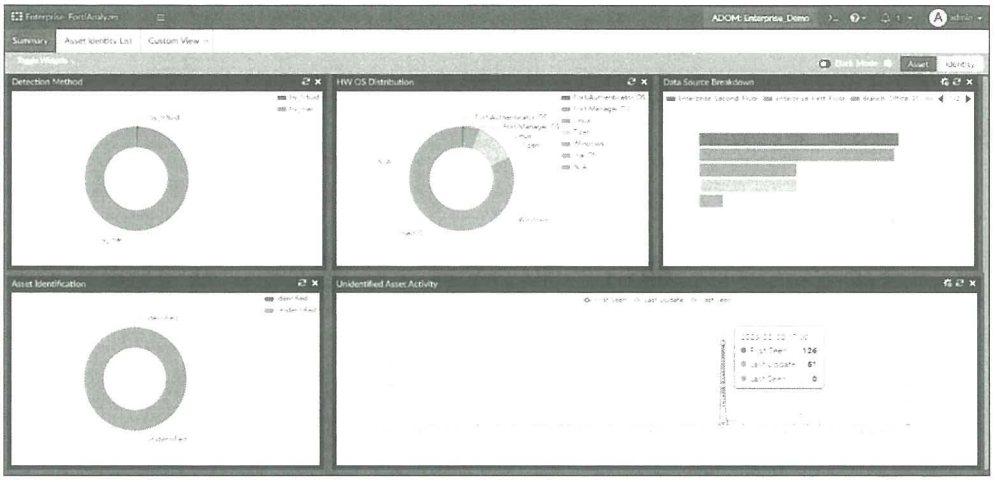
FortiAnalyzer automation driven analytics empowers network security operations teams to complete a fast assessment of network devices, systems, and users, with correlated log data and FortiGuard threat intelligence for analysis of real-time and historical events.

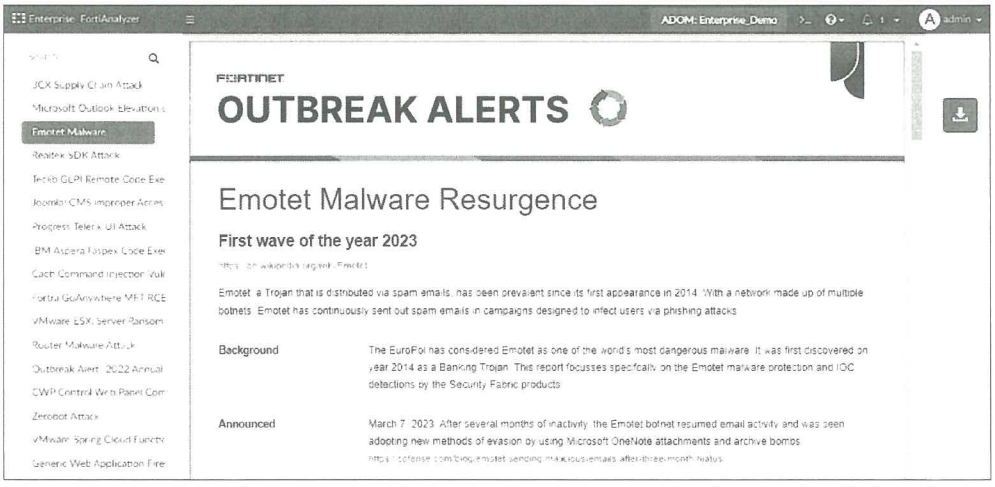
- **FortiView** Monitors and Views provide deep insights with context and meaning of network activity, risks, vulnerabilities, attack attempts, indicators of compromise and anomalies, sanctioned and unsanctioned user activity.
- **Log View** enables analysts to expand their investigation and utilize search filters on managed device logs, drill down on logs, with custom views and log groups, including a SIEM database with normalized logs for Fortinet devices in Fabric ADOMs.
- **Reports** provide comprehensive analysis of your Security Posture, including reports for Operational Technology (OT), security rating, security rating for PCI, Secure SD-WAN, VPN, FortiNDR network anomaly detection, cyber threat assessments, 360 Security Reviews, situational awareness, compliance, auditing, and more.

Capabilities

Assets and Identity

FortiAnalyzer Fabric View with Assets and Identity monitoring provides SOC teams with elevated awareness and visibility into an organization's endpoints and users with dashboards and correlated device and UEBA information, vulnerability detections, EMS tagging, and asset classifications through telemetry with EMS, NAC, Fortinet Fabric Agent, and an OT Dashboard View.





Subscriptions and Extensions

Subscription Licenses and FortiGuard Security Services

- **FortiGuard Outbreak Detection Service** delivers automated content package download for detecting the latest malware, including a summary of outbreaks and kill chain mapping for how the malware works. The package includes a FortiGuard Report for the outbreak, Event Handler, and a Report Template to detect outbreaks.
- **FortiGuard Indicators of Compromise Service** empowers security teams with forensic data from 500 000 IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system, that have been determined with high confidence to be malicious infections or intrusions, and historical rescan of logs for threat hunting.
- **Shadow IT Monitoring Service** provides continuous monitoring of unapproved devices, resources, unsanctioned accounts and unauthorized use of SaaS and IaaS, API integration, and third party apps. The service identifies rogue users using personal accounts for managing company assets, using correlated FortiOS and FortiCASB data with a FortiCASB account subscribed for SaaS features.
- **OT Security Service** provides security teams with advanced OT analytics, risk and compliance reports, OT event handlers, and use-case correlation rules.
- **Security Rating and Compliance Service** helps security teams design, implement, and maintain their security posture, and provides actionable configuration recommendations as well as key performance and risk indicators.
- **Security Automation Service** subscription enables further automation for incident response with enhanced monitoring and escalation, built-in incident management workflows, connectors, playbooks and more.

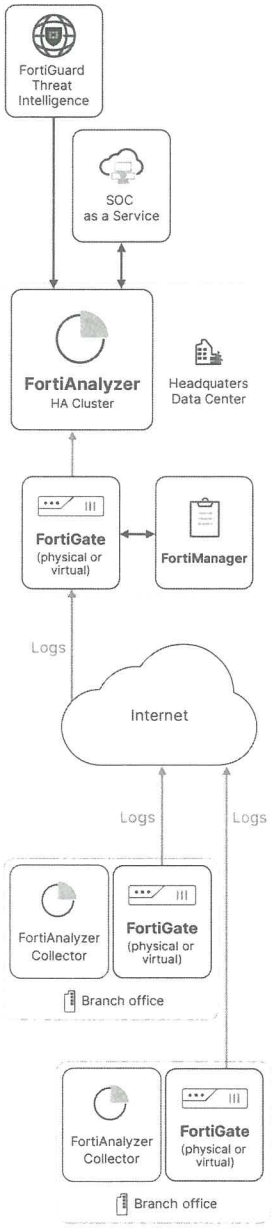
Management Extension Applications (MEAs)

The Management Extensions pane allows you to enable licensed applications that are released and signed by Fortinet, which can be installed and run on FortiAnalyzer, including the FortiSIEM and FortiSOAR.

Deployments

Deploying FortiAnalyzer

FortiAnalyzer can be deployed as a physical hardware appliance, virtual machine (VM) and virtual machine subscription (VM-S), as well as private or public cloud instance, with scalability, redundancy and backup, and high availability capabilities.



FortiAnalyzer High Availability (HA)

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

Multi-Tenancy with Flexible Quota Management

FortiAnalyzer provides the ability to manage multiple sub-accounts with each account having its own administrators and users. The time-based archive/analytic log data policy, per Administrative Domain (ADOM), allows automated quota management based on the defined policy, with trending graphs to guide policy configuration and usage monitoring.

Analyzer Collector Modes

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

FortiAnalyzer Fabric

FortiAnalyzer Fabric allows SOC Administrators to configure two operation modes - Supervisor and Member. This allows viewing of member devices, ADOMs and authorized logging devices, as well as incidents and events created on members. Admins get access to Reports and FortiView across all member FortiAnalyzers, and can perform global search in Log View of logs collected across FortiAnalyzer Fabric members with pre-defined device filters and log drill down for each Member and Member ADOMs.

Log Forwarding for Third-Party Integration

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

Cloud Services

FortiAnalyzer Cloud

FortiAnalyzer Cloud offers customers a PaaS-based delivery option for automation-driven, single pane analytics, providing log management, analytics, and reporting for Fortinet NGFW and SD-WAN with an easily accessible cloud-based solution. FortiAnalyzer Cloud delivers reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture. Customers can easily access their FortiAnalyzer Cloud from their FortiCloud single sign-on portal.

Virtual Offerings

FortiAnalyzer VM Subscription

The FortiAnalyzer VM Subscription license model consolidates into one single SKU: VM product SKU, FortiCare Support SKU, FortiGuard IOC and Outbreak Detection Service, Security Automation services, to simplify the product purchase, upgrade, and renewal. FortiAnalyzer-VM S provides organizations with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet and third party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer-VM S series SKUs come in stackable 5, 50, and 500 GB/ day logs licenses, so that multiple units of this SKU can be purchased together providing organizations with the ability and cost-efficiencies to scale and meet their logging needs.

FortiAnalyzer VM

Fortinet offers the FortiAnalyzer-VM licensing in a stackable perpetual license model with a-la-carte technical support and subscription services.

This software-based version of the FortiAnalyzer hardware appliance is designed to run on many virtualization platforms, which allows you to expand your virtual solution as your environment expands.

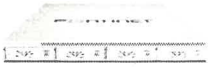
FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity						
GB/ day of Logs *	+1	+5	+25	+100	+500	+2000
Devices/VDOMs Maximum	10 000	10 000	10 000	10 000	10 000	10 000
FortiGuard IOC Service			✓			
Security Automation Service			✓			
Hypervisor Support	Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit https://docs.fortinet.com/product/fortianalyzer/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"					
vCPU Support (Minimum / Maximum)	4 / Unlimited					
Network Interface Support (Min / Max) **	1 / 12					
Memory Support (Minimum / Maximum)	16 GB / Unlimited for 64-bit					

* Unlimited GB/ day when deployed in collector mode.

** VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

Specifications






FORTIANALYZER APPLIANCES	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000G
Capacity and Performance				
GB/ day of Logs	25	100	200	660
Analytic Sustained Rate (logs/ sec)*	500	2000	4000	20 000
Collector Sustained Rate (logs/ sec)*	750	3000	6000	30 000
Devices/VDOMs (Maximum)	50	180	800	2000
Max Number of Days Analytics**	90	50	50	60
Options				
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓	✓
Security Automation Service	✓	✓	✓	✓
Enterprise Bundle	✓	✓	✓	✓
Hardware Bundle	✓	✓	✓	✓
OT Security Service	✓	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓	✓
Hardware Specifications				
Form Factor (supports EIA/non-EIA standards)	Desktop	1 RU Rackmount	1 RU Rackmount	2 RU Rackmount
Total Interfaces	2x RJ45 GE	4x RJ45 GE	4x RJ-45 2x GE SFP	2× 2.5GbE RJ45 + 2× 25GbE SFP28
Storage Capacity	4TB (2× 2TB)	8 TB (2× 4 TB)	16TB (4× 4TB) 3.5 in SAS HDDs	32 TB (8 × 4TB) 3.5 in SAS SED HDD
Usable Storage (After RAID)	2 TB	4 TB	8 TB	24 TB
Removable Hard Drives	No	No	✓	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10	RAID 0/1/5/6/10/50/60
RAID Type	Software	Software	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	1	1	10	50
Redundant Hot Swap Power Supplies	No	Optional	Optional	✓
Trusted Platform Module (TPM) ***	Gen 2	Gen 2	✓	✓
Dimensions				
Height x Width x Length (inches)	9.5 × 3.5 × 8	1.73 × 17.24 × 16.38	1.73 × 17.32 × 21.65	3.46 × 17.24 × 24.41
Height x Width x Length (cm)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	4.4 × 44.0 × 55.0	8.8 × 43.8 × 62.0
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	25.75 lbs (11.68 kg)	49.6 lbs (22.5 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100-240Vac, 50~60Hz, 4A max	100-240Vac, 50~60Hz, 4A max
Power Consumption (Average / Maximum)	36 W / 43 W	90.1 W / 99 W	115W / 150W	251.36W / 302W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	433 BTU/h	857.73 BTU/h
Operating Temperature	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)
Storage Temperature	-4°F to 167° F (-20°C to 75° C)	-13°F to 167° F (-25°C to 75° C)	-4°F to 167° F (-20°C to 75° C)	-40°F to 158° F (-40°C to 70° C)
Humidity	5% to 95% non-condensing	20% to 90% non-condensing	5% to 95% non-condensing	5% to 95% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 16 404 ft (5000 m)
Compliance				
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

Specifications



FORTIANALYZER APPLIANCES	FAZ-3100G	FAZ-3510G	FAZ-3700G
Capacity and Performance			
GB/ day of Logs	3000	5000	8300
Analytic Sustained Rate (logs/sec)*	42 000	60 000	100 000
Collector Sustained Rate (logs/sec)*	60 000	90 000	150 000
Devices/VDOMs (Maximum)	4000	10 000	10 000
Max Number of Days Analytics**	30	35	60
Options			
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓
Security Automation Service	✓	✓	✓
Enterprise Bundle	✓	✓	✓
Hardware Bundle	✓	✓	✓
OT Security Service	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓
Hardware Specifications			
Form Factor (supports EIA/non-EIA standards)	3 RU Rackmount	4 RU Rackmount	4 RU Rackmount
Total Interfaces	2x GE RJ45, 2× 25GE SFP28	2× 10GbE RJ45, 2× 25GbE SFP28	2× 10GE RJ-45 + 2× 25GE SFP28
Storage Capacity	64 TB (16 × 4TB) 3.5" SAS SED HDD + 3.84 (2× 1.92TB) 2.5" NVMe SSD	24× 4TB (96TB) + 2× 3.84TB (7.68TB)	240TB (60× 4TB) 3.5 in HDD + 19.2TB (6× 3.2TB) NVMe SSD
Usable Storage (After RAID)	56 TB	84 TB	224 TB
Removable Hard Drives	✓	✓	✓
RAID Levels Supported	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60
RAID Type	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	50	50	50
Redundant Hot Swap Power Supplies	✓	✓	✓
Trusted Platform Module (TPM) ***	✓	✓	✓
Dimensions			
Height x Width x Length (inches)	5.2 × 17.2 × 25.5	7 × 17.2 × 27.5	7.0 × 17.2 × 30.2
Height x Width x Length (cm)	13.0 × 44.0 × 65.0	17.8 × 43.7 × 69.9	17.8 × 43.7 × 76.7
Weight	69.6 lbs (31.57 kg)	65 lbs (29.5 kg)	118 lbs (53.5 kg)
Environment			
AC Power Supply	100-127V~/10A, 200-240V~/5A	100-127V~/10A, 200-240V~/5A	2000W AC****
Power Consumption (Average/Max)	395 W / 510 W	983 W / 1278 W	850 W / 1423.4 W
Heat Dissipation	1740.19 BTU/h	3424 BTU/h	4858 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	50°F to 95°F (10°C to 35°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)	-4°F to 167°F (-20°C to 75°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	5% to 95% (non-condensing)	5% to 95% (non-condensing)	8% to 90% (non-condensing)
Forced Airflow	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 13 123 ft (4000 m)	Up to 10 000 ft (3048 m)	Up to 7400 ft (2250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

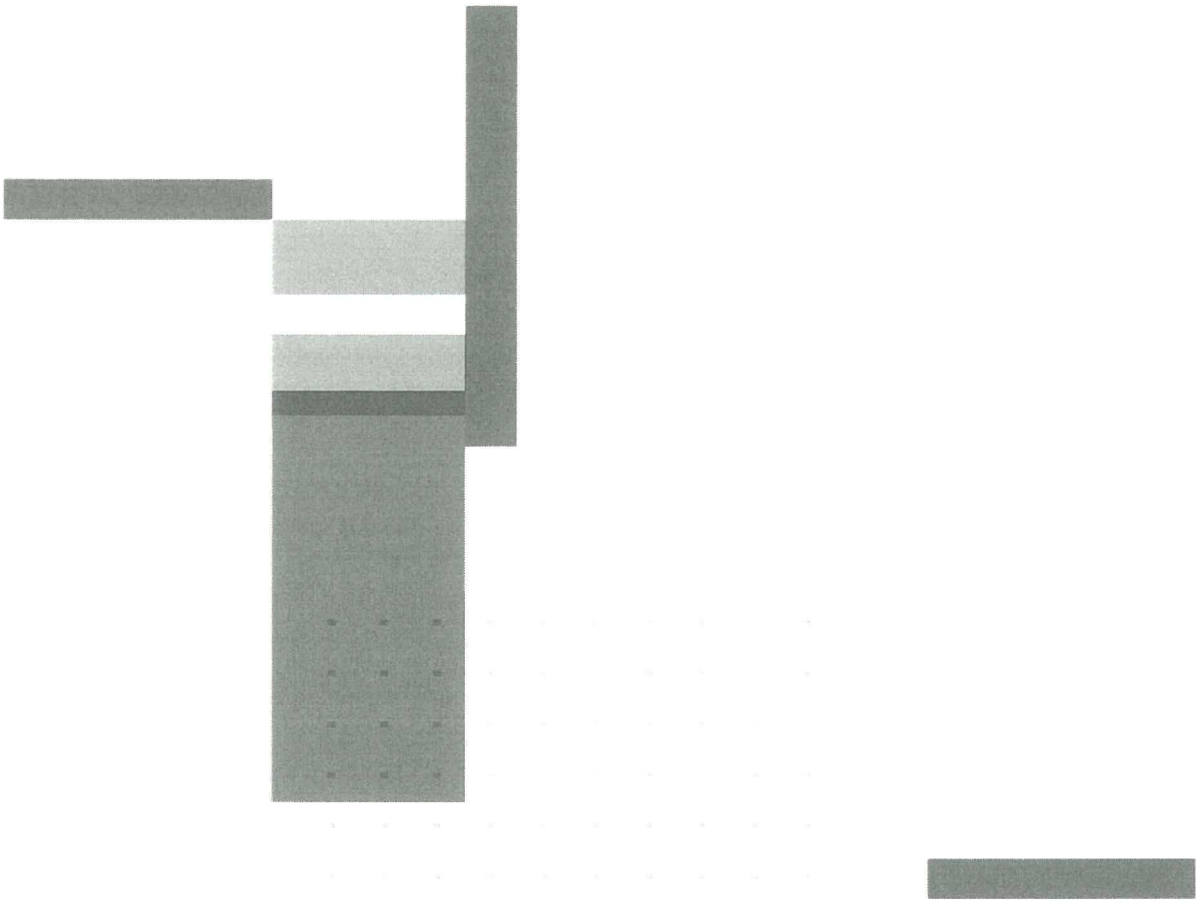
****3700G must connect to a 200V - 240V power source.

Ordering Information

Product	SKU	Description
FortiAnalyzer	FAZ-150G	Centralized log and analysis appliance — 2x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.
	FAZ-300G	Centralized log and analysis appliance — 4x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.
	FAZ-810G	Centralized log and analysis appliance — 4x GE, 2x SFP, 16 TB self-encrypting storage, up to 200 GB/ day of logs.
	FAZ-1000G	Centralized logging and analysis appliance - 2× 2.5GbE RJ45 + 2× 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs.
	FAZ-3100G	Centralized log and analysis appliance — 2x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3000 GB/ day of logs.
	FAZ-3510G	Centralized log and analysis appliance — 2× 10GbE RJ45, 2× 25GbE SFP28, 96 TB storage, up to 5000 GB/ day of logs.
	FAZ-3700G	Centralized log and analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 240TB HDD + 19.2TB NVMe SSD storage, up to 8300 GB/ day of Logs.
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-465-01-DD	Subscription license for 5 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC2-10-AZVMS-465-01-DD	Subscription license for 50 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC3-10-AZVMS-465-01-DD	Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
FortiAnalyzer-VM	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of Logs.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs.
FortiAnalyzer Cloud Storage Subscription	FC1-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
	FC2-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
	FC3-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
FortiAnalyzer - Backup to Cloud Service	FC-10-FAZ00-286-02-DD	One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.
FortiAnalyzer Cloud with SOCaaS	FC-10-[Model Code]-464-02-DD	FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.
FortiAnalyzer Cloud	FC-10-[Model Code]-585-02-DD	FortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service.
Security Automation Service	FC-10-[Model Code]-335-02-DD	Subscription license for Security Automation Service - Appliance.
	FC[GB Day Code]-10-LV0VM-335-02-DD	Subscription license for Security Automation Service - Virtual Machine.
FortiGuard IOC and Outbreak Detection Service	FC-10-[Model Code]-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.
	FC[GB Day Code]-10-LV0VM-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.
OT Security Service	FC-10-[Model Code]-159-02-DD	OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules.
FortiAnalyzer Security Rating and Compliance Service	FC-10-[Model Code]-175-02-DD	Subscription license for FortiAnalyzer Security Rating and Compliance Service.
Enterprise Protection Bundle	FC-10-[Model Code]-466-02-DD	Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).
Hardware Bundle	FAZ-[Hardware Model]-BDL-466-DD	Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Avatars

When FortiClient sends logs to FortiAnalyzer, an avatar for each user can be displayed in the *Source* column in the *FortiView* and *Log View* panes. FortiAnalyzer can display an avatar when FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiAnalyzer enabled.

— 、15

- When FortiClient Telemetry connects to FortiGate, FortiClient sends logs (including avatars) to FortiGate, and the logs display in FortiAnalyzer under the FortiGate device as a sub-type of security.
  The avatar is synchronized from FortiGate to FortiAnalyzer by using the FortiOS REST API.
- When FortiClient Telemetry connects to FortiClient EMS, FortiClient sends logs (including avatars) directly to FortiAnalyzer, and logs display in a FortiClient ADOM.

If FortiAnalyzer cannot find the defined picture, a generic, gray avatar is displayed.

You can also optionally define an avatar for FortiAnalyzer administrators. See Creating administrators on page 351.

Showing and hiding passwords

In some cases you can show and hide passwords by using the toggle icon. When you can view the password, the *Toggle show password* icon is displayed:

When you can hide the password, the *Toggle hide password* icon is displayed:

Target audience and access level

This guide is intended for administrators with full privileges, who can access all panes in the FortiAnalyzer GUI, including the *System Settings* pane.

In FortiAnalyzer, administrator privileges are controlled by administrator profiles. Administrators who are assigned profiles with limited privileges might be unable to view some panes in the GUI and might be unable to perform some tasks described in this guide. For more information about administrator profiles, see Administrator profiles on page 358.

If you logged in by using the `admin` administrator account, you have the *Super_User* administrator profile, which is assigned to the *admin* account by default and gives the `admin` administrator full privileges.

Initial setup

This topic provides an overview of the tasks that you need to do to get your FortiAnalyzer unit up and running.

ADOMs must be enabled to support FortiCarrier, FortiClient EMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox logging and reporting. See Administrative Domains (ADOMs) on page 296.

Logs

Logs in FortiAnalyzer are in one of the following phases.

- Real-time log: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file.
- Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline.
- Analytics logs or historical logs: Indexed in the SQL database and online.

In order for FortiAnalyzer to accept logs, the sending device must be registered in FortiAnalyzer. You can add devices to FortiAnalyzer by specifying the serial number and other details, or you may point the device's log settings to the FortiAnalyzer. If initiated by the remote device, the device must be authorized before logs can be received on FortiAnalyzer. See Adding devices on page 41.

For more information on the types of logs collected for each device, see Types of logs collected for each device on page 88.

Log encryption 一、6

Beginning in FortiAnalyzer 6.2, all logs from Fortinet devices (using Fortinet's proprietary protocol: OFTP) must be encrypted. FortiAnalyzer encryption level must be equal or less than the sending device's level. For example, when configuring logging from a FortiGate, FortiAnalyzer must have the same encryption level or lower than FortiGate in order to accept logs from FortiGate.

To configure the encryption level on FortiAnalyzer:

1. In the FortiAnalyzer CLI, enter the following commands:

```
config system global
    set enc-algorithm {high | low | medium}
```

To configure the encryption level on FortiGate:

1. In the FortiGate CLI, enter the following commands:

```
config log fortianalyzer setting
    set enc-algorithm {high-medium | high | low}
```

See also Appendix B - Log Integrity and Secure Log Transfer on page 405.

Log storage

Logs and files are stored on the FortiAnalyzer disks. Logs are also temporarily stored in the SQL database.

FortiView dashboards for FortiGate and FortiCarrier devices

Category	View	Description
Threats	Top Threats	Lists the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus.
	Threat Map	Displays a map of the world that shows the top traffic destinations starting at the country of origin. Threats are displayed when the threat score is greater than zero and either the source or destination IP is a public IP address. The *Threat Window* below the map, shows the threat, source, destination, severity, and time. The color gradient of the lines indicate the traffic risk. A yellow line indicates a high risk and a red line indicates a critical risk. This view does not support filtering and *Day*, *Night*, and *Ocean* themes. See also Viewing the threat map on page 58.
	Compromised Hosts	Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats. To use this feature: 1. UTM logs of the connected FortiGate devices must be enabled. 2. The FortiAnalyzer must subscribe to FortiGuard to keep its threat database up-to-date.
	FortiSandbox Detection	Displays a summary of FortiSandbox related detections. The following information is displayed: Filename, End User and/or IP, Destination IP, Analysis (Clean, Suspicious or Malicious rating), Action (Passthrough, Blocked, etc.), and Service (HTTP, FTP, SMTP, etc.). Select an entry to view additional information in the drilldown menu. Clicking a FortiSandbox action listed in the *Process Flow* displays details about that action, including the *Overview*, *Indicators*, *Behavior Chronology Chart*, *Tree View*, and more. Information included in the *Details* and *Tree View* tab is only available with FortiSandbox 3.1.0 and above.

Category	View	Description
Traffic	Top Sources	Displays the highest network traffic by source IP address and interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Source Addresses	Displays the top source addresses by source object, interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Destinations	Displays the highest network traffic by destination IP addresses, the applications used to access the destination, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Destination Addresses	Displays the top destination addresses by destination objects, applications, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Country/Region	Displays the highest network traffic by country in terms of traffic sessions, including the destination, threat score, sessions, and bytes.
	Policy Hits	Lists the policy sessions by policy, device name, VDOM, number of hits, bytes, and last used time and date.
	DNS Logs	Summarizes the DNS activity on the network. Double click an entry to drill down to the specific details about that domain.
	ZTNA Servers	ZTNA servers by bytes.
Shadow IT	Top Cloud Applications	Displays the top cloud applications used on the network. When viewing information about an application, FortiAnalyzer will first check the Shadow IT database, and if no results are found, it will use the metadata.
	Top Cloud Users	Displays the top cloud users on the network.
Applications & Websites	Top Applications	Displays the top applications used on the network including the application name, category, risk level, and sessions blocked and allowed. Bytes sent and received can also be enabled through the widget settings. Top Applications can be viewed as a stackbar, bar, table, or bubble chart. For a usage example, see Finding application and user information on page 68.
	Top Website Domains	Displays the top allowed and blocked website domains on the network.
	Top Website Categories	Displays the top website categories.
	Top Browsing Users	Displays the top web-browsing users, including source, group, number of sites visited, browsing time, and number of bytes sent and received.

Category	View	Description
VPN	SSL & Dialup IPsec	Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec). You can view VPN traffic for a specific user from the top view and drilldown views. In the top view, double-click a user to view the VPN traffic for the specific user. In the drilldown view, click an entry from the table to display the traffic logs that match the VPN user and the destination.
	Site-to-Site IPsec	Displays the names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network.
System	Admin Logins	Displays the users who logged into the managed device.
	System Events	Displays events on the managed device.
	Resource Usage	Displays device CPU, memory, logging, and other performance information for the managed device. Resource Usage includes two widgets: *Resource Usage Average* and *Resource Usage Peak*.
	Failed Authentication Attempts	Displays the IP addresses of the users who failed to log into the managed device.

Using FortiView

When ADOMs are enabled, *FortiView* displays information for each ADOM. Please ensure you are in the correct ADOM. See Switching between ADOMs on page 26.

Viewing FortiView dashboards

When viewing FortiView dashboards, use the controls in the toolbar to select a device, specify a time period, refresh the view, and switch to full-screen mode.

Many widgets on FortiView dashboards let you drill down to view more details. To drill down to view more details, click, double-click, or right-click an element to view details about different dimensions in different tabs. You can continue to drill down by double-clicking an entry. Click the close icon in the widget's toolbar to return to the previous view.

Many FortiView widgets support multiple chart types such as table view, bubble view, map view, tile view, etc.

- In widgets that support multiple views, select the settings icon in the top-right corner of the widget to choose another view.

SD-WAN Bandwidth Overview	The bandwidth of the SD-WAN network over time. This widget displays a line chart of the sent/received rate (bps) in the selected time period for SD-WAN members interfaces.
SD-WAN Performance Status	The SD-WAN performance status comparison with interfaces. Mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check. Click on a scatter chart to view additional details.
SD-WAN Rules Utilization	The SD-WAN rule traffic utilization by interface and application.
SD-WAN Utilization by Application	The share of bandwidth utilization by application for each WAN link.
Top SD-WAN SLA Issues	The top SD-WAN SLA issues.
Health Check Status	This widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.
SD-WAN Events	This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.
Application Bandwidth Utilization	The total bandwidth from all applications as well as the bandwidth per-SD-WAN interface. This widget can be viewed in a sanky chart or table chart format.
Per-Application Performance	The performance for the selected application based on chosen metric. You can select an application in the widget's *Application* dropdown menu. *Latency*, *Jitter*, *Packet Loss*, and *Bandwidth* metrics are available.
Global-Application Performance	The global application performance for the selected metric. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
SD-WAN Interfaces	The information for SD-WAN interfaces and ADVPN shortcut interfaces. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
Audio MOS Score	The MOS score by interface. Mousing over the chart displays a summary of the MOS score and VoIP quality at that point. The interface must have a performance SLA with MOS enabled to display in the chart.

To update the *Refresh Interval*, click the settings icon at the top of the widget, and then select a value from the dropdown.

To filter a chart, click a key in the legend.

SD-WAN Summary

SD-WAN Summary monitor includes the following widgets:

SD-WAN Health Overview	The SD-WAN devices' status.

device(s) and time frame for the event logs.

The *Total Events* widget on this dashboard displays a line chart of event logs by level. You can hover your cursor over the line chart to display a summary of the count and time at that point.

The other widgets on this dashboard list the event names for the displayed event types. These widgets can be toggled on/off from the *Toggle Widgets* dropdown. By clicking an event name in the widget, you can open a list view of those event logs filtered by the devices and time frame you selected on the dashboard.

Viewing historical and real-time logs

By default, *Log View* displays historical logs. *Custom View* and *Chart Builder* are only available in historical log view.

To view real-time logs, in the log message list view toolbar, click *Tools* > *Real-time Log*.

To switch back to historical log view, click *Tools* > *Historical Log*.

Viewing raw and formatted logs

By default, *Log View* displays formatted logs. The log view you select affects available view options. You cannot customize columns when viewing raw logs.

To view raw logs, in the log message list view toolbar, click *Tools* > *Display Raw*.

To switch back to formatted log view, click *Tools* > *Formatted Log*.

For more information about FortiGate raw logs, see the *FortiGate Log Message Reference* in the Fortinet Document Library. For more information about raw logs of other devices, see the *Log Message Reference* for the platform type.

Option	Description
	• *Match Criteria*: Select an operator from the dropdown. • *Value*: Select the event type from the dropdown. To delete a condition, click the *delete* icon next to the condition.
Generic Text Filter	(Optional) Enter a filter string. For more information, see Using the Generic Text Filter on page 177.

Creating notification profiles

Notification profiles are used to send alert notifications when an event is generated by an event handler. You can configure the notification profile to send the alert to an email address, SNMP community, and/or syslog server. You can also configure the notification profile to send the alert through a fabric connector.

You can create, edit, clone, and delete notification profiles in *FortiSoC/Incidents & Events* > *Handlers* > *Notification Profile List*.

To assign a notification profile to a basic event handler, see Creating a custom event handler on page 168.

To assign a notification profile to a correlation handler, see Creating a custom correlation handler on page 171.

To create a notification profile:

1. Go to *FortiSoC/Incidents & Events* > *Handlers* > *Notification Profile List*.
2. Click *Create New*.
   The *Add New Notification Profile* pane displays.
3. Configure the following options, and click *OK* to save the notification profile.

Option	Description
Name	Enter a name for the notification profile.
Send Alert through Fabric Connectors	Send an alert through one or more fabric connectors selected from the dropdown. Click the plus (+) to add fabric connectors. For more information, see Fabric Connectors on page 112.
Send Alert Email	Send an alert to one or more email addresses. Specify the email parameters, including the mail server. For more information, see Mail Server on page 333.
To	Enter the email address(es) to send the alert to. Use a semicolon (;) to separate multiple email addresses.
From	Enter a from address for the alert email.
Subject	Enter a subject line for the alert email.
Email Server	Select the mail server for the alert email.
Send SNMP(...) Trap	Send an alert to an SNMP community or user selected from the dropdown. For more information, see SNMP on page 324.

FortiSoC

FortiSoC is a subscription service that enables playbook automation for security operations on FortiAnalyzer.

FortiAnalyzer's SIEM capabilities parse, normalize, and correlate logs from Fortinet products and the security event log of Windows and Linux hosts (with Fabric Agent integration). Parsing is predefined by FortiAnalyzer and does not require manual configuration by administrators. SIEM logs are displayed as *Fabric logs* in *Log View* and can be used when generating reports. See Types of logs collected for each device on page 88.

FortiSoC provides incident management capabilities with playbook automation to accelerate incident response. When FortiAnalyzer has a valid subscription license, the FortiSoC module is activated and administrators are able access playbook automation features. Task automation can be configured by SOC analysts using playbooks which consist of a trigger and sequence of automated actions. Playbooks can be created from scratch or by using one of the predefined templates. Fabric connectors further enhance FortiSoC functionality by allowing playbooks to perform tasks using connected devices, including FortiOS and FortiClient EMS.

FortiSoC includes a trial with a limited capacity allowing up to five playbooks per day. A SOC subscription is required to run at full capacity. For additional information about licensing, please see support.fortinet.com.

For information about FortiSoC incidents and events, see Incident and Event Management on page 135.

Viewing FortiSoC dashboards

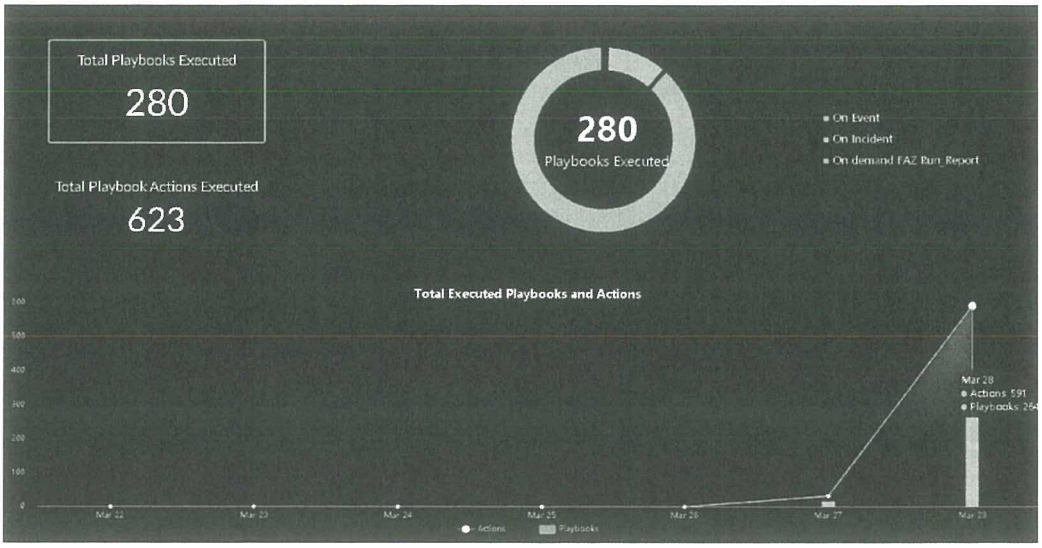
FortiSoC includes multiple dashboards for viewing information about playbooks, incidents, and events.

There is a toolbar available for each dashboard, providing the following options:

Dark Mode	Enable/disable dark mode. Dark mode shows a black background for the dashboard.
Refresh	From the *Refresh* dropdown in the toolbar, you can select a frequency for the dashboard to automatically refresh the information. If you need to manually refresh the dashboard before it is done automatically, click *Refresh* in the toolbar. By default, the refresh frequency is set to *Manual Refresh*. Click *Refresh* in the toolbar to refresh the dashboard when needed.

Playbooks

一、12

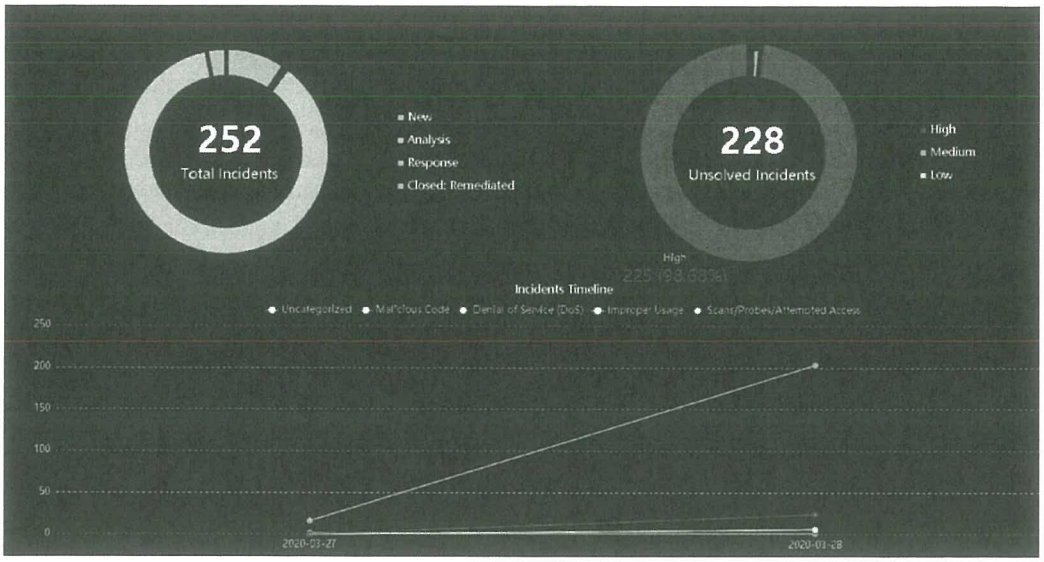


The *Playbooks* dashboard includes:

Total Playbooks Executed	The total number of playbooks executed.
Total Playbook Actions Executed	The total number of playbook actions (tasks) executed.
Playbooks Executed	The number of times each playbook has been run.
Overall Time Saved	The estimated time saved by administrators resulting from FortiSoC automation.
Total Executed Playbooks and Actions	A timeline of the number of playbooks and actions run for each day. Both actions and playbooks can be toggled on or off in the graph by clicking the corresponding name below the graph.

Incidents

一、12

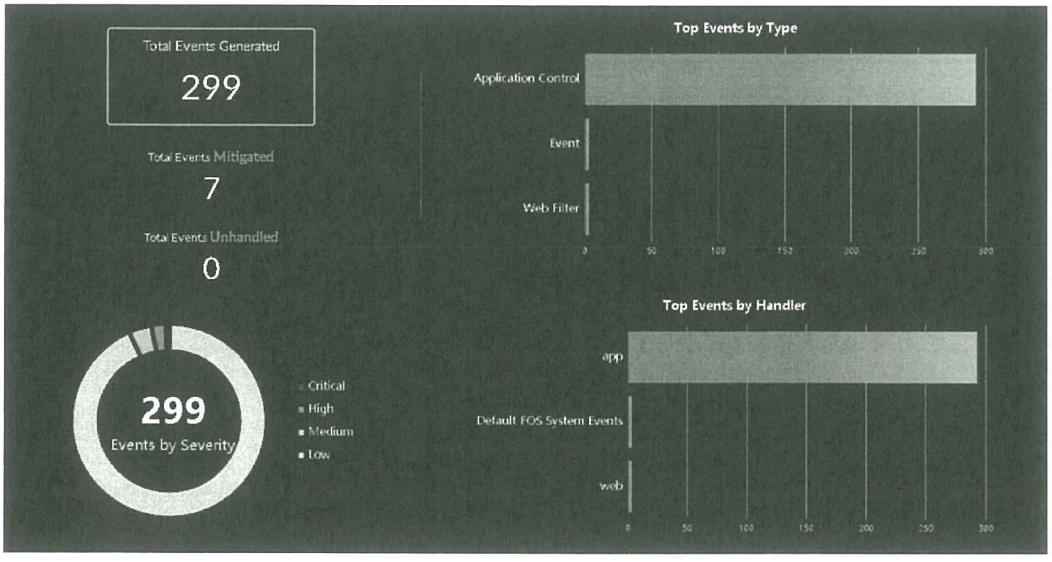


The *Incidents* dashboard includes:

Total Incidents	Displays the total number of incidents created by their status.
Unsolved Incidents	Displays the total number of unsolved (not closed) incidents by severity.
Incidents Timeline	Total incidents breakdown by category trend by day.

Events

一、12



The *Events* dashboard includes:

Outbreak Alerts

The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows FortiAnalyzer administrators to view outbreak alerts and automatically download related event handlers and reports from FortiGuard.

When FortiAnalyzer has a valid license for the Outbreak Detection Service, outbreak alerts from Fortinet are displayed in the *FortiSoC* > *Outbreak Alerts* pane. Outbreak alerts can be viewed from any ADOM. You can navigate between outbreak alerts by clicking on the corresponding tab at the top of the pane, and click the download icon to download a copy of the outbreak alert.

Outbreak event handlers and reports are created in real-time by Fortinet to detect and respond to emerging outbreaks. Outbreak reports and event handlers are automatically downloaded so that they are available in your environment. See Viewing imported event handlers and reports on page 212.

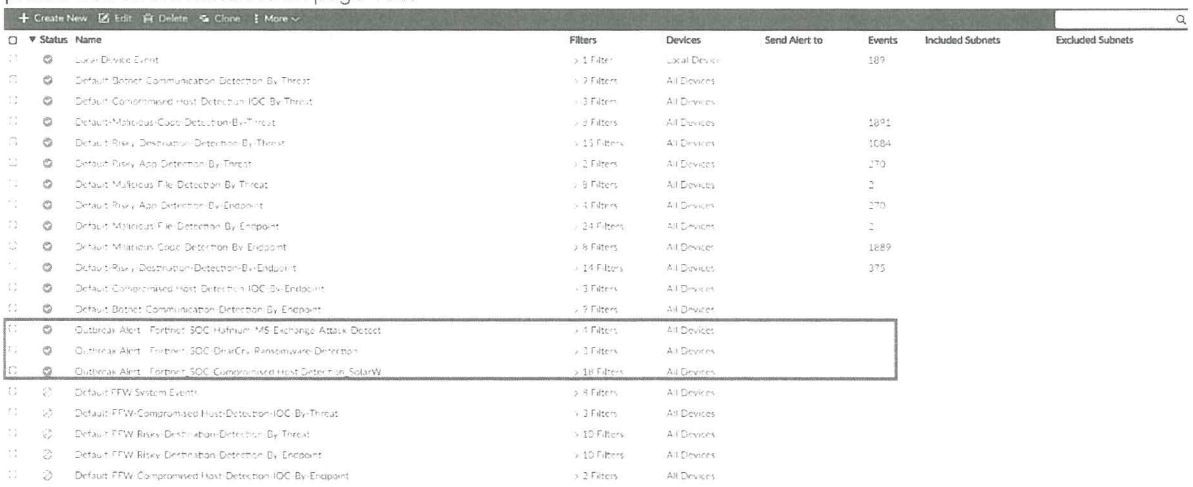
Without a valid license for the Outbreak Detection Service, *Outbreak Alerts* displays a default alert page, and outbreak event handlers and reports are not available from FortiGuard. To obtain a valid license for FortiAnalyzer Outbreak Detection Service, contact Fortinet FortiCare.

Viewing imported event handlers and reports

With a valid license, the FortiAnalyzer Outbreak Detection Service automatically downloads event handlers and reports created by Fortinet in response to known outbreaks. This section includes information on how to view downloaded outbreak event handlers and reports.

To view outbreak event handlers and reports:

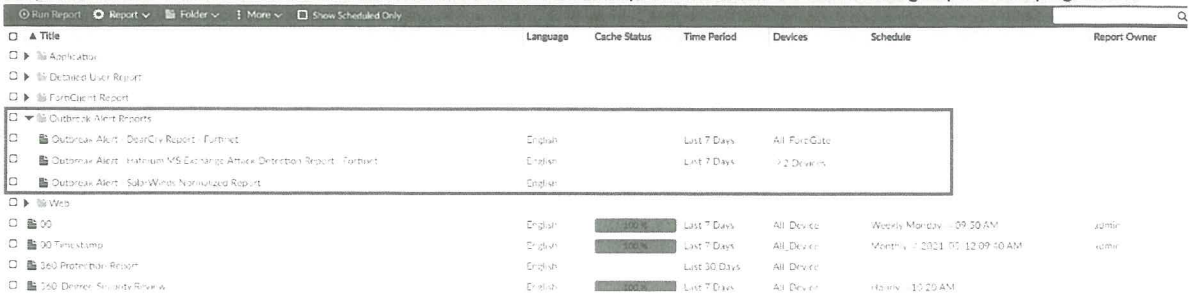
1. Go to *FortiSoC* > *Handlers* > *Event Handler List*.
   Event handlers created by the FortiAnalyzer Outbreak Detection Service are displayed with the Outbreak Alert prefix. See Event handlers on page 135.



2. Go to *Reports* > *All Reports*.
   The *Outbreak Alert Reports* folder includes available reports from the FortiAnalyzer Outbreak Detection Service.

— 、7

Reports can be run in HTML, PDF, XML, CSV, and JSON output formats. See Generating reports on page 215.



Viewing a CRL

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *Result* page opens.
4. Click *OK* to return to the CRL list.

Deleting a CRL

To delete a CRL or CRLs:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL or CRLs you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

Log Forwarding

— 、13

You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server when you use the default forwarding mode in log forwarding.

The *client* is the FortiAnalyzer unit that forwards logs to another device. The *server* is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs.

In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. See Log storage on page 33 for more information.

To see a graphical view of the log forwarding configuration, and to see details of the devices involved, go to *System Settings* > *Logging Topology*. For more information, see Logging Topology on page 285.

Modes

FortiAnalyzer supports two log forwarding modes: forwarding (default), and aggregation.

Forwarding

Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

This mode can be configured in both the GUI and CLI.

Force this administrator to change password upon next log on.	Force the administrator to change their password the next time that they log in to the FortiAnalyzer. This option is only available if *Password Policy* is enabled in *Admin Settings*. See Password policy on page 382.
FortiToken Cloud	Enable or disable two-factor authentication with FortiToken Cloud, then select the token delivery method from the following options: • *FortiToken Mobile*: Use the FortiToken Mobile app to get tokens. The administrator is sent an email with a link to activate their token in the FortiToken Mobile app on their mobile device. • *Email*: Receive the token by email. • *SMS*: Receive the token by SMS message. This option is not available if Admin Type is set to *PKI* or *SSO*. See Two-factor authentication on page 385.
Administrative Domain	Choose the ADOMs this administrator will be able to access. • *All ADOMs*: The administrator can access all the ADOMs. • *All ADOMs except specified ones*: The administrator cannot access the selected ADOMs. • *Specify*: The administrator can access the selected ADOMs. Specifying the ADOM shows the *Specify Device Group to Access* check box. Select the *Specify Device Group to Access* check box and select the Device Group this administrator is allowed to access. The newly created administrator will only be able to access the devices within the Device Group and sub-groups. If the *Admin Profile* is *Super_User*, then this setting is *All ADOMs*. This field is available only if ADOMs are enabled. See Administrative Domains (ADOMs) on page 296.
Admin Profile	Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features. See Administrator profiles on page 358.
JSON API Access	Select the permission for JSON API Access. Select *Read-Write*, *Read*, or None. The default is *None*.
Trusted Hosts	Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added. See Trusted hosts on page 349 for more information.
Theme Mode	Select *Use Global Theme* to apply a theme to all administrator accounts. Select *Use Own Theme* to allow administrators to select their own theme.
Meta Fields	Optionally, enter the new administrator's email address and phone number.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced options, see the *FortiAnalyzer CLI Reference*.

TAI WIN TECHNOLOGY CORPORATION
泰 瑩 科 技 股 份 有 限 公 司

☐ 總　公　司：105407台北市松山區南京東路四段130號4樓
TEL:886-2-2578-1133　FAX:886-2-2578-0334

☐ 台中辦事處：407612台中市西屯區市政北七路186號3樓之2
TEL:886-4-2254-9376　FAX:886-4-2255-0423

☐ 高雄辦事處：806612高雄市前鎮區中山二路91號19樓之3
TEL:886-7-331-5252　FAX:886-7-331-5551

外 標 封

採購名稱：防火牆日誌紀錄器
截止投標時間：113年11月25日下午05時整

標號：TMU113-103 (第一次公告)
開標時間：113年11月25日下午05時整

11031 臺北市信義區吳興街 250 號

臺北醫學大學總務處事務組收

事務組採購承辦人：李清萬先生

投標廠商	泰瑩科技股份有限公司			統一編號	28208184
廠商地址	台北市南京東路四段130号4樓			廠商電話	02-2578-1133
廠商聯絡人	陳妤嘉	聯絡人電話	0908590611	聯絡人E-mail	yoga.chen@tai-win.com.tw

※注意事項：

一、投標文件遞送請注意時效，寄達本校事務組採購承辦人處，如逾時視為無效標。

二、投標文件應以不透明容器(封套)密封，外標封標籤請書寫完整基本資料後貼於標封封面，如未載明本案採購案名、標號及投標廠商、地址、電話或封口處未密封或信封套為透明者，皆視為無效標。

投標文件送達紀錄

▶廠商請擇一勾選

☐郵寄或快遞送達(免簽章及免填送達時間)
☐專人送達(送件須簽章並註記送達時間)
投標廠商送件人簽章：陳妤嘉
送達日期及時間：113年11月25日 15:46

本校收件人簽名：李清萬
收件日期及時間：113.11.25 15:46

TAI WIN TECHNOLOGY CORPORATION
泰瑩科技股份有限公司

□總　公　司：105407台北市松山區南京東路四段130號4樓
TEL:886-2-2578-1133　FAX:886-2-2578-0334

□台中辦事處：407612台中市西屯區市政北七路186號3樓之2
TEL:886-4-2254-9376　FAX:886-4-2255-0423

□高雄辦事處：806612高雄市前鎮區中山二路91號19樓之3
TEL:886-7-331-5252　FAX:886-7-331-5551

資、規格封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本資、規格封內請依投標須知規定裝入相關審核文件(請影印為 A4 尺寸)，並以迴紋針固定於左上角，俾利開標審核作業。

投標廠商	泰瑩科技股份有限公司	統一編號	28208184
廠商地址	台北市南京東路四段130號4F	廠商聯絡人	陳妤嘉
廠商電話	02-2578-1133	聯絡人電話	0908590611

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

開標/~~議價~~/~~決標~~/~~流標~~/~~廢標~~紀錄

時間：113 年 11 月 25 日下午 05 時 00 分　地點：本校醫學綜合大樓後棟一樓總務處會議室

採購案號	1130213887		請購單位	資訊處	
標的名稱及數量摘要	防火牆日誌紀錄器		開標次別	第一次	
公告日期	113/11/13		招標方式	■公開招標 □限制性招標	
投標廠商	標價	優先減價後之標價	第一次比減價格後之標價	第二次比減價格後之標價	第三次比減價格後之標價
四海資訊股份有限公司	資、規格符合				
威尼克科技有限公司	資、規格符合				
泰瑩科技股份有限公司	資、規格符合				

審標結果
~~/流標原因~~
~~/廢標原因~~

一、本案第一次公告後投標廠商計 3 家，開標前合格投標廠商 3 家，審標結果 3 家符合招標文件規定，其餘 0 家不合格。

二、_____報價（減價後）新臺幣（下同）_____元整最低，且在底價新臺幣_____元整以內，經主持人當場依政府採購法第 52 條第 1 項第 1 款宣布決標。

三、□投標廠商未達 3 家，經主持人當場宣布流標。

四、□開標後經審標結果，無得為決標對象之廠商，經主持人當場宣布廢標。

五、其他：本案經政府電子採購網第一次公告後共計三家廠商投標，且經資、規格標審標結果，三家廠商皆符合招標文件規定，提採購委員會進行比減價。

決標原則、得標廠商及決標金額

決標原則：依政府採購法第 52 條第 1 項第 1 款。
得標廠商：_____
決標金額：新台幣　佰　拾　萬　仟　佰　拾　元整。（含稅）（中文大寫）
押標金：新台幣_____元整。
履約保證金：□同押標金　□_____。
保固期限：□　　年　□無保固。
其他：_____
_____
（超底價決標時須另註明超底價之金額、比率及必須決標之緊急情事）

得標廠商代表簽名(或蓋章)

（不通知投標廠商到場者，免簽名或蓋章）

決標過程	請參詳上表。（註明減價/比減價格/超底價決標/協商/綜合評選之過程）
異議或申訴事件	無（註明尚未解決之異議或申訴事件之處理情形）
備註	

主持人	黃秀斯（簽章）	監辦人員（依規定由本校財務處人員擔任）	主辦會計 許淑群（簽章）
請購單位人員	陳暐傑（簽章）		
記錄（由本校事務組經辦人員擔任）	李清萬 113.11.25（簽章）	事務組組長	簽章

列印時間：113/11/28 13:28

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為
廠商代碼： 53099614 (威尼克科技有限公司)
廠商現況： 01-核准設立
廠商名稱： 威尼克科技有限公司

資料取得時間：113/11/28 13:28

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

李清高

標價清單

※請列出分項價格

採購名稱：防火牆日誌紀錄器

項目	數量	單價	總價
甲、 功能需求內容說明 1. 獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。 2. 系統日誌接收效能可達 6,000 logs/sec (含)以上。 3. 系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。 4. 系統儲存容量可達 16 TB(含)以上，支援磁碟陣列 RAID 0/1, 1s/5, 5s/10 規範。 5. 具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。 6. 具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。 7. 具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。 8. 具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。 9. 具備事件監看與告警功能,可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。 10. 具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。 11. 具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。 12. 具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。 13. 具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服	2台	$1300000	$2600000

項目	數量	單價	總價

器或 Common Event Format（CEF）伺服器，以利與既有日誌系統整合。

14. 具備管理區域（Administrative Domain）分割功能，並可針對不同管理人員賦予不同的管理權限。
15. 具備 REST API，以利與既有資安環境整合。採購項目說明

乙、 維護標的資訊一覽表

1. 維護等級5x8_設備清單

項次	設備型號	數量	維護期間
1	防火牆日誌紀錄器	1台	驗收日次日起算一年

2. 上述硬體設備得標廠商應提供自驗收次日起 1 年(5*8)人力到場維護保固服務及原廠經銷授權證明。
3. 得標廠商須提供原設備參數轉移與配合網路架構優化相關技術服務。
4. 為確保本案日後維護之保障，廠商須提供網路設備之原廠授權經銷商證明。

★本招標案件不得使用大陸廠牌資通訊產品(含軟體、硬體及服務)

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 投標標價清單:(第一次公告) 標號：TMU113-103

請購單位：資訊處，請購人：陳暐傑 先生，聯絡電話：2736-1661 轉 2626

合　　計	新臺幣貳佰陸拾零萬零仟零佰零拾零元整(含稅)				
型　　號	FAZ-810G	原 產 地	美國	Maker	Fortinet
交 貨 期	廠商須於 113 年 12 月 13 日前，將採購標的送達請購單位指定地點，安裝測試完畢，且測試結果符合投標須知及標單、契約等規定。				
備　　註	※保固期至少為一年(或依原廠保固期較長為主)，請務必列出分項價格及廠牌。				

廠商資料		
	投標商名稱：威尼克科技有限公司	投標廠商及負責人章：
	投標商統編：53049614	
	投標商地址：臺北市永和區中山路1段269號3F	
	投標聯絡人：林伯勳	
	聯絡人電話：0930-275-766 手機：0930-275-766	投標日：113 年 11 月 21 日

價 格 封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本價格封內僅裝入『標價清單』等，其他投標文件請一律裝入資、規格封內。

投標廠商	威尼克科技有限公司	統一編號	53099614
廠商地址	新北市永和區中山路1段267號5F	廠商聯絡人	朱木伯熏
廠商電話	0930-275-766	聯絡人電話	0930-275-766

列印時間 : 113/11/28 13:26

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為
廠商代碼： 22644575 (四海資訊股份有限公司)
廠商現況： 01-核准設立
廠商名稱： 四海資訊股份有限公司

資料取得時間：113/11/28 13:26

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **投標標價清單:(第一次公告)** 標號：TMU113-103

標價清單

※請列出分項價格

採購名稱：防火牆日誌紀錄器

項目	數量	單價	總價
甲、 功能需求內容說明	2台		
1.獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。		NT$1,225,000	
2.系統日誌接收效能可達 6,000 logs/sec (含)以上。			NT$2,450,000
3.系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。			
4.系統儲存容量可達 16 TB(含)以上，支援磁碟陣列 RAID 0/1,1s/5,5s/10 規範。			
5.具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。			
6.具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。			
7.具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。			
8.具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。			
9.具備事件監看與告警功能,可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。			
10.具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。			
11.具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。			
12.具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。			
13.具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服			

項目	數量	單價	總價

器或 Common Event Format（CEF）伺服器，以利與既有日誌系統整合。

14. 具備管理區域（Administrative Domain）分割功能，並可針對不同管理人員賦予不同的管理權限。

15. 具備 REST API，以利與既有資安環境整合。採購項目說明

乙、 維護標的資訊一覽表

1. 維護等級5x8_設備清單

項次	設備型號	數量	維護期間
1	防火牆日誌紀錄器	1台	驗收日次日起算一年

2. 上述硬體設備得標廠商應提供自驗收次日起 1 年(5*8)人力到場維護保固服務及原廠經銷授權證明。

3. 得標廠商須提供原設備參數轉移與配合網路架構優化相關技術服務。

4. 為確保本案日後維護之保障，廠商須提供網路設備之原廠授權經銷商證明。

★本招標案件不得使用大陸廠牌資通訊產品(含軟體、硬體及服務)

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 投標標價清單:(第一次公告) 標號：TMU113-103

請購單位：資訊處，請購人：陳暐傑 先生，聯絡電話：2736-1661 轉 2626

合　　計	新臺幣 貳 佰 肆 拾 伍 萬 零 仟 零 佰 零 拾 零 元整(含稅)				
型　　號	FAZ-810G	原 產 地	美國	Maker	Fortinet
交 貨 期	廠商須於 113 年 12 月 13 日前，將採購標的送達請購單位指定地點，安裝測試完畢，且測試結果符合投標須知及標單、契約等規定。				
備　　註	※保固期至少為一年(或依原廠保固期較長為主)，請務必列出分項價格及廠牌。				

廠商資料		
	投標商名稱：四海資訊股份有限公司	投標廠商及負責人章：
	投標商統編 :22644575	
	投標商地址：臺中市北屯區陳平路117巷46之3號	
	投標聯絡人： 林高春	
	聯絡人電話 :(04)225950185　　手機 :0919-589-796	投標日：113年11月22日

四海資訊股份有限公司
Whole World Informcition Co., Ltd
總公司：40464台中市北區陝西路33號2F
電　話：(04)-2295-0210　　傳真：(04)-2295-0189
台　北：11473台北市內湖區文德路159號
電　話：(02)-2797-9331　　傳真：(02)-2658-9772

印刷品	
限　時	
掛　號	
平　信	

價 格 封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本價格封內僅裝入『標價清單』等，其他投標文件請一律裝入資、規格封內。

投標廠商	四海資訊股份有限公司	統一編號	22644575
廠商地址	台中市北屯區陳平路117巷46之3號	廠商聯絡人	林高春
廠商電話	02-27979331	聯絡人電話	0919-58-9796

列印時間：113/11/28 13:27

拒絕往來廠商查詢

以廠商資料查詢拒絕往來廠商名單，查詢結果如下：

查詢特定條件為
廠商代碼： 28208184 (泰瑩科技股份有限公司)
廠商現況： 01-核准設立
廠商名稱： 泰瑩科技股份有限公司

資料取得時間：113/11/28 13:27

項次	廠商代碼	廠商名稱	負責人姓名	工廠隸屬之事業主體統一編號及名稱	備註	機關名稱	生效日	截止日
無符合條件資料								

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **投標標價清單:(第一次公告)** 標號：TMU113-103

標價清單

※請列出分項價格

採購名稱：防火牆日誌紀錄器

項目	數量	單價	總價
甲、 功能需求內容說明	2台		
1.獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。 2.系統日誌接收效能可達 6,000 logs/sec (含)以上。 3.系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。 4.系統儲存容量可達 16 TB(含)以上，支援磁碟陣列 RAID 0/1,1s/5,5s/10 規範。 5.具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。 6.具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。 7.具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。 8.具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。 9.具備事件監看與告警功能,可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。 10.具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。 11.具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。 12.具備資安維運中心 (SOC) 檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。 13.具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服		NT$1,944,000 NT$1,389,800	

項目	數量	單價	總價

器或 Common Event Format (CEF) 伺服器，以利與既有日誌系統整合。

14. 具備管理區域 (Administrative Domain) 分割功能，並可針對不同管理人員賦予不同的管理權限。

15. 具備 REST API，以利與既有資安環境整合。採購項目說明

乙、 維護標的資訊一覽表

1. 維護等級5x8_設備清單

項次	設備型號	數量	維護期間
1	防火牆日誌紀錄器	1台	驗收日次日起算一年

2. 上述硬體設備得標廠商應提供自驗收次日起 1 年(5*8)人力到場維護保固服務及原廠經銷授權證明。

3. 得標廠商須提供原設備參數轉移與配合網路架構優化相關技術服務。

4. 為確保本案日後維護之保障，廠商須提供網路設備之原廠授權經銷商證明。

★本招標案件不得使用大陸廠牌資通訊產品(含軟體、硬體及服務)

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 投標標價清單:(第一次公告) 標號：TMU113-103

請購單位：資訊處，請購人：陳暐傑 先生，聯絡電話：2736-1661 轉 2626

合　　計	新臺幣 貳佰 參拾捌萬 玖仟捌佰 ~~拾~~ ~~元~~整(含稅)				
型　　號	FAZ-810G	原 產 地	美國	Maker	Fortinet
交 貨 期	廠商須於 113 年 12 月 13 日前，將採購標的送達請購單位指定地點，安裝測試完畢，且測試結果符合投標須知及標單、契約等規定。				
備　　註	※保固期至少為一年(或依原廠保固期較長為主)，請務必列出分項價格及廠牌。				

廠商資料		
	投標商名稱：秦荃科技股份有限公司	投標廠商及負責人章：
	投標商統編：28208184	
	投標商地址：台北市南京東路四段130号4F	
	投標聯絡人：陳彥嘉	
	聯絡人電話：0908590611　　手機：0908590611	投標日：113年11月25日

TAI WIN TECHNOLOGY CORPORATION
泰 瑩 科 技 股 份 有 限 公 司

□總　公　司：105407台北市松山區南京東路四段130號4樓
TEL:886-2-2578-1133　FAX:886-2-2578-0334

□台中辦事處：407612台中市西屯區市政北七路186號3樓之2
TEL:886-4-2254-9376　FAX:886-4-2255-0423

□高雄辦事處：806612高雄市前鎮區中山二路91號19樓之3
TEL:886-7-331-5252　FAX:886-7-331-5551

價 格 封

採購名稱：防火牆日誌紀錄器　　標號：TMU113-103(第一次公告)

※本價格封內僅裝入『標價清單』等，其他投標文件請一律裝入資、規格封內。

投標廠商	泰瑩科技股份有限公司	統一編號	28208184
廠商地址	台北市南京東路四段130號4樓	廠商聯絡人	陳如玉
廠商電話	02-2578-1133	聯絡人電話	0908590611

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

廠商投標議比價單

議價日期	中華民國一一三年十一月二十八日
議價地點	本校醫學綜合大樓前棟三樓第一會議室
議價會議	一一三學年度採購委員會第九次會議
請購單位	資訊處
採購名稱	防火牆日誌紀錄器
交貨期	依投標須知及標單相關規定
備註	※標價需含營業稅額。 ※標價含開狀手續費、報關費、提貨、倉租及將貨運至本校請購單位指定地點等所需之一切費用並需含安裝、裝機完成。 ※結匯金額以所議定之新臺幣金額為上限，期間若因匯率變動致結匯金額超過概由乙方補足，若另有議定條件則不在此限。

議比價記錄

開標價格	優先減價	第一次比減價	第二次比減價	第三次比減價
NT$245000/	NT$ ※「開標價格」最低者可享有優先減價權。	NT$225000/ ※需低於優先減價，否則請註明「無法再減」字樣。	NT$221500/	NT$無法再減
決標價格	新台幣 佰 拾 萬 仟 佰 拾 元整。(含稅)			

※附加條件：

1. _____。
2. _____。
3. _____。
4. _____。

投標廠商資料	
	投標廠統編：22644575
	投標廠名稱：四海資訊(股)公司
	投標代表人：林高泰
	投標商電話：0919589796
	投標商地址：台中市北屯區陳平路110巷46-3號

投標廠商蓋章：四海資訊股份有限公司 林高泰

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

廠商投標議比價單

議價日期	中華民國一一三年十一月二十八日
議價地點	本校醫學綜合大樓前棟三樓第一會議室
議價會議	一一三學年度採購委員會第九次會議
請購單位	資訊處
採購名稱	防火牆日誌紀錄器
交貨期	依投標須知及標單相關規定
備註	※標價需含營業稅額。 ※標價含開狀手續費、報關費、提貨、倉租及將貨運至本校請購單位指定地點等所需之一切費用並需含安裝、裝機完成。 ※結匯金額以所議定之新臺幣金額為上限，期間若因匯率變動致結匯金額超過概由乙方補足，若另有議定條件則不在此限。

議比價記錄

開標價格	優先減價	第一次比減價	第二次比減價	第三次比減價
NT$2690000	NT$ ※「開標價格」最低者可享有優先減價權。	NT$2290000 ※需低於優先減價，否則請註明「無法再減」字樣。	NT$ 2240000	NT$ 無法再減
決標價格	新台幣 佰 拾 萬 仟 佰 拾 元整。(含稅)			

※附加條件：

1. _____。
2. _____。
3. _____。
4. _____。

投標廠商資料

投標廠統編：53099614

投標廠名稱：威尼克科技有限公司

投標代表人：林伯勳

投標商電話：028660378

投標商地址：新北市永和區中山路一段267巷3樓

投標廠商蓋章

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

廠商投標議比價單

議價日期	中華民國一一三年十一月二十八日
議價地點	本校醫學綜合大樓前棟三樓第一會議室
議價會議	一一三學年度採購委員會第九次會議
請購單位	資訊處
採購名稱	防火牆日誌紀錄器
交貨期	依投標須知及標單相關規定
備註	※標價需含營業稅額。 ※標價含開狀手續費、報關費、提貨、倉租及將貨運至本校請購單位指定地點等所需之一切費用並需含安裝、裝機完成。 ※結匯金額以所議定之新臺幣金額為上限，期間若因匯率變動致結匯金額超過概由乙方補足，若另有議定條件則不在此限。

議比價記錄

開標價格	優先減價	第一次比減價	第二次比減價	第三次比減價
NT$2,389,800	NT$2,300,000 ※「開標價格」最低者可享有優先減價權，	NT$2,280,000 ※需低於優先減價，否則請註明「無法再減」字樣，	NT$2,230,000	NT$2,190,000

決標價格：新台幣 壹佰玖拾一萬 ~~仟 佰 拾~~ 元整。(含稅)

※附加條件：

1. _____。
2. _____。
3. _____。
4. _____。

投標廠商資料

投標廠統編：28208184

投標廠名稱：泰瑩科技股份有限公司

投標代表人：陳好嘉

投標商電話：0908590641

投標商地址：台北市南京東路四段130號4F

投標廠商蓋章

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 開標/議價/決標/~~流標/廢標~~紀錄

時間：113 年 11 月 28 日下午 02 時 00 分　　地點：本校醫學綜合大樓前棟三樓第一會議室

採購案號	1130213887		請購單位	資訊處	
標的名稱及數量摘要	防火牆日誌紀錄器		開標次別	第一次	
公告日期	113/11/13		招標方式	■公開招標□限制性招標	
投標廠商	標價	優先減價後之標價	第一次比減價格後之標價	第二次比減價格後之標價	第三次比減價格後之標價
四海資訊股份有限公司	$ 2,450,000	--	$ 2,250,000	$ 2,215,000	$ 無法再減
威尼克科技有限公司	$ 2,600,000	--	$ 2,290,000	$ 2,240,000	$ 無法再減
泰瑩科技股份有限公司	$ 2,389,800	$ 2,300,000	$ 2,280,000	$ 2,230,000	$ 2,190,000

本校（以下簡稱甲方）與得標廠商（以下簡稱乙方）同意就首揭財物議定下列條款：

一、經開標議、比價後，以■含稅價格新台幣$1,900,000元決標。　□以CIP＿＿＿＿＿決標。（開標當日依決標前一辦公日臺灣銀行外匯交易收盤即期賣出匯率為1：＿＿＿；如匯率超過1：＿＿＿＿，其差額由廠商負擔。）

二、乙方應於決標翌日起十四個工作天內繳交履約保證金新臺幣**契約金額之一定比率10%**。

三、乙方須於■民國＿＿年＿＿月＿＿日以前提供履約標的之供應(□含安裝測試)。□結匯計算單開出後＿＿＿天內交貨■其他：廠商應於113年12月13日前完成交貨安裝測試　。

四、雙方同意■另訂契約(本紀錄視為契約之一部分)。　□本紀錄視同契約。

五、保固期限：□無保固　■自驗收合格之日起，■保固一年□保固＿＿＿年□其他＿＿＿＿＿＿；■保固保證金以成交金額3%計算。

六、如屬財物採購，乙方須負責運送及安裝，國外採購案並須負擔開狀、結匯、提貨、倉租等相關費用。

七、其他約定條款如後：

1. 乙方保證金：履約完成，驗收合格且無待解決事項後無息發還，如乙方對甲方負有因本紀錄而生之債務，甲方就乙方所繳保證金有優先扣抵之權。
2. 交貨/履約地點：交貨地點為甲方所在地或甲方指定之場所，如貨品於裝運途中，因裝箱不良等原因，在開箱清點時發現有破損時，乙方應負責照數賠償。
3. 驗收：乙方於可得驗收時，應通知甲方辦理驗收。乙方所交貨品或履約結果，如經甲方驗收使用結果發現內容與原附圖說資料，及甲方所審定規格不符或性能效果不佳時，均應限期無條件調換、改善、拆除、重作、退貨或換貨(以下簡稱改正)，其一切損失應由乙方自理。如未在調換期限內交貨或逾期未改正者，概按照逾期違約金之規定辦理。
4. 逾期違約金：乙方如未依照規定期限履約，□應按逾期日數，每日依全部契約價金總額3‰計算支付逾期違約金予甲方。□但未完成履約之部分不影響其他已完成部分之使用者，得按未完成履約部分之契約價金，每日依其3‰計算逾期違約金。■其他依契約內文所示。逾期違約金總額，以全部契約價金總額之百分之二十為上限，甲方得自應付價金中扣抵，其有不足者，通知乙方繳納或自保證金扣抵。但遇天災或事變等不可抗力或不可歸責於乙方之事由提有證明者，經甲方查明同意，確非人力所能抗拒者，不在此限。如逾期達三十天，乙方無正當理由而不履行契約者，甲方得解除契約，乙方所繳納之保證金不予發還。
5. 付款辦法：□驗收合格後一次付款 □分期付款，條件：＿＿＿＿＿＿＿＿ □契約訂妥並俟外匯核准後，開發信用狀 ■其他依契約內文所示。
6. 如有押標金，押標金不予發還之情形，依政府採購法第三十一條第二項規定辦理。
7. 本紀錄如有未規定事項，悉依政府採購法及民法等相關法令規定辦理。
8. 乙方於國內員工總人數逾一百人，履約期間僱用身心障礙者及原住民人數各應達國內員工總人數百分之一，並均以整數為計算標準，未達整數部分不予計入。僱用不足者，應分別依規定向所在地之直轄市或縣（市）勞工主管機關設立之身心障礙者就業基金專戶及原住民中央主管機關設立之原住民族就業基金專戶，繳納上月之代金；並不得僱用外籍勞工取代僱用不足額部分。甲方應將國內員工總人數逾一百人之乙方資料公開於政府採購資訊公告系統，以供勞工及原住民主管機關查核代金繳納情形，甲方不另辦理查核。

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

開標/議價/決標/~~流標/廢標~~紀錄

時間：113 年 11 月 28 日下午 02 時 00 分　　地點：本校醫學綜合大樓前棟三樓第一會議室

審標結果 ~~/流標原因~~ ~~/廢標原因~~	一、本案一次公告後投標廠商計 3 家，開標前合格投標廠商計 3 家，審標結果 3 家符合招標文件規定，其餘 0 家不合格。 二、泰瑩科技股份有限公司報價（減價後）新臺幣（下同）1,900,000 元整最低，且在底價新臺幣 1,980,000 元整以內，依政府採購法第 52 條第 1 項第 1 款。 三、☐投標廠商未達 3 家，經主持人當場宣布流標。 四、☐開標後經審標結果，無得為決標對象之廠商，經主持人當場宣布廢標。 五、其他：本案經政府電子採購網第一次公告後共計三家廠商投標，且經資、規格標審標結果，三家廠商皆符合招標文件規定，提本會進行比減價。
決標原則、得標廠商及決標金額	決標原則：依政府採購法第 52 條第 1 項第 1 款。 得標廠商：泰瑩科技股份有限公司 決標金額：新台幣 X 仟 壹 佰 玖 拾 X 萬 X 仟 X 佰 X 拾 元整。(含稅)(中文大寫) 押標金：新台幣 $119,000 元整。 履約保證金：☐同押標金 ■ **契約金額之一定比率 10%**。 保固期限：■ 一 年 ☐無保固。 其他： （超底價決標時須另註明超底價之金額、比率及必須決標之緊急情事） 得標廠商代表簽名(或蓋章) ［印］ （不通知投標廠商到場者，免簽名或蓋章）
決標過程	請參詳上表。 （註明減價/比減價格/超底價決標/協商/綜合評選之過程）
異議或申訴事件	無 （註明尚未解決之異議或申訴事件之處理情形）
備註	

主持人	［簽名］（簽章）	監辦人員（依規定由本校財務處人員擔任）	主辦會計 許淑群（簽章）
請購單位人員	［簽名］（簽章）	記錄	劉又溱 113.11.28（簽章）
事務組經辦人員	李清萬 113.11.28（簽章）	事務組組長	［簽名］（簽章）

採購委員 ☐採購小組會 ■採購委員會	※事務組議價會則免簽。 ［簽名］（簽章）

檔　　號：0113/S510/1
保存年限：永久

簽　於　總務處

日　　期：113年11月29日

密等及解密條件或保密期限：

附　　件：113採購委員會第09次會議-會議記錄.pdf

主旨：檢陳113學年度採購委員會第九次會議紀錄一份，詳如附件，請　鑒核。

會辦單位：

決行層級：機關首長決行

— 批核軌跡及意見 —

序	單位	職稱	姓名	意見	辦理時間
1	總務處事務組	專員	劉又溱	附件資料已更正。	113/11/29 15:12:46 承辦
2	總務處事務組	組長	李彥蓉	擬： 1. 檢陳113學年度採購委員會第九次會議紀錄。 2. 依簽呈決議辦理並存參備查。	113/11/29 15:31:50 核示
3	總務處	副總務長	沈盛達	擬如事務組所擬陳核。	113/11/29 15:43:40 核示
4	總務處	總務長	張正恆	擬如事務組所擬。陳請核示。	113/11/29 16:05:40 核示
5	秘書處	主任秘書	蔡宛真	會議記錄陳請鈞長鑒核。	113/11/30 00:18:59 核示
6	副校長室	副校長	朱娟秀	擬如主秘擬	113/11/30 06:05:02 核示
7	校長室	校長	吳參斯	如擬 決行	113/12/02 07:03:13 決行

（主旨：檢陳113學年度採購委員會第九次會議紀錄一份，詳如附件，請　鑒核。）

8	總務處事務組	專員	劉又溱		113/12/02 07:51:03 承辦

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

時間：113 年 11 月 28 日(週四)下午 02:00
地點：本校醫學綜合大樓前棟三樓第一會議室
主席：吳麥斯校長
(以下稱謂敬略)
出席：許淑群、張正恆、李佳蓉、林中魁、許銘仁、林俊茂、馮琮涵、邱佳慧、邱泓文、簡怡雯、許志瑋
列席：李彥蓉、劉又溱、李清萬、方仁琦、陳靖怡、蕭淑媛、沈純慧、陳雨靜、傅盈甄、王淑慧、萬序恬、陳暐傑、林芊逸、林威廷、邱丙筌、張榮岳、林姵妤(陳劭綺代)
請假：朱娟秀　　記錄：劉又溱

壹、主席致詞：略

貳、前次會議追蹤事項：無

參、討論案：

一、「國際磨課師平台使用費」，擬採限制性招標方式辦理，陳請討論。

請購單位說明：

因該平台為本校重要開放教育策略發展，擬委由國外廠商「FutureLearn Limited」提供平台服務壹年，優惠價每年英鎊貳萬參仟元整，業經簽呈核可，擬依本校限制性招標申請單第 16 款辦理，陳請討論。

決議：同意本案採限制性招標方式辦理，由 FutureLearn Limited 以英鎊貳萬參仟元整得標，本案須支付足額英磅（約台幣 1,035,000 元）。

二、「數位自學課程證書年費方案」，擬採限制性招標方式辦理，陳請討論。

請購單位說明：

為推動全校數位自學方案，擬續訂 Coursera 平台線上課程壹年，該平台為國外廠商「Coursera Inc.」所提供，專案優惠價每年美金肆萬壹仟捌佰肆拾參元整，業經簽呈核可，擬依本校限制性招標單第 16 款辦理，陳請討論。

決議：同意本案採限制性招標方式辦理，由 Coursera Inc.以美金肆萬壹仟捌佰肆拾參元整得標，本案須支付足額美金（約台幣 1,401,741 元）。

三、「續訂 ScienceDirect 電子期刊」，擬引用共同供應契約方式辦理，陳請討論。

請購單位說明：

1.本案為續訂電子資源且為 CONCERT 聯盟項目，由聯盟代表國內大專院校議價得優惠價（共同供應契約招標案號：STPI-P-112228），業經簽呈核可，同意以共同供應契約方式辦理，陳請討論。

2.由 Elsevier B.V.以美金 489,303.43 元整得標，本案須支付足額美金(約台幣 15,903,000 元)。

決議：同意本案引用共同供應契約方式辦理，由 Elsevier B.V.以美金肆拾捌萬玖仟參佰零參點肆參元整得標，本案須支付足額美金(約台幣 15,903,000 元)。

四、「續訂 Oxford Journals Online 電子期刊」，擬引用共同供應契約方式辦理，陳請討論。

請購單位說明：

1.本案為續訂電子資源且為 CONCERT 聯盟項目，由聯盟代表國內大專院校議價得優惠價（共同供應契約招標案號：STPI-P-112220），業經簽呈核可，同意以共同供應契約方式辦理，陳請討論。

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

2.由 Oxford University Press 以美金 53,865 元整得標，本案須支付足額美金（約台幣 1,751,000 元）。

決議：同意本案引用共同供應契約方式辦理，由 Oxford University Press 以美金伍萬參仟捌佰陸拾伍元整得標，本案須支付足額美金(約台幣 1,751,000 元)。

五、「雙和 B 基地室內裝修工程監造作業委任案」，擬辦理契約變更，陳請討論。

請購單位說明：

1.本案業經 111 學年度採購委員會第 18 次會議決議，由萬有為建築師事務所以新台幣壹仟貳佰萬元整得標。

2.依契約第十三條第一項：「甲方於必要時得通知乙方變更本契約，乙方於接獲通知後，除雙方另有協議外，應於 10 日內向甲方提出服務範圍、委任酬金、履約期限、付款辦法或其他本契約內容須變更之相關文件，並依甲方相關辦法辦理採購變更後，始得為之」。本案契約範圍共 19 件裝修工程案，其中 16 案辦理採購工程變更，致裝修工程契約總價及監造作業內容增加，故通知萬有為建築師事務所變更契約，裝修工程採購變更內容說明如下：

(1)19 案裝修工程原契約總價：1,291,180,000 元整
(2)16 案裝修工程案進行採購變更，變更之追加、追減及新增工項金額如下：
A.原契約追加金額計：35,589,699 元整
B.原契約追減金額計：70,120,172 元整
C.新增項目金額計：48,570,884 元整

3.萬有為建築師事務所依契約規定提報變更相關文件及追加委任酬金金額為 1,433,858 元，陳請討論。

決議：同意本案契約變更並增加委任酬金，另進行追加委任酬金議價。

六、「2024 年台灣醫療科技展空間設計佈置費」，擬辦理設計變更，陳請討論。

請購單位說明：

1.本案業經 113 學年度採購委員會第 5 次會議決議，由藝創國際空間設計有限公司以新台幣參佰壹拾萬元整得標。

2.依契約第十條契約之變更：「本契約書之所有約款，在任何方面均不得放棄、更改、修改或增訂，除非經甲乙雙方或其所授權之人書面簽署外，其它任何口頭或書面之變更，增刪約款之約定，均不生拘束或規範當事人間之效力。如果在任何時刻乙方預見原定之計畫時程將有延誤，不論是因為甲方所要求之服務上的變更，還是因其他非乙方可控制之原因，乙方應告知甲方，並經甲乙雙方一致同意後修改計畫時程。任何變更所導致的費用變更應反應於變更指示中。」

3.因 10/18 討論會議決議調整展出方向，同時調整整體攤位架構，並請廠商重新繪製圖面及 3D 圖，依與大會協調時程 11/8 重新提交醫療展主辦單位攤位架構認證申請，依此相關變更說明如下：

(1) 追加項目：42 吋觸控電視增加 1 台與 65 吋觸控電視 6 台，共計加帳 80,400 元整。
(2) 追減項目：42 吋壁掛式減少 9 台，共計減帳 44,100 元整。
(3) 新增項目：為符合參展需求新增工項，廠商報價 503,790 元。.

4.綜上，經請購單位及事務組依原契約項目單價核算後，共計加帳 36,300 元整，新增工項後續另進行議價，陳請討論。

決議：同意本案設計變更，原契約共計加帳新台幣參萬陸仟參佰元整，另進行新增工項議價。

七、「韌性國家醫療整備國際研討會外包場地佈置費」，擬採限制性招標方式辦理，陳請討論。

請購單位說明：

為辦理本校與衛生福利部於 113 年 11 月 30 日共同舉辦「韌性國家醫療整備畫國際研討會」，考量現有人力不足並參考校院單位過往舉辦國際會議經驗，擬委由「淵暘公關管理顧問有限公司」協助提供場地佈置及人力服務，業經簽呈核可，依本校限制性招標申請單第 16 款辦理，陳請討論。

決議：同意本案採限制性招標方式辦理。

肆、採購議案：

一、「續訂學術發展評比資料庫平台」

請購單位：技術服務組，採購案號：1130203511，預算來源：校內預算 113-3202-006-101，預算金額：5,287,000元

說明： 本案經校內採購招標公告網二次公告後僅「碩睿資訊有限公司」投標，且資、規格標審標結果符合招標文件規定，提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	碩睿資訊有限公司	$5,564,692	--	$5,400,000	$5,350,000	$5,270,000	$5,270,000

決議：由碩睿資訊有限公司以新台幣伍佰貳拾柒萬元整得標。

二、「研究評估分析系統暨臺北醫學大學學術知識庫暨專家研究網」

請購單位：圖書館，採購案號：1130203420，預算來源：校內預算 113-3407-003-101（依簽呈核示，本案經費後續將由深耕計畫經費支應），預算金額：4,475,412元

說明： 本案經政府電子採購網二次公告後僅「飛資得醫學資訊股份有限公司」投標，且資、規格審標結果符合招標文件規定，提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	飛資得醫學資訊股份有限公司	$4,403,424	--	$4,350,000	$4,300,000	$4,240,000	$4,240,000

決議：由飛資得醫學資訊股份有限公司以新台幣肆佰貳拾肆萬元整得標。

三、「續訂 Micromedex Healthcare Series 醫療照護系列資料庫」

請購單位：技術服務組，採購案號：1130203510，預算來源：教育部獎勵私立大學校院校務發展計畫 113-3202-002-211，預算金額：3,521,000元

說明： 本案經政府電子採購網二次公告後僅「碩睿資訊有限公司」投標，且資、規格審標結果符合招標文件規定，提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	碩睿資訊有限公司	$3,705,946	--	$3,650,000	$3,600,000	$3,509,000	$3,509,000

決議：由碩睿資訊有限公司以新台幣參佰伍拾萬玖仟元整得標。

臺北醫學大學會議紀錄
會議名稱 一一三學年度採購委員會 會議次別 第九次會議

四、「訂購 ACM 及 ACP 電子書資料庫」

請購單位：技術服務組，採購案號：1130203431，預算來源：教育部獎勵私立大學校院校務發展計畫 113-3202-002-211，預算金額：3,290,000元

說明： 本案經政府電子採購網二次公告後僅「碩睿資訊有限公司」投標，且資、規格審標結果符合招標文件規定，提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	碩睿資訊有限公司	$3,439,550	--	$3,400,000	$3,350,000	$3,250,000	$3,250,000

決議：由碩睿資訊有限公司以新台幣參佰貳拾伍萬元整得標。

五、「600MHz 核磁共振儀年度保固維護保養」

請購單位：共同儀器中心，採購案號：1130203435，預算來源：校內預算 113-3407-003-101，預算金額：2,300,000元

說明： 本案經校內採購招標公告網二次公告後僅「台灣安捷倫科技股份有限公司」投標，且資格標審標結果符合招標文件規定，提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	台灣安捷倫科技股份有限公司	$3,468,775	--	$3,000,000	$2,500,000	$1,950,000	$1,950,000

決議：由台灣安捷倫科技股份有限公司以新台幣壹佰玖拾伍萬元整得標。

六、「防火牆日誌紀錄器」

請購單位：資訊處，採購案號：1130203887，預算來源：教育部獎勵私立大學校院校務發展計畫 113-3600-001-212，預算金額：2,389,800元

說明： 本案經政府電子採購網第一次公告後共計三家廠商投標，經資、規格標審標結果三家廠商皆符合招標文件規定，提本會進行比減價。

比減價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	四海資訊股份有限公司	$2,450,000	--	$2,250,000	$2,215,000	無法再減	--
2	威尼克科技有限公司	$2,600,000	--	$2,290,000	$2,240,000	無法再減	--
3	泰瑩科技股份有限公司	$2,389,800	$2,300,000	$2,280,000	$2,230,000	$2,190,000	$1,900,000

決議：由泰瑩科技股份有限公司以新台幣壹佰玖拾萬元整得標。

七、「橫向網路流量分析系統」

請購單位：資訊處，採購案號：1130203933，預算來源：教育部獎勵私立大學校院校務發展計畫 113-3600-001-212，預算金額：1,000,000元

說明： 本案經校內採購招標公告網第一次公告後共計三家廠商投標，經資、規格標審標結果三家廠商皆符合招標文件規定，提本會進行比減價。

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

比減價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	昊正科技股份有限公司	$1,010,000	--	不克到場放棄減價	--	--	--
2	動力安全資訊股份有限公司	$997,500	--	$830,000	進入底價	--	$830,000
3	精誠軟體服務股份有限公司	$855,000	$854,000	無法再減	--	--	--

決議：由動力安全資訊股份有限公司以新台幣捌拾參萬元整得標。

八、「雙和 B 基地室內裝修工程監造作業委任案」契約變更議價

請購單位：營繕組，採購案號：1110205971，預算來源：校內預算 111-3004-016-112，預算金額：13,884,899元，成交金額：12,000,000元

說明：請購單位提出契約變更，廠商提報追加酬金金額 1,433,858 元整，提本會進行議價。

追加委任酬金議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	萬有為建築師事務所	$1,433,858	--	$1,415,000	$1,400,000	進入底價	$1,400,000

決議：1.本案追加委任酬金經議價後，萬有為建築師事務所同意以新台幣壹佰肆拾萬元整承攬。

2.變更後工程款：$12,000,000+$1,400,000(追加委任酬金)=$13,400,000

3.本案以新台幣壹仟參佰肆拾萬元整辦理竣工結算。

九、「2024 年台灣醫療科技展空間設計佈置費」新增工項議價

請購單位：營運績效組，採購案號：1130201295，預算來源：管發校院基金 112-1601-002-400，預算金額：4,521,000元，成交金額：3,100,000元

說明：請購單位提出設計變更，並依原契約項目進行追加減帳，共計加帳 36,300 元，新增工項報價 503,790 元，提本會進行議價。

新增工項議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	藝創國際空間設計有限公司	$503,790	--	$450,000	$400,000	進入底價	$400,000

決議：1.本案新增工項經議價後，藝創國際空間設計有限公司同意以新台幣肆拾萬元整承攬。

2.變更後契約價款：$3,100,000+$36,300(原契約加帳)+$400,000(新增工項)=$3,536,300。

3.本案以新台幣參佰伍拾參萬陸仟參佰元整辦理驗收結算。

十、「韌性國家醫療整備國際研討會外包場地佈置費」

請購單位：管理發展中心，採購案號：1130204779，預算來源：衛生福利部 112-5400-011-300，預算金額：1,476,168元

說明：本案採限制性招標方式辦理。

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	淵暘公關管理顧問有限公司	$1,476,168	--	$1,470,000	$1,460,000	$1,400,000	$1,400,000

決議：由淵暘公關管理顧問有限公司以新台幣壹佰肆拾萬元整得標，並同意發票送達後一個月內付款。

伍、臨時動議：無

陸、結束時間：下午 03：38

臺北醫學大學
一一三學年度採購委員會第九次會議
會議簽到單

日期：113年11月28日　　採購委員會會議時間：14:00~16:00
主席：吳麥斯校長　　會議地點：本校醫學綜合大樓前棟三樓第一會議室

出席委員

職稱	姓名	簽到
校長	吳麥斯	
副校長	朱娟秀	請假
總務長	張正恆	
財務長	許淑群	
醫學資訊研究所	邱泓文	
解剖學暨細胞生物學科	馮琮涵	
牙體技術學系	林中魁	
管理發展中心	許志瑋	
保健營養學系	簡怡雯	
藥理學科	許銘仁	
中草藥臨床藥物研發博士學位學程	李佳蓉	
通識教育中心	邱佳慧	
生物化學暨細胞分子生物學科	林俊茂	

列席人員（職稱敬略）

單位	姓名	簽到
總務處事務組	李彥蓉	

臺北醫學大學
一一三學年度採購委員會第九次會議
會議簽到單

日期：113年11月28日　　採購委員會會議時間：14:00~16:00
主席：吳麥斯校長　　會議地點：本校醫學綜合大樓前棟三樓第一會議室

列席人員（職稱敬略）

單位	姓名	簽到
總務處事務組	劉又溙	
總務處事務組	李清萬	
總務處事務組	方仁琦	
總務處事務組	張庭碩	
總務處事務組	陳靖怡	
共同儀器中心	王淑慧	
圖書館	蕭淑媛	
技術服務組	沈純慧	
技術服務組	陳雨靜	
技術服務組	傅盈甄	
數位自學中心	萬序恬	
資訊處	陳暐傑	
資訊處	林芊逸	
資訊處	林威廷	
營運績效組	張桀岳	
總務處營繕組	邱丙笙	
韌性國家醫療整備計畫管理中心	林姵妤	陳品綺代

應到：13人；實到：12人；請假：1人；出席率：92.3%

（出席率僅計算出席人員出席率）

新增決標公告

列印時間：113/11/28 16:48:4

新增決標公告 成功

決標公告 公告日: 113/11/29

機關資料	機關代碼	03724606
	機關名稱	臺北醫學大學
	單位名稱	臺北醫學大學
	機關地址	110 臺北市 信義區 吳興街250號
	聯絡人	李清萬
	聯絡電話	(02) 27361661 # 2912
	傳真號碼	(02) 27363327
	電子郵件信箱	chingwan@tmu.edu.tw

已公告資料	標案案號	TMU113-103
	招標方式	公開招標
	決標方式	最低標
	是否依政府採購法施行細則第64條之2辦理	否
	新增公告傳輸次數	01
	是否依據採購法第106條第1項第1款辦理	否
	標案名稱	防火牆日誌紀錄器
	決標資料類別	決標公告
	是否屬共同供應契約採購	否
	是否屬二以上機關之聯合採購(不適用共同供應契約規定)	否
	是否複數決標	否
	是否共同投標	否
	是否依據採購法第99條	否

標的分類	<財物類> 452 計算機及其零件與配件
是否屬統包	否
是否應依公共工程專業技師簽證規則實施技師簽證	否
開標時間	113/11/25 17:00
原公告日期	113/11/13 原公告日期係指最近1次招標公告或更正日期
採購金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
採購金額級距	公告金額以上未達查核金額
辦理方式	補助
是否適用條約或協定之採購	是否適用WTO政府採購協定(GPA)：否 是否適用臺紐經濟合作協定(ANZTEC)：否 是否適用臺星經濟夥伴協定(ASTEP)：否
本採購是否屬「具敏感性或國安(含資安)疑慮之業務範疇」採購	否
本採購是否屬「涉及國家安全」採購	否
預算金額是否公開	否 預算金額不公開理由： 機關認為不宜公開
預算金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
是否訂有底價	是
是否受機關補助	是

項次	補助機關代碼	補助機關名稱	補助金額
1	3.9	教育部	2,389,800元 貳佰參拾捌萬玖仟捌佰元

履約地點	臺北市(非原住民地區)
履約地點（含地區）	臺北市 - 信義區

	履約標的是否包含環境保護產品	否
	本案採購契約是否採用主管機關訂定之範本	是
	本案採購契約是否採用主管機關訂定之最新版範本	財物類財物採購契約範本最新版之時間為「112.11.23」 是
	是否為政策及業務宣導業務	否
投標廠商	投標廠商家數	3
	投標廠商1	
	廠商代碼	28208184
	廠商名稱	泰瑩科技股份有限公司
	是否得標	是
	組織型態	公司登記
	廠商業別	其他
	廠商地址	105 臺北市 松山區 南京東路4段130號4樓
	廠商電話	(02) 25781133 # 202
	決標金額	1,900,000元 壹佰玖拾萬元
	得標廠商國別	中華民國(Republic of China (Taiwan))
	是否為中小企業	是
	是否為原住民個人或政府立案之原住民團體	否 預計分包予原住民個人或政府立案之原住民團體之金額： 0元 零元
	履約起迄日期	113/11/28 - 113/12/13 (預估)
	雇用員工總人數是否超過100人	否
	投標廠商2	
	廠商代碼	22644575
	廠商名稱	四海資訊股份有限公司
	是否得標	否
	組織型態	公司登記
	投標廠商3	
	廠商代碼	53099614
	廠商名稱	威尼克科技有限公司
	是否得標	否
	組織型態	公司登記
決標品項	決標品項數	1
	第1品項	
	品項名稱	防火牆日誌紀錄器
	是否以單價及預估需求數量之乘積決定最低標	否
	得標廠商1	
	得標廠商	泰瑩科技股份有限公司
	預估需求數量	1
	得標廠商原始投標金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
	決標金額	1,900,000元 壹佰玖拾萬元
	底價金額	1,980,000元 壹佰玖拾捌萬元
	標比	95.96%
	原產地國別	原產地國別 美國(United States of America) 原產地國別 1,900,000元 得標金額 壹佰玖拾萬元
	未得標廠商1	
	未得標廠商	四海資訊股份有限公司
	是否合格	是
	標價金額	2,450,000元 貳佰肆拾伍萬元

未得標原因	資格、規格合於招標文件但非最低(高)標
標價偏低理由	
未得標廠商2	
未得標廠商	威尼克科技有限公司
是否合格	是
標價金額	2,600,000元 貳佰陸拾萬元
未得標原因	資格、規格合於招標文件但非最低(高)標
標價偏低理由	

決標資料		
	決標公告序號	001
	決標日期	113/11/28
	決標公告日期	113/11/29
	契約編號	TMU113-035W
	是否刊登公報	是
	是否依據採購法第11條之1，成立採購工作及審查小組	否
	底價金額	1,980,000元 壹佰玖拾捌萬元
	底價金額是否公開	是
	總決標金額	1,900,000元 壹佰玖拾萬元
	決標金額是否係依預估條件估算之預估金額	否
	總決標金額是否公開	是
	是否依採購法第58條規定採次低標或次次低標決標	否
	契約是否訂有依物價指數調整價金規定	否，招標文件未訂物價指數調整條款 無預算
	履約執行機關	機關代碼：03724606 機關名稱：臺北醫學大學

機關主（會）計是否派員監辦	是 實地監辦
機關有關單位（機關內之政風、監查（察）、督察、檢核或稽核單位）是否派員監辦	是 實地監辦
附加說明	

核准日期:民國49年6月1日
核准文號:教育部台(49)高第6598號

地址:台北市吳興街250號
No. 250, WuXing Street, Taipei 11031 Taiwan, R.O.C
統一編號Company Tax ID: 03724606

財團法人臺北醫學大學收款收據

收執聯

日期 Date : 2024/12/06

Taipei Medical University Receipt

收據號碼 Receipt NO : AA11301632

繳款人姓名或單位名稱 Payer Name or Payer Department	泰瑩科技股份有限公司
身分證字號或統一編號 ID Card Number or Company Tax	28208184

收費項目 Charge Item	金額 Amount	收費項目 Charge Item	金額 Amount
存入保證金(履保.保固)	190,000		
以下空白			

財團法人臺北醫學大學

Taipei Medical University

總計金額 Total Amount	新臺幣 壹拾玖萬元整 (NTD$190,000)
用途說明 Instructions	防火牆日誌紀錄器

備註 Remark [票號]:KB2232932 [到期日]:2024/12/05

主辦人員 Handler : 出納組 113.12.06 黃文嘉

主辦出納 Chief Cashier : 專用收據章 主辦出納

主辦會計 Chief Accountant : 1080801 136396 專用收據章 主辦會計

校長 President : 專用收據章 臺北醫學大學校長

*本收據若經塗改或未蓋經辦人員章無效
Invalid if Altered or Altered Without Handler's Signature

七、「韌性國家醫療整備國際研討會外包場地佈置費」,擬採限制性招標方式辦理,陳請討論。

請購單位說明：

為辦理本校與衛生福利部於 113 年 11 月 30 日共同舉辦「韌性國家醫療整備書國際研討會」,考量現有人力不足並參考校院單位過往舉辦國際會議經驗,擬委由「淵暘公關管理顧問有限公司」協助提供場地佈置及人力服務,業經簽呈核可,依本校限制性招標申請單第 16 款辦理,陳請討論。

決議：同意本案採限制性招標方式辦理。

肆、採購議案：

一、「續訂學術發展評比資料庫平台」

請購單位：技術服務組,採購案號：1130203511,預算來源：校內預算 113-3202-006-101,預算金額：5,287,000元

說明：本案經校內採購招標公告網二次公告後僅「碩睿資訊有限公司」投標,且資、規格標審標結果符合招標文件規定,提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	碩睿資訊有限公司	$5,564,692	--	$5,400,000	$5,350,000	$5,270,000	$5,270,000

決議：由碩睿資訊有限公司以新台幣伍佰貳拾柒萬元整得標。

二、「研究評估分析系統暨臺北醫學大學學術知識庫暨專家研究網」

請購單位：圖書館,採購案號：1130203420,預算來源：校內預算 113-3407-003-101（依簽呈核示,本案經費後續將由深耕計畫經費支應）,預算金額：4,475,412元

說明：本案經政府電子採購網二次公告後僅「飛資得醫學資訊股份有限公司」投標,且資、規格審標結果符合招標文件規定,提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	飛資得醫學資訊股份有限公司	$4,403,424	--	$4,350,000	$4,300,000	$4,240,000	$4,240,000

決議：由飛資得醫學資訊股份有限公司以新台幣肆佰貳拾肆萬元整得標。

三、「續訂 Micromedex Healthcare Series 醫療照護系列資料庫」

請購單位：技術服務組,採購案號：1130203510,預算來源：教育部獎勵私立大學校院校務發展計畫 113-3202-002-211,預算金額：3,521,000元

說明：本案經政府電子採購網二次公告後僅「碩睿資訊有限公司」投標,且資、規格審標結果符合招標文件規定,提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	碩睿資訊有限公司	$3,705,946	--	$3,650,000	$3,600,000	$3,509,000	$3,509,000

決議：由碩睿資訊有限公司以新台幣參佰伍拾萬玖仟元整得標。

臺北醫學大學會議紀錄

會議名稱 一一三學年度採購委員會 會議次別 第九次會議

四、「訂購 ACM 及 ACP 電子書資料庫」

請購單位：技術服務組,採購案號：1130203431,預算來源：教育部獎勵私立大學校院校務發展計畫 113-3202-002-211,預算金額：3,290,000元

說明：本案經政府電子採購網二次公告後僅「碩睿資訊有限公司」投標,且資、規格審標結果符合招標文件規定,提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	碩睿資訊有限公司	$3,439,550	--	$3,400,000	$3,350,000	$3,250,000	$3,250,000

決議：由碩睿資訊有限公司以新台幣參佰貳拾伍萬元整得標。

五、「600MHz 核磁共振儀年度保固維護保養」

請購單位：共同儀器中心,採購案號：1130203435,預算來源：校內預算 113-3407-003-101,預算金額：2,300,000元

說明：本案經校內採購招標公告網二次公告後僅「台灣安捷倫科技股份有限公司」投標,且資格標審標結果符合招標文件規定,提本會進行議價。

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	台灣安捷倫科技股份有限公司	$3,468,775	--	$3,000,000	$2,500,000	$1,950,000	$1,950,000

決議：由台灣安捷倫科技股份有限公司以新台幣壹佰玖拾伍萬元整得標。

六、「防火牆日誌紀錄器」

請購單位：資訊處,採購案號：1130203887,預算來源：教育部獎勵私立大學校院校務發展計畫 113-3600-001-212,預算金額：2,389,800元

說明：本案經政府電子採購網第一次公告後共計三家廠商投標,經資、規格標審標結果三家廠商皆符合招標文件規定,提本會進行比減價。

比減價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	四海資訊股份有限公司	$2,450,000	--	$2,250,000	$2,215,000	無法再減	--
2	威尼克科技有限公司	$2,600,000	--	$2,290,000	$2,240,000	無法再減	--
3	泰瑩科技股份有限公司	$2,389,800	$2,300,000	$2,280,000	$2,230,000	$2,190,000	$1,900,000

決議：由泰瑩科技股份有限公司以新台幣壹佰玖拾萬元整得標。

七、「橫向網路流量分析系統」

請購單位：資訊處,採購案號：1130203933,預算來源：教育部獎勵私立大學校院校務發展計畫 113-3600-001-212,預算金額：1,000,000元

說明：本案經校內採購招標公告網第一次公告後共計三家廠商投標,經資、規格標審標結果三家廠商皆符合招標文件規定,提本會進行比減價。

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

比減價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	昊正科技股份有限公司	$1,010,000	--	不克到場放棄減價	--	--	--
2	動力安全資訊股份有限公司	$997,500	--	$830,000	進入底價	--	$830,000
3	精誠軟體服務股份有限公司	$855,000	$854,000	無法再減	--	--	--

決議：由動力安全資訊股份有限公司以新台幣捌拾參萬元整得標。

八、「雙和 B 基地室內裝修工程監造作業委任案」契約變更議價

請購單位：營繕組，採購案號：1110205971，預算來源：校內預算 111-3004-016-112，預算金額：13,884,899元，成交金額：12,000,000元

說明：請購單位提出契約變更，廠商提報追加酬金金額 1,433,858 元整，提本會進行議價。

追加委任酬金議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	萬有為建築師事務所	$1,433,858	--	$1,415,000	$1,400,000	進入底價	$1,400,000

決議：1.本案追加委任酬金經議價後，萬有為建築師事務所同意以新台幣壹佰肆拾萬元整承攬。

2.變更後工程款：$12,000,000+$1,400,000(追加委任酬金)=$13,400,000

3.本案以新台幣壹仟參佰肆拾萬元整辦理竣工結算。

九、「2024 年台灣醫療科技展空間設計佈置費」新增工項議價

請購單位：營運績效組，採購案號：1130201295，預算來源：管發校院基金 112-1601-002-400，預算金額：4,521,000元，成交金額：3,100,000元

說明：請購單位提出設計變更，並依原契約項目進行追加減帳，共計加帳 36,300 元，新增工項報價 503,790 元，提本會進行議價。

新增工項議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	藝創國際空間設計有限公司	$503,790	--	$450,000	$400,000	進入底價	$400,000

決議：1.本案新增工項經議價後，藝創國際空間設計有限公司同意以新台幣肆拾萬元整承攬。

2.變更後契約價款：$3,100,000+$36,300(原契約加帳)+$400,000(新增工項)=$3,536,300。

3.本案以新台幣參佰伍拾參萬陸仟參佰元整辦理驗收結算。

十、「韌性國家醫療整備國際研討會外包場地佈置費」

請購單位：管理發展中心，採購案號：1130204779，預算來源：衛生福利部 112-5400-011-300，預算金額：1,476,168元

說明：本案採限制性招標方式辦理。

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

議價紀錄

項次	廠商名稱	開標價格	優先減價	第一次減價	第二次減價	第三次減價	決標價格
1	淵暘公關管理顧問有限公司	$1,476,168	--	$1,470,000	$1,460,000	$1,400,000	$1,400,000

決議：由淵暘公關管理顧問有限公司以新台幣壹佰肆拾萬元整得標，並同意發票送達後一個月內付款。

伍、臨時動議：無

陸、結束時間：下午 03：38

臺北醫學大學
——三學年度採購委員會第九次會議
會議簽到單

日期：113年11月28日　　採購委員會會議時間：14:00~16:00
主席：吳麥斯校長　　會議地點：本校醫學綜合大樓前棟三樓第一會議室

出　席　委　員

職　稱	姓　名	簽　到
校　長	吳 麥 斯	吳麥斯
副校長	朱 娟 秀	請　假
總務長	張 正 恆	張正恆
財務長	許 淑 群	許淑群
醫學資訊研究所	邱 泓 文	邱泓文
解剖學暨細胞生物學科	馮 琮 涵	馮琮涵
牙體技術學系	林 中 魁	林中魁
管理發展中心	許 志 瑋	許志瑋
保健營養學系	簡 怡 雯	簡怡雯
藥理學科	許 銘 仁	許銘仁
中草藥臨床藥物研發博士學位學程	李 佳 蓉	李佳蓉
通識教育中心	邱 佳 慧	邱佳慧
生物化學暨細胞分子生物學科	林 俊 茂	林俊茂

列　席　人　員（職稱敬略）

單　位	姓　名	簽　到
總務處事務組	李 彥 蓉	李彥蓉

臺北醫學大學
——三學年度採購委員會第九次會議
會議簽到單

日期：113年11月28日　　採購委員會會議時間：14:00~16:00
主席：吳麥斯校長　　會議地點：本校醫學綜合大樓前棟三樓第一會議室

列　席　人　員(職稱敬略)

單　位	姓　名	簽　到
總務處事務組	劉 又 溱	劉又溱
總務處事務組	李 清 萬	李清萬
總務處事務組	方 仁 琦	方仁琦
總務處事務組	張 庭 碩	張庭碩
總務處事務組	陳 靖 怡	陳靖怡
共同儀器中心	王 淑 慧	王淑慧
圖書館	蕭 淑 媛	蕭淑媛
技術服務組	沈 純 慧	沈純慧
技術服務組	陳 雨 靜	陳雨靜
技術服務組	傅 盈 甄	傅盈甄
數位自學中心	萬 序 恬	萬序恬
資訊處	陳 暐 傑	陳暐傑
資訊處	林 芊 逸	林芊逸
資訊處	林 威 廷	林威廷
營運績效組	張 榮 岳	張榮岳
總務處營繕組	邱 丙 笙	邱丙笙
新性國家醫療整備計畫管理中心	林 姵 妤	林姵妤

應　到：13 人；實　到：12 人；請　假：1 人；出席率：92.3 %

(出席率僅計算出席人員出席率)

新增決標公告

列印時間：113/11/28 16:48:4

新增決標公告 成功

決標公告 公告日: 113/11/29

機關資料	機關代碼	03724606
	機關名稱	臺北醫學大學
	單位名稱	臺北醫學大學
	機關地址	110 臺北市 信義區 吳興街250號
	聯絡人	李清萬
	聯絡電話	(02) 27361661 # 2912
	傳真號碼	(02) 27363327
	電子郵件信箱	chingwan@tmu.edu.tw

已公告資料	標案案號	TMU113-103
	招標方式	公開招標
	決標方式	最低標
	是否依政府採購法施行細則第64條之2辦理	否
	新增公告傳輸次數	01
	是否依據採購法第106條第1項第1款辦理	否
	標案名稱	防火牆日誌紀錄器
	決標資料類別	決標公告
	是否屬共同供應契約採購	否
	是否屬二以上機關之聯合採購(不適用共同供應契約規定)	否
	是否複數決標	否
	是否共同投標	否
	是否依據採購法第99條	否
	標的分類	<財物類> 452 計算機及其零件與配件
	是否屬統包	否
	是否應依公共工程專業技師簽證規則實施技師簽證	否
	開標時間	113/11/25 17:00
	原公告日期	113/11/13 原公告日期係指最近1次招標公告或更正日期
	採購金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
	採購金額級距	公告金額以上未達查核金額
	辦理方式	補助
	是否適用條約或協定之採購	是否適用WTO政府採購協定(GPA)：否 是否適用臺紐經濟合作協定(ANZTEC)：否 是否適用臺星經濟夥伴協定(ASTEP)：否
	本採購是否屬「具敏感性或國安(含資安)疑慮之業務範疇」採購	否
	本採購是否屬「涉及國家安全」採購	否
	預算金額是否公開	否 預算金額不公開理由： 機關認為不宜公開
	預算金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
	是否訂有底價	是
	是否受機關補助	是

項次	補助機關代碼	補助機關名稱	補助金額
1	3.9	教育部	2,389,800元 貳佰參拾捌萬玖仟捌佰元

履約地點	臺北市(非原住民地區)
履約地點（含地區）	臺北市 - 信義區

	履約標的是否包含環境保護產品	否
	本案採購契約是否採用主管機關訂定之範本	是
	本案採購契約是否採用主管機關訂定之最新版範本	財物類財物採購契約範本最新版之時間為「112.11.23」 是
	是否為政策及業務宣導業務	否
投標廠商	投標廠商家數	3
	投標廠商1	
	廠商代碼	28208184
	廠商名稱	泰瑩科技股份有限公司
	是否得標	是
	組織型態	公司登記
	廠商業別	其他
	廠商地址	105 臺北市 松山區 南京東路4段130號4樓
	廠商電話	(02) 25781133 # 202
	決標金額	1,900,000元 壹佰玖拾萬元
	得標廠商國別	中華民國(Republic of China (Taiwan))
	是否為中小企業	是
	是否為原住民個人或政府立案之原住民團體	否 預計分包予原住民個人或政府立案之原住民團體之金額： 0元 零元
	履約起迄日期	113/11/28 - 113/12/13 (預估)
	雇用員工總人數是否超過100人	否
	投標廠商2	
	廠商代碼	22644575
	廠商名稱	四海資訊股份有限公司
	是否得標	否
	組織型態	公司登記
	投標廠商3	
	廠商代碼	53099614
	廠商名稱	威尼克科技有限公司
	是否得標	否
	組織型態	公司登記
決標品項	決標品項數	1
	第1品項	
	品項名稱	防火牆日誌紀錄器
	是否以單價及預估需求數量之乘積決定最低標	否
	得標廠商1	
	得標廠商	泰瑩科技股份有限公司
	預估需求數量	1
	得標廠商原始投標金額	2,389,800元 貳佰參拾捌萬玖仟捌佰元
	決標金額	1,900,000元 壹佰玖拾萬元
	底價金額	1,980,000元 壹佰玖拾捌萬元
	標比	95.96%
	原產地國別	原產地國別 美國(United States of America) 原產地國別 1,900,000元 得標金額 壹佰玖拾萬元
	未得標廠商1	
	未得標廠商	四海資訊股份有限公司
	是否合格	是
	標價金額	2,450,000元 貳佰肆拾伍萬元

未得標原因	資格、規格合於招標文件但非最低(高)標
標價偏低理由	
未得標廠商2	
未得標廠商	威尼克科技有限公司
是否合格	是
標價金額	2,600,000元 貳佰陸拾萬元
未得標原因	資格、規格合於招標文件但非最低(高)標
標價偏低理由	

決標資料		
	決標公告序號	001
	決標日期	113/11/28
	決標公告日期	113/11/29
	契約編號	TMU113-035W
	是否刊登公報	是
	是否依據採購法第11條之1，成立採購工作及審查小組	否
	底價金額	1,980,000元 壹佰玖拾捌萬元
	底價金額是否公開	是
	總決標金額	1,900,000元 壹佰玖拾萬元
	決標金額是否係依預估條件估算之預估金額	否
	總決標金額是否公開	是
	是否依採購法第58條規定採次低標或次次低標決標	否
	契約是否訂有依物價指數調整價金規定	否，招標文件未訂物價指數調整條款 無預算
	履約執行機關	機關代碼：03724606 機關名稱：臺北醫學大學

機關主（會）計是否派員監辦	是 實地監辦
機關有關單位（機關內之政風、監查（察）、督察、檢核或稽核單位）是否派員監辦	是 實地監辦
附加說明	

檔　　號：0113/S510/1
保存年限：永久

簽　於　總務處

日　　期：113年11月29日

密等及解密條件或保密期限：

附　　件：113採購委員會第09次會議-會議記錄.pdf

主旨：檢陳113學年度採購委員會第九次會議紀錄一份，詳如附件，請　鑒核。

會辦單位：

決行層級：機關首長決行

— 批核軌跡及意見 —

序	單位	職稱	姓名	意見	辦理時間
1	總務處事務組	專員	劉又溱	附件資料已更正。	113/11/29 15:12:46 承辦
2	總務處事務組	組長	李彥蓉	擬： 1. 檢陳113學年度採購委員會第九次會議紀錄。 2. 依簽呈決議辦理並存參備查。	113/11/29 15:31:50 核示
3	總務處	副總務長	沈盛達	擬如事務組所擬陳核。	113/11/29 15:43:40 核示
4	總務處	總務長	張正恆	擬如事務組所擬。陳請核示。	113/11/29 16:05:40 核示
5	秘書處	主任秘書	蔡宛真	會議記錄陳請鈞長鑒核。	113/11/30 00:18:59 核示
6	副校長室	副校長	朱娟秀	擬如主秘擬	113/11/30 06:05:02 核示
7	校長室	校長	吳麥斯	如擬 決行	113/12/02 07:03:13 決行

（主旨：檢陳113學年度採購委員會第九次會議紀錄一份，詳如附件，請　鑒核。）

8	總務處事務組	專員	劉又溱		113/12/02 07:51:03 承辦

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

時間：113 年 11 月 28 日(週四)下午 02:00
地點：本校醫學綜合大樓前棟三樓第一會議室
主席：吳麥斯校長
(以下稱謂敬略)
出席：許淑群、張正恆、李佳蓉、林中魁、許銘仁、林俊茂、馮琮涵、邱佳慧、邱泓文、簡怡雯、許志瑋
列席：李彥蓉、劉又溱、李清萬、方仁琦、陳靖怡、蕭淑媛、沈純慧、陳雨靜、傅盈甄、王淑慧、萬序恬、陳暐傑、林芊逸、林威廷、邱丙奎、張榮岳、林姵妤(陳劭綺代)
請假：朱娟秀
記錄：劉又溱

壹、主席致詞：略

貳、前次會議追蹤事項：無

參、討論案：

一、「國際磨課師平台使用費」，擬採限制性招標方式辦理，陳請討論。

請購單位說明：

因該平台為本校重要開放教育策略發展，擬委由國外廠商「FutureLearn Limited」提供平台服務壹年，優惠價每年英鎊貳萬參仟元整，業經簽呈核可，擬依本校限制性招標申請單第 16 款辦理，陳請討論。

決議：同意本案採限制性招標方式辦理，由 FutureLearn Limited 以英鎊貳萬參仟元整得標，本案須支付足額英磅（約台幣 1,035,000 元）。

二、「數位自學課程證書年費方案」，擬採限制性招標方式辦理，陳請討論。

請購單位說明：

為推動全校數位自學方案，擬續訂 Coursera 平台線上課程壹年，該平台為國外廠商「Coursera Inc.」所提供，專案優惠價每年美金肆萬壹仟捌佰肆拾參元整，業經簽呈核可，擬依本校限制性招標單第 16 款辦理，陳請討論。

決議：同意本案採限制性招標方式辦理，由 Coursera Inc.以美金肆萬壹仟捌佰肆拾參元整得標，本案須支付足額美金（約台幣 1,401,741 元）。

三、「續訂 ScienceDirect 電子期刊」，擬引用共同供應契約方式辦理，陳請討論。

請購單位說明：

1.本案為續訂電子資源且為 CONCERT 聯盟項目，由聯盟代表國內大專院校議價得優惠價（共同供應契約招標案號：STPI-P-112228），業經簽呈核可，同意以共同供應契約方式辦理，陳請討論。

2.由 Elsevier B.V.以美金 489,303.43 元整得標，本案須支付足額美金(約台幣 15,903,000 元)。

決議：同意本案引用共同供應契約方式辦理，由 Elsevier B.V.以美金肆拾捌萬玖仟參佰零參點肆參元整得標，本案須支付足額美金(約台幣 15,903,000 元)。

四、「續訂 Oxford Journals Online 電子期刊」，擬引用共同供應契約方式辦理，陳請討論。

請購單位說明：

1.本案為續訂電子資源且為 CONCERT 聯盟項目，由聯盟代表國內大專院校議價得優惠價（共同供應契約招標案號：STPI-P-112220），業經簽呈核可，同意以共同供應契約方式辦理，陳請討論。

臺北醫學大學會議紀錄

會議名稱	一一三學年度採購委員會	會議次別	第九次會議

2.由 Oxford University Press 以美金 53,865 元整得標，本案須支付足額美金（約台幣 1,751,000 元）。

決議：同意本案引用共同供應契約方式辦理，由 Oxford University Press 以美金伍萬參仟捌佰陸拾伍元整得標，本案須支付足額美金(約台幣 1,751,000 元)。

五、「雙和 B 基地室內裝修工程監造作業委任案」，擬辦理契約變更，陳請討論。

請購單位說明：

1.本案業經 111 學年度採購委員會第 18 次會議決議，由萬有為建築師事務所以新台幣壹仟貳佰萬元整得標。

2.依契約第十三條第一項：「甲方於必要時得通知乙方變更本契約，乙方於接獲通知後，除雙方另有協議外，應於 10 日內向甲方提出服務範圍、委任酬金、履約期限、付款辦法或其他本契約內容須變更之相關文件，並依甲方相關辦法辦理採購變更後，始得為之」。本案契約範圍共 19 件裝修工程案，其中 16 案辦理採購工程變更，致裝修工程契約總價及監造作業內容增加，故通知萬有為建築師事務所變更契約，裝修工程採購變更內容說明如下：

(1)19 案裝修工程原契約總價：1,291,180,000 元整
(2)16 案裝修工程案進行採購變更，變更之追加、追減及新增工項金額如下：
A.原契約追加金額計：35,589,699 元整
B.原契約追減金額計：70,120,172 元整
C.新增項目金額計：48,570,884 元整

3.萬有為建築師事務所依契約規定提報變更相關文件及追加委任酬金金額為 1,433,858 元，陳請討論。

決議：同意本案契約變更並增加委任酬金，另進行追加委任酬金議價。

六、「2024 年台灣醫療科技展空間設計佈置費」，擬辦理設計變更，陳請討論。

請購單位說明：

1.本案業經 113 學年度採購委員會第 5 次會議決議，由藝創國際空間設計有限公司以新台幣參佰壹拾萬元整得標。

2.依契約第十條契約之變更：「本契約書之所有約款，在任何方面均不得放棄、更改、修改或增訂，除非經甲乙雙方或其所授權之人書面簽署外，其它任何口頭或書面之變更，增刪約款之約定，均不生拘束或規範當事人間之效力。如果在任何時刻乙方預見原定之計畫時程將有延誤，不論是因為甲方所要求之服務上的變更，還是因其他非乙方可控制之原因，乙方應告知甲方，並經甲乙雙方一致同意後修改計畫時程。任何變更所導致的費用變更應反應於變更指示中。」

3.因 10/18 討論會議決議調整展出方向，同時調整整體攤位架構，並請廠商重新繪製圖面及 3D 圖，依與大會協調時程 11/8 重新提交醫療展主辦單位攤位架構認證申請，依此相關變更說明如下：

(1)追加項目：42 吋觸控電視增加 1 台與 65 吋觸控電視 6 台，共計加帳 80,400 元整。
(2)追減項目：42 吋壁掛式減少 9 台，共計減帳 44,100 元整。
(3)新增項目：為符合參展需求新增工項，廠商報價 503,790 元。

4.綜上，經請購單位及事務組依原契約項目單價核算後，共計加帳 36,300 元整，新增工項後續另進行議價，陳請討論。

決議：同意本案設計變更，原契約共計加帳新台幣參萬陸仟參佰元整，另進行新增工項議價。

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 開標/議價/決標/~~流標/廢標~~紀錄

時間：113 年 11 月 28 日下午 02 時 00 分　　地點：本校醫學綜合大樓前棟三樓第一會議室

審標結果 ~~/流標原因~~ ~~/廢標原因~~	一、本案一次公告後投標廠商計 3 家，開標前合格投標廠商計 3 家，審標結果 3 家符合招標文件規定，其餘 0 家不合格。 二、泰瑩科技股份有限公司報價（減價後）新臺幣（下同）1,900,000 元整最低，且在底價新臺幣 1,980,000 元整以內，依政府採購法第 52 條第 1 項第 1 款。 三、☐投標廠商未達 3 家，經主持人當場宣布流標。 四、☐開標後經審標結果，無得為決標對象之廠商，經主持人當場宣布廢標。 五、其他：本案經政府電子採購網第一次公告後共計三家廠商投標，且經資、規格標審標結果，三家廠商皆符合招標文件規定，提本會進行比減價。	
決標原則、得標廠商及決標金額	決標原則：依政府採購法第 52 條第 1 項第 1 款。 得標廠商：泰瑩科技股份有限公司 決標金額：新台幣 X 仟 壹 佰 玖 拾 X 萬 X 仟 X 佰 X 拾 元整。(含稅)(中文大寫) 押標金：新台幣 $119,000 元整。 履約保證金：☐同押標金 ■ **契約金額之一定比率 10%**。 保固期限：■ 一 年 ☐無保固。 其他： （超底價決標時須另註明超底價之金額、比率及必須決標之緊急情事）	得標廠商代表簽名(或蓋章) [stamps] （不通知投標廠商到場者，免簽名或蓋章）
決標過程	請參詳上表。 （註明減價/比減價格/超底價決標/協商/綜合評選之過程）	
異議或申訴事件	無 （註明尚未解決之異議或申訴事件之處理情形）	
備註		

主持人	[signature]（簽章）	監辦人員（依規定由本校財務處人員擔任）	主辦會計 許淑群（簽章）
請購單位人員	[signature]（簽章）	記錄	劉又溱 113.11.28（簽章）
事務組經辦人員	李清萬 113.11.28（簽章）	事務組組長	[signature]（簽章）
採購委員 ☐採購小組會 ■採購委員會	※事務組議價會則免簽。 [signatures]（簽章）		

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

開標/議價/決標/~~流標/廢標~~紀錄

時間：113 年 11 月 28 日下午 02 時 00 分　　地點：本校醫學綜合大樓前棟三樓第一會議室

採購案號	1130213887		請購單位	資訊處	
標的名稱及數量摘要	防火牆日誌紀錄器		開標次別	第一次	
公告日期	113/11/13		招標方式	■公開招標□限制性招標	
投標廠商	標價	優先減價後之標價	第一次比減價格後之標價	第二次比減價格後之標價	第三次比減價格後之標價
四海資訊股份有限公司	$ 1,450,000	--	$ 1,250,000	$ 1,215,000	$ 無法再減
威尼克科技有限公司	$ 1,600,000	--	$ 1,290,000	$ 1,240,000	$ 無法再減
泰瑩科技股份有限公司	$ 1,389,800	$ 1,300,000	$ 1,280,000	$ 1,230,000	$ 1,190,000

本校（以下簡稱甲方）與得標廠商（以下簡稱乙方）同意就首揭財物議定下列條款：

一、經開標議、比價後，以■含稅價格新台幣$1,900,000元決標。　□以CIP＿＿＿＿＿決標。（開標當日依決標前一辦公日臺灣銀行外匯交易收盤即期賣出匯率為1：＿＿＿；如匯率超過1：＿＿＿＿，其差額由廠商負擔。）

二、乙方應於決標翌日起十四個工作天內繳交履約保證金新臺幣 **契約金額之一定比率10%**。

三、乙方須於■民國＿＿年＿＿月＿＿日以前提供履約標的之供應(□含安裝測試)。□結匯計算單開出後＿＿＿天內交貨■其他：廠商應於113年12月13日前完成交貨安裝測試　。

四、雙方同意■另訂契約(本紀錄視為契約之一部分)。　□本紀錄視同契約。

五、保固期限：□無保固　■自驗收合格之日起，■保固一年□保固＿＿＿年□其他＿＿＿＿＿＿；■保固保證金以成交金額3%計算。

六、如屬財物採購，乙方須負責運送及安裝，國外採購案並須負擔開狀、結匯、提貨、倉租等相關費用。

七、其他約定條款如後：

1. 乙方保證金：履約完成，驗收合格且無待解決事項後無息發還，如乙方對甲方負有因本紀錄而生之債務，甲方就乙方所繳保證金有優先扣抵之權。
2. 交貨/履約地點：交貨地點為甲方所在地或甲方指定之場所，如貨品於裝運途中，因裝箱不良等原因，在開箱清點時發現有破損時，乙方應負責照數賠償。
3. 驗收：乙方於可得驗收時，應通知甲方辦理驗收。乙方所交貨品或履約結果，如經甲方驗收使用結果發現內容與原附圖說資料，及甲方所審定規格不符或性能效果不佳時，均應限期無條件調換、改善、拆除、重作、退貨或換貨(以下簡稱改正)，其一切損失應由乙方自理。如未在調換期限內交貨或逾期未改正者，概按照逾期違約金之規定辦理。
4. 逾期違約金：乙方如未依照規定期限履約，□應按逾期日數，每日依全部契約價金總額3‰計算支付逾期違約金予甲方。□但未完成履約之部分不影響其他已完成部分之使用者，得按未完成履約部分之契約價金，每日依其3‰計算逾期違約金。■其他依契約內文所示。逾期違約金總額，以全部契約價金總額之百分之二十為上限，甲方得自應付價金中扣抵，其有不足者，通知乙方繳納或自保證金扣抵。但遇天災或事變等不可抗力或不可歸責於乙方之事由提有證明者，經甲方查明同意，確非人力所能抗拒者，不在此限。如逾期達三十天，乙方無正當理由而不履行契約者，甲方得解除契約，乙方所繳納之保證金不予發還。
5. 付款辦法：□驗收合格後一次付款 □分期付款，條件：＿＿＿＿＿＿＿＿ □契約訂妥並俟外匯核准後，開發信用狀 ■其他依契約內文所示。
6. 如有押標金，押標金不予發還之情形，依政府採購法第三十一條第二項規定辦理。
7. 本紀錄如有未規定事項，悉依政府採購法及民法等相關法令規定辦理。
8. 乙方於國內員工總人數逾一百人，履約期間僱用身心障礙者及原住民人數各應達國內員工總人數百分之一，並均以整數為計算標準，未達整數部分不予計入。僱用不足者，應分別依規定向所在地之直轄市或縣（市）勞工主管機關設立之身心障礙者就業基金專戶及原住民中央主管機關設立之原住民族就業基金專戶，繳納上月之代金；並不得僱用外籍勞工取代僱用不足額部分。甲方應將國內員工總人數逾一百人之乙方資料公開於政府採購資訊公告系統，以供勞工及原住民主管機關查核代金繳納情形，甲方不另辦理查核。

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

廠商投標議比價單

議價日期	中華民國一一三年十一月二十八日
議價地點	本校醫學綜合大樓前棟三樓第一會議室
議價會議	一一三學年度採購委員會第九次會議
請購單位	資訊處
採購名稱	防火牆日誌紀錄器
交貨期	依投標須知及標單相關規定
備註	※標價需含營業稅額。 ※標價含開狀手續費、報關費、提貨、倉租及將貨運至本校請購單位指定地點等所需之一切費用並需含安裝、裝機完成。 ※結匯金額以所議定之新臺幣金額為上限，期間若因匯率變動致結匯金額超過概由乙方補足，若另有議定條件則不在此限。

議比價記錄

開標價格	優先減價	第一次比減價	第二次比減價	第三次比減價
NT$2,389,800	NT$2,300,000 ※「開標價格」最低者可享有優先減價權。	NT$2,280,000 ※需低於優先減價，否則請註明「無法再減」字樣。	NT$2,230,000	NT$2,190,000

決標價格：新台幣 壹佰玖拾 ~~萬 仟 佰 拾~~ 元整。(含稅)

※附加條件：

1. _____。
2. _____。
3. _____。
4. _____。

投標廠商資料

投標廠統編：28208184

投標廠名稱：泰瑩科技股份有限公司

投標代表人：陳好嘉

投標商電話：0908590611

投標商地址：台北市南京東路四段[illegible]

投標廠商蓋章

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

廠商投標議比價單

議價日期	中華民國一一三年十一月二十八日
議價地點	本校醫學綜合大樓前棟三樓第一會議室
議價會議	一一三學年度採購委員會第九次會議
請購單位	資訊處
採購名稱	防火牆日誌紀錄器
交貨期	依投標須知及標單相關規定
備註	※標價需含營業稅額。 ※標價含開狀手續費、報關費、提貨、倉租及將貨運至本校請購單位指定地點等所需之一切費用並需含安裝、裝機完成。 ※結匯金額以所議定之新臺幣金額為上限，期間若因匯率變動致結匯金額超過概由乙方補足，若另有議定條件則不在此限。

議比價記錄

開標價格	優先減價	第一次比減價	第二次比減價	第三次比減價
NT$245000/	NT$ ※「開標價格」最低者可享有優先減價權。	NT$225000/ ※需低於優先減價，否則請註明「無法再減」字樣。	NT$221500/	NT$無法再減
決標價格	新台幣 佰 拾 萬 仟 佰 拾 元整。(含稅)			

※附加條件：

1. _____。
2. _____。
3. _____。
4. _____。

投標廠商資料	
	投標廠統編：22644575
	投標廠名稱：四海資訊(股)公司
	投標代表人：林高泰
	投標商電話：0919589796
	投標商地址：台中市北屯區陳平路110巷46-3號

投標廠商蓋章：四海資訊股份有限公司 陳

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

廠商投標議比價單

議價日期	中華民國一一三年十一月二十八日
議價地點	本校醫學綜合大樓前棟三樓第一會議室
議價會議	一一三學年度採購委員會第九次會議
請購單位	資訊處
採購名稱	防火牆日誌紀錄器
交貨期	依投標須知及標單相關規定
備註	※標價需含營業稅額。 ※標價含開狀手續費、報關費、提貨、倉租及將貨運至本校請購單位指定地點等所需之一切費用並需含安裝、裝機完成。 ※結匯金額以所議定之新臺幣金額為上限，期間若因匯率變動致結匯金額超過概由乙方補足，若另有議定條件則不在此限。

議比價記錄

開標價格	優先減價	第一次比減價	第二次比減價	第三次比減價
NT$2600000	NT$ ※「開標價格」最低者可享有優先減價權。	NT$2290000 ※需低於優先減價，否則請註明「無法再減」字樣。	NT$ 2240000	NT$ 無法再減

決標價格：新台幣 佰 拾 萬 仟 佰 拾 元整。(含稅)

※附加條件：

1. _____。
2. _____。
3. _____。
4. _____。

投標廠商資料

投標廠統編：53099614

投標廠名稱：威尼克科技有限公司

投標代表人：程伯勳

投標商電話：028660378

投標商地址：新北市永和區中山路一段267號3樓

投標廠商蓋章

□正本
□副本

財務採購契約

採購名稱：防火牆日誌紀錄器

契約編號：TMU113-035W

廠　　商：泰瑩科技股份有限公司

財物採購契約範本

(112.11.23 版本)

招標機關**臺北醫學大學**(以下簡稱機關)及得標廠商 **泰瑩科技股份有限公司**(以下簡稱廠商)雙方同意依政府採購法(以下簡稱採購法)及其主管機關訂定之規定訂定本契約，共同遵守，其條款如下：

第一條　契約文件及效力

(一)契約包括下列文件：

1. 招標文件及其變更或補充。
2. 投標文件及其變更或補充。
3. 決標文件及其變更或補充。
4. 契約本文、附件及其變更或補充。
5. 依契約所提出之履約文件或資料。

(二)契約文件，包括以書面、錄音、錄影、照相、微縮、電子數位資料或樣品等方式呈現之原件或複製品。

(三)契約所含各種文件之內容如有不一致之處，除另有規定外，依下列原則處理：

1. 招標文件內之投標須知及契約條款優於招標文件內之其他文件所附記之條款。但附記之條款有特別聲明者，不在此限。
2. 招標文件之內容優於投標文件之內容。但投標文件之內容經機關審定優於招標文件之內容者，不在此限。招標文件如允許廠商於投標文件內特別聲明，並經機關於審標時接受者，以投標文件之內容為準。
3. 文件經機關審定之日期較新者優於審定日期較舊者。
4. 大比例尺圖者優於小比例尺圖者。
5. 決標紀錄之內容優於開標或議價紀錄之內容。
6. 同一優先順位之文件，其內容有不一致之處，屬機關文件者，以對廠商有利者為準；屬廠商文件者，以對機關有利者為準。
7. 本契約之附件與本契約內之廠商文件，其內容與本契約條文有歧異者，除對機關較有利者外，其歧異部分無效。
8. 招標文件內之標價清單，其品項名稱、規格、數量，優於招標文件內其他文件之內容。

(四)契約文件之一切規定得互為補充，如仍有不明確之處，應依公平合理原則解釋之。如有爭議，依採購法之規定處理。

(五)契約文字：

1. 契約文字以中文為準。但下列情形得以外文為準：

(1)特殊技術或材料之圖文資料。

(2)國際組織、外國政府或其授權機構、公會或商會所出具之文件。

(3)其他經機關認定確有必要者。

2. 契約文字有中文譯文，其與外文文意不符者，除資格文件外，以中文為準。其因譯文有誤致生損害者，由提供譯文之一方負責賠償。

3. 契約所稱申請、報告、同意、指示、核准、通知、解釋及其他類似行為所為之意思表示，除契約另有規定或當事人同意外，應以中文(正體字)書面為之。書面之遞交，得以面交簽收、郵寄、傳真或電子資料傳輸至雙方預為約定之人員或處所。

(六)契約所使用之度量衡單位，除另有規定者外，以法定度量衡單位為之。

(七)契約所定事項如有違反法令或無法執行之部分，該部分無效。但除去該部分，契約亦可成立者，不影響其他部分之有效性。該無效之部分，機關及廠商必要時得依契約原定目的變更之。

(八)經雙方代表人或其授權人簽署契約正本2份，機關及廠商各執1份，並由雙方各依印花稅法之規定繳納印花稅。副本2份(請載明)，由機關、廠商及相關機關、單位分別執用。副本如有誤繕，以正本為準。

第二條　履約標的

(一)廠商應給付之標的及工作事項(由機關於招標時載明)：**防火牆日誌紀錄器(詳招標規格書)**

(二)機關辦理事項(由機關於招標時載明，無者免填)：＿＿＿＿＿＿＿＿

第三條　契約價金之給付

■新臺幣壹佰玖拾萬元整(含稅)

契約價金之給付，得為下列方式(由機關擇一於招標時載明)：

■依契約價金總額結算。因契約變更致履約標的項目或數量有增減時，就變更部分予以加減價結算。若有相關項目如稅捐、利潤或管理費等另列一式計價者，應依結算總價與原契約價金總額比例增減之。但契約已訂明不適用比例增減條件，或其性質與比例增減無關者，不在此限。

□依實際供應之項目及數量結算，以契約中所列履約標的項目及單價，依完成履約實際供應之項目及數量給付。若有相關項目如稅捐、利潤或管理費等另列一式計價者，應依結算總價與原契約價金總額比例增減之。但契約已訂明不適用比例增減條件，或其性質與比例增減無關者，不在此限。

□部分依契約價金總額結算，部分依實際供應之項目及數量結算。屬於依

契約價金總額結算之部分，因契約變更致履約標的項目或數量有增減時，就變更部分予以加減價結算。屬於依實際供應之項目及數量結算之部分，以契約中所列履約標的項目及單價，依完成履約實際供應之項目及數量給付。若有相關項目如稅捐、利潤或管理費等另列一式計價者，應依結算總價與契約價金總額比例增減之。但契約已訂明不適用比例增減條件，或其性質與比例增減無關者，不在此限。

□其他：_____

第四條　契約價金之調整

(一)驗收結果與規定不符，而不妨礙安全及使用需求，亦無減少通常效用或契約預定效用，經機關檢討不必拆換、更換或拆換、更換確有困難者，得於必要時減價收受。

1. 採減價收受者，按不符項目標的之契約單價 20%（由機關視需要於招標時載明；未載明者，依採購法施行細則第 98 條第 2 項規定）與不符數量之乘積減價，並處以減價金額___%(由機關視需要於招標時載明；未載明者為 20%)之違約金。但其屬尺寸不符規定者，減價金額得就尺寸差異之比率計算之；屬工料不符規定者，減價金額得按工料差額計算之；非屬尺寸、工料不符規定者，減價金額得就重量、權重等差異之比率計算之。
2. 個別項目減價及違約金之合計，以標價清單或詳細價目表該項目所載之複價金額為限。

(二)依契約價金總額結算給付者，未列入標價數量清單之項目或數量，其已於契約載明應由廠商供應或為廠商完成履約所必須者，仍應由廠商負責供應，不得據以請求加價。如經機關確認屬漏列且未於其他項目中編列者，應以契約變更增加契約價金。

(三)契約價金，除另有規定外，含廠商及其人員依中華民國法令應繳納之稅捐、規費及強制性保險之保險費。依法令應以機關名義申請之許可或執照，由廠商備具文件代為申請者，其需繳納之規費不含於契約價金，由廠商代為繳納後機關覈實支付，但已明列項目而含於契約價金者，不在此限。

(四)中華民國以外其他國家或地區之稅捐、規費或關稅，由廠商負擔。

(五)廠商履約遇有下列政府行為之一，致履約費用增加或減少者，契約價金得予調整：

1. 政府法令之新增或變更。
2. 稅捐或規費之新增或變更。

3. 政府公告、公定或管制費率之變更。

(六)前款情形，屬中華民國政府所為，致履約成本增加者，其所增加之必要費用，由機關負擔；致履約成本減少者，其所減少之部分，得自契約價金中扣除。其他國家政府所為，致履約成本增加或減少者，契約價金不予調整。

(七)廠商為履約須進口自用機具、設備或材料者，其進口及復運出口所需手續及費用，由廠商負責。

(八)契約規定廠商履約標的應經第三人檢驗者，除另有規定外，其檢驗所需費用，由廠商負擔。

第五條　契約價金之給付條件

(一)除契約另有約定外，依下列條件辦理付款：

1. 預付款(無者免填)：

(1)契約預付款為契約價金總額____%(由機關於招標時載明；其額度以不逾契約價金總額或契約價金上限之30%為原則)，付款條件如下：_____(由機關於招標時載明)。

(2)預付款於雙方簽定契約，廠商辦妥履約各項保證，並提供預付款還款保證，經機關核可後在___日(由機關於招標時載明)內撥付。

(3)預付款應於銀行開立專戶，專用於本採購，機關得隨時查核其使用情形。

(4)預付款之扣回方式如下：_____(由機關於招標時載明；無者免填)。

2. 分期付款(無者免填)：

(1)契約分期付款為契約價金總額____%(由機關於招標時載明)，其各期之付款條件：_____(由機關於招標時載明)

(2)廠商於符合前述各期付款條件後提出證明文件及預付款還款保證(契約未約定預付款還款保證者則免)。機關於15工作天內完成審核程序後，通知廠商提出請款單據，並於接到廠商請款單據後15工作天內付款。但涉及向補助機關申請核撥補助款者，付款期限為30工作天。

3. 分批付款(由機關視需要於招標時載明，無者免填)：

□分批交貨，分批付款，每批數交貨完畢後付款。廠商於符合前述付款條件後提出證明文件。機關於15工作天內完成審核程序後，通知廠商提出請款單據，並於接到廠商請款單據後 15 工作天內付款。但涉及向補助機關申請核撥補助款者，付款期限為30工作天。

□得分批交貨，但全部批數交貨完畢後付款。廠商於符合前述付款條件後提出證明文件。機關於 15 工作天內完成審核程序後，通知廠商提出請款單據，並於接到廠商請款單據後 15 工作天內付款。但涉及向補助機關申請核撥補助款者，付款期限為 30 工作天。

4. 訓練費之付款(由機關視需要於招標時載明，無者免填)：

□訓練完成後付款。廠商於符合前述付款條件後提出證明文件。機關於 15 工作天內完成審核程序後，通知廠商提出請款單據，並於接到廠商請款單據後 15 工作天內付款。但涉及向補助機關申請核撥補助款者，付款期限為 30 工作天。

□其他：_____（由機關於招標時載明）。

5. 安裝測試費之付款(由機關視需要於招標時載明，無者免填)：

□安裝測試完成後付款。廠商於符合前述付款條件後提出證明文件。機關於 15 工作天內完成審核程序後，通知廠商提出請款單據，並於接到廠商請款單據後 15 工作天內付款。但涉及向補助機關申請核撥補助款者，付款期限為 30 工作天。

□其他：_____（由機關於招標時載明）。

6. ■**驗收後付款：於驗收合格，廠商繳納保固保證金（契約未明定需繳納保固保證金者則免）後，機關於接到廠商提出請款單據後按機關付款流程付款。但涉及向補助機關申請核撥補助款者，依撥款時程及機關付款流程付款。**

7. 其他付款條件：_____

8. 機關辦理付款及審核程序，如發現廠商有文件不符、不足或有疑義而需補正或澄清者，機關應一次通知澄清或補正，不得分次辦理。其審核及付款期限，自資料澄清或補正之次日重新起算；機關並應先就無爭議且可單獨計價之部分辦理付款。

9. 廠商履約有下列情形之一者，機關得暫停給付契約價金至情形消滅為止：

(1)履約實際進度因可歸責於廠商之事由，落後預定進度達__%（由機關於招標時載明，未載明者為 20%）以上，且經機關通知限期改善未積極改善者。

(2)履約有瑕疵經書面通知改善而逾期未改善者。

(3)未履行契約應辦事項，經通知仍延不履行者。

(4)廠商履約人員不適任，經通知更換仍延不辦理者。

(5)其他違反法令或契約情形。

10. 物價指數調整(無者免填)：

(1)履約進行期間，如遇物價波動時，得依行政院主計總處公布之物價指數_____(由機關載明指數名稱)，就漲跌幅超過5%之部分，調整契約價金(由機關於招標時載明得調整之標的項目)。

(2)適用物價指數基期更換者，其換基當月起完成之履約標的，自動適用新基期指數核算履約標的調整款，原依舊基期指數結清之履約標的款不予追溯核算。每月公布之物價指數修正時，處理原則亦同。

11. 契約價金得依前目或_____(如指定指數，由機關於招標時載明，無者免填)調整者，應註明下列事項：

(1)得調整之成本項目及金額。

(2)調整所依據之一定物價指數及基期。

(3)得調整及不予調整之情形。

(4)調整公式。

(5)廠商應提出之調整數據及佐證資料。

(6)管理費及利潤不予調整。

(7)逾履約期限之部分，以契約規定之履約期限當時之物價指數(如指定指數，由機關於招標時載明，無者免填)為當期資料。但逾期履約係可歸責於機關者，不在此限。

12. 契約價金總額曾經減價而確定，其所組成之各單項價格得依約定或合意方式調整（例如減價之金額僅自部分項目扣減）；未約定或未能合意調整方式者，如廠商所報各單項價格未有不合理之處，視同就廠商所報各單項價格依同一減價比率（決標金額/投標金額）調整。投標文件中報價之分項價格合計數額與決標金額不同者，依決標金額與該合計數額之比率調整之。但人力項目之報價不隨之調低。

13. 廠商計價領款之印章，除另有約定外，以廠商於投標文件所蓋之章為之。

14. 廠商應依身心障礙者權益保障法、原住民族工作權保障法及採購法規定僱用身心障礙者及原住民。僱用不足者，應依規定分別向所在地之直轄市或縣（市）勞工主管機關設立之身心障礙者就業基金及原住民族中央主管機關設立之原住民族綜合發展基金之就業基金，定期繳納差額補助費及代金；並不得僱用外籍勞工取代僱用不足額部分。招標機關應將國內員工總人數逾100人之廠商資料公開於政府電子採購網，以供勞工及原住民族主管機關查核差額補助費

及代金繳納情形，招標機關不另辦理查核。

15. 契約價金總額，除另有規定外，為完成契約所需全部材料、人工、機具、設備及施工所必須之費用。

16. 因非可歸責於廠商之事由，機關有延遲付款之情形，廠商投訴對象：

(1)採購機關之政風單位；

(2)採購機關之上級機關；

(3)法務部廉政署；

(4)採購稽核小組；

(5)採購法主管機關；

(6)行政院主計總處。

(二)廠商請領契約價金時應提出電子或紙本統一發票，依法免用統一發票者應提出收據。

(三)廠商請領契約價金時應提出之其他文件為(由機關於招標時載明，無者免填)：

□外國廠商之商業發票。

□成本或費用證明。

□海運、空運提單或其他運送證明。

□送貨簽收單。

□裝箱單。

□重量證明。

□檢驗或檢疫證明。

□保險單或保險證明。

■保固證明。

□契約規定之其他給付憑證文件(若有規範)。

(四)前款文件，應有出具人之簽名或蓋章。但慣例無需簽名或蓋章者，不在此限。

(五)履約標的自中華民國境外輸入，契約允許以不可撤銷信用狀支付外國廠商契約價金，廠商遲延押匯或所提示之文件不符契約或信用狀規定，致機關無法提貨時，不論機關是否辦理擔保提貨，其因此而發生之額外倉租及其他費用，概由廠商負擔。

(六)廠商履約有逾期違約金、損害賠償、採購標的損壞或短缺、不實行為、未完全履約、不符契約規定、溢領價金或減少履約事項等情形時，機關得自應付價金中扣抵；其有不足者，得通知廠商給付或自保證金扣抵。

(七)履約範圍包括代辦訓練操作或維護人員者，其費用除廠商本身所需者外，有關受訓人員之旅費及生活費用，由機關自訂標準支給，不包括在

契約價金內。

(八)分包契約依採購法第 67 條第 2 項報備於機關，並經廠商就分包部分設定權利質權予分包廠商者，該分包契約所載付款條件應符合本條前列各款規定(採購法第 98 條之規定除外)，或與機關另行議定。

(九)廠商於履約期間給與全職從事本採購案之員工薪資，如採按月計酬者，至少為_____元（由機關於招標時載明，不得低於勞動基準法規定之最低基本工資；未載明者，為新臺幣 3 萬元）。

第六條　稅捐

(一)以新臺幣報價之項目，除招標文件另有規定外，應含稅，包括營業稅。由自然人投標者，不含營業稅，但仍包括其必要之稅捐。

(二)廠商為進口施工或測試設備、臨時設施、於我國境內製造財物所需設備或材料、換新或補充前已進口之設備或材料等所生關稅、貨物稅及營業稅等稅捐、規費，由廠商負擔。

(三)進口財物或臨時設施，其於中華民國以外之任何稅捐、規費或關稅，由廠商負擔。

第七條　履約期限

(一)履約期限(由機關於招標時載明)：

■廠商應於 113 年 12 月 13 日以前或(□決標次日□機關簽約日□機關通知日□收到信用狀日)起___天內將採購標的送達**機關**指定之場所/完成安裝測試(交易條件)。

□廠商應於__年__月__日以前或(□決標日□簽約日□收到信用狀日)起__天/月內將採購標的送達____(指定之場所)，安裝測試完畢，且測試結果符合契約規定。

□分批交貨之期限：_____

□完成交貨之期限：_____

□完成安裝測試之期限：_____

□其他：_____

(二)測試期間(無者免填)：_____

(三)本契約所稱日(天)數，除已明定為日曆天或工作天者外，以■日曆天□工作天計算(由機關於招標時勾選；未勾選者，為日曆天)：

1. 以日曆天計算者，所有日數均應計入。

2. 以工作天計算者，下列放假日，均應不計入：

(1)星期六（補行上班日除外）及星期日。但與(2)至(6)放假日相互重疊者，不得重複計算。

(2)中華民國開國紀念日（1月1日）、和平紀念日（2月28日）、兒童節（4月4日，放假日依「紀念日及節日實施辦法」規定）、勞動節（5月1日）、國慶日（10月10日）。

(3)勞動節之補假（依勞動部規定）；軍人節（9月3日）之放假及補假（依國防部規定，但以國軍之採購為限）。

(4)農曆除夕及補假、春節及補假、民族掃墓節、端午節、中秋節。

(5)行政院人事行政總處公布之調整放假日及補假。

(6)全國性選舉投票日及行政院所屬中央各業務主管機關公告放假者。

3. 履約項目如包括工程之施工，免計工作天之日，以不得施工為原則。廠商如欲施工，應先徵得機關書面同意，該日數□應；□免計入履約期限（由機關於招標時勾選，未勾選者，免計入履約期限）。

4. 其他：_____（由機關於招標時載明）。

□前述期間全天之工作時間為上午___時___分至下午____時____分，中午休息時間為中午____時____分至下午____時____分；半天之工作時間為上午____時____分至下午____時____分。

(四)契約如需辦理變更，其履約標的項目或數量有增減時，變更部分之履約期限由雙方視實際需要議定增減之。不受增減項目或數量影響之部分，契約原約定之履約期限不予變更。

(五)履約期限展延：

1. 履約期限內，有下列情形之一，且確非可歸責於廠商，而需展延履約期限者，廠商應於事故發生或消失後__日內（由機關於招標時載明；未載明者，為7日）通知機關，並檢具事證，以書面向機關申請展延履約期限。機關得審酌其情形後，以書面同意延長履約期限，不計算逾期違約金。其事由未逾半日者，以半日計；逾半日未達1日者，以1日計。

(1)發生契約規定不可抗力之事故。

(2)因天候影響無法施工。

(3)機關要求全部或部分暫停履約。

(4)因辦理契約變更或增加履約標的數量或項目。

(5)機關應辦事項未及時辦妥。

(6)由機關自辦或機關之其他廠商因承包契約相關履約標的之延誤而影響契約進度者。

(7)其他非可歸責於廠商之情形，經機關認定者。

2. 前目事故之發生，致契約全部或部分必須停止履約時，廠商應於停

止履約原因消滅後立即恢復履約。其停止履約及恢復履約，廠商應儘速向機關提出書面報告。

(六)期日：

1. 履約期間自指定之日起算者，應將當日算入。履約期間自指定之日後起算者，當日不計入。
2. 履約標的須於一定期間內送達機關之場所者，履約期間之末日，以機關當日下班時間為期間末日之終止。當日為機關之辦公日，但機關因故停止辦公致未達原定截止時間者，以次一辦公日之同一截止時間代之。

(七)廠商履約交貨之批數如下(由機關視需要於招標時載明，無者免填)。

■一次交清。

□分____批交貨。

第八條　履約管理

(一)與契約履約標的有關之其他標的，經機關交由其他廠商承包時，廠商有與其他廠商互相協調配合之義務，以使該等工作得以順利進行。因工作不能協調配合，致生錯誤、延誤履約期限或意外事故，其可歸責於廠商者，由廠商負責並賠償。受損之一方應於事故發生後儘速書面通知機關，由機關邀集雙方協調解決。

(二)履約標的未經驗收移交機關前，所有已完成之履約標的及到場之材料、機具、設備，包括機關供給及廠商自備者，均由廠商負責保管。如有損壞缺少，概由廠商負責。其屬經機關已估驗計價者，由廠商賠償。部分業經驗收付款者，其所有權屬機關，禁止轉讓、抵押、出租、任意更換或其他有害所有權行使之行為。

(三)履約標的未經驗收前，機關因需要使用時，廠商不得拒絕。但應由雙方會同使用單位協商認定權利與義務後，由機關先行接管。使用期間因非可歸責於廠商之事由，致遺失或損壞者，應由機關負責。

(四)契約所需履約標的材料、機具、設備、工作場地設備等，除契約另有規定外，概由廠商自備。

(五)前款工作場地設備，指廠商為契約履約之場地或履約地點以外專為契約材料加工之場所之設備，包括履約管理、工人住宿、材料儲放等房舍及其附屬設施。該等房舍設施，應具備滿足工作人員生活與工作環境所必要的條件。

(六)廠商自備之材料、機具、設備，其品質應符合契約之規定，進入機關履約場所後由廠商負責保管。非經機關許可，不得擅自運離。

(七)各項設施或設備，依法令規定須由專業技術人員安裝、履約或檢驗者，廠商應依規定辦理。

(八)廠商接受機關或機關委託之機構之人員指示辦理與履約有關之事項前，應先確認該人員係有權代表人，且所指示辦理之事項未逾越或未違反契約規定。廠商接受無權代表人之指示或逾越或違反契約規定之指示，不得用以拘束機關或減少、變更廠商應負之契約責任，機關亦不對此等指示之後果負任何責任。

(九)契約之一方未請求他方依契約履約者，不得視為或構成一方放棄請求他方依契約履約之權利。

(十)契約內容有須保密者，廠商未經機關書面同意，不得將契約內容洩漏予與履約無關之第三人。

(十一)廠商履約期間所知悉之機關機密或任何不公開之文書、圖畫、消息、物品或其他資訊，均應保密，不得洩漏。

(十二)轉包及分包：

1. 廠商不得將契約轉包。廠商亦不得以不具備履行契約分包事項能力、未依法登記或設立，或依採購法第 103 條規定不得參加投標或作為決標對象或作為分包廠商之廠商為分包廠商。
2. 廠商擬分包之項目及分包廠商，機關得予審查。
3. 廠商對於分包廠商履約之部分，仍應負完全責任。分包契約報備於機關者，亦同。
4. 分包廠商不得將分包契約轉包。其有違反者，廠商應更換分包廠商。
5. 廠商違反不得轉包之規定時，機關得解除契約、終止契約或沒收保證金，並得要求損害賠償。
6. 前目轉包廠商與廠商對機關負連帶履行及賠償責任。再轉包者，亦同。
7. 廠商應於下列分包部分開始作業前，將分包廠商名單送機關備查(由機關視個案情形於招標時載明，未載明者無)：

(1)專業部分：　　。

(2)達一定數量或金額之部分_____。

(3)進度落後達__%之部分：_____。(未載明落後百分比者不適用)

(十三)廠商及分包廠商履約，不得有下列情形：僱用無工作權之人員、供應不法來源之履約標的、使用非法車輛或工具、提供不實證明、違反人口販運防制法、商品標示法、非法棄置廢棄物或其他不法或不當行為。

(十四)契約訂有履約標的之原產地者，廠商供應之標的應符合該原產地之規定。

(十五)採購標的之進出口、供應、興建或使用涉及政府規定之許可證、執照或其他許可文件者，依文件核發對象，由機關或廠商分別負責取得。但屬應由機關取得者，機關得通知廠商代為取得，費用詳第4條。屬外國政府或其授權機構核發之文件者，由廠商負責取得，並由機關提供必要之協助。如因未能取得上開文件，致造成契約當事人一方之損害，應由造成損害原因之他方負責賠償。

(十六)廠商應對其履約場所作業及履約方法之適當性、可靠性及安全性負完全責任。

(十七)廠商之履約場所作業有發生意外事件之虞時，廠商應立即採取防範措施。發生意外時，應立即採取搶救、復原、重建及對機關與第三人之賠償等措施。

(十八)機關於廠商履約中，若可預見其履約瑕疵，或其有其他違反契約之情事者，得通知廠商限期改善。

(十九)廠商不於前款期限內，依照改善或履行者，機關得採行下列措施：

1. 自行或使第三人改善或繼續其工作，其費用由廠商負擔。
2. 終止或解除契約，並得請求損害賠償。
3. 通知廠商暫停履約。

(二十)履約所需臨時場所，除另有規定外，由廠商自理。廠商應規範其人員、設備僅得於該臨時場所或機關提供之場所內履約，並避免其人員、設備進入其他場所或鄰地。

(二十一)機關提供之履約場所，各得標廠商有共同使用之需要者，廠商應依與其他廠商協議或機關協調之結果共用場所。

(二十二)機關提供或將其所有之財物供廠商加工、改善或維修，其須將標的運出機關場所者，該財物之滅失、減損或遭侵占時，廠商應負賠償責任。機關並得視實際需要規定廠商繳納與標的等值或一定金額之保證金_____（由機關視需要於招標時載明）。

(二十三)廠商於機關場所履約者，應隨時清除在該場所暨週邊一切廢料、垃圾、非必要或檢驗不合格之材料、工具及其他設備，以確保該場所之安全及環境整潔，其所需費用概由廠商負責。

(二十四)廠商供應履約標的之包裝方式，應符合下列規定(無者免填)：

■防潮、防水、防震、防破損、防變質、防鏽蝕、防曬、防鹽漬、防污或防碰撞等。

□恆溫、冷藏、冷凍或密封。

□每單位包裝之重量、體積或數量：_____

□包裝材料：_____

□包裝外應標示之文字或標誌：_____

□包裝內應隨附之文件：_____

□其他必要之方式：_____

(二十五)採購標的之包裝及運輸方式，契約未訂明者，由廠商擇適當方式為之。包裝及運輸方式不當，致採購標的受損，除得向保險公司求償者外，由廠商負責賠償。

(二十六)以海空運輸入履約標的：

1. 以 CFR/CPT 或 CIF/CIP 條件簽約者，廠商應依照契約規定負責洽船或洽機裝運。以其他條件簽約者，由機關負責洽船或洽機裝運。
2. 廠商安排之承運船舶，如因船齡或船級問題而發生之額外保險費，概由廠商負擔。除另有規定外，財物不得裝於艙面。

(二十七)廠商履約人員對於所應履約之工作有不適任之情形者，機關得要求更換，廠商不得拒絕。

(二十八)履約項目如包括工程之施工，廠商及分包廠商履約時，除依規定申請聘僱或調派外籍勞工者外，均不得僱用外籍勞工。違法僱用外籍勞工者，機關除通知「就業服務法」主管機關依規定處罰外，情節重大者，得與廠商終止或解除契約。其因此造成損害者，並得向廠商請求損害賠償。

(二十九)其他(由機關擇需要者於招標時載明)

□關鍵基礎設施(或機關指定之設施)人員管制特別約定：

1. 本採購履約標的涉關鍵基礎設施(或機關指定之設施)，廠商及分包廠商之履約人員於進場或參與工作前，應配合機關之要求辦理適任性查核經機關審核同意者，始得進場或參與工作。屬臨時性進場者（例如送貨司機及其隨車人員）得免辦理查核，但應接受機關或其指定之單位或人員(例如但不限於專案管理單位)全程陪同或監督管理。
2. 廠商及分包廠商之履約人員執行工作，應接受機關或其指定之單位或人員(例如但不限於專案管理單位)全程陪同或監督管理。

□其他：

第九條　履約標的品管

(一)廠商在履約中，應對履約品質依照契約有關規範，嚴予控制，並辦理自主檢查。

(二)機關於廠商履約期間如發現廠商履約品質不符合契約規定，得通知廠商限期改善或改正。廠商逾期未辦妥時，機關得要求廠商部分或全部停止履約，至廠商辦妥並經機關書面同意後方可恢復履約。廠商不得為此要

求展延履約期限或補償。

(三)契約履約期間如有由機關分段查驗之規定，廠商應按規定之階段報請機關監督人員查驗。機關監督人員發現廠商未按規定階段報請查驗，而擅自繼續次一階段工作時，得要求廠商將未經查驗及擅自履約部分拆除重做，其一切損失概由廠商自行負擔。但機關監督人員應指派專責查驗人員隨時辦理廠商申請之查驗工作，不得無故遲延。

(四)契約如有任何部分須報請政府主管機關查驗時，除依法規應由機關提出申請者外，應由廠商提出申請，並按照規定負擔有關費用。

(五)廠商應免費提供機關依契約辦理查驗、測試、檢驗、初驗及驗收所必須之儀器、機具、設備、人工及資料。但契約另有規定者，不在此限。契約規定以外之查驗、測試或檢驗，其結果不符合契約規定者，由廠商負擔所生之費用；結果符合者，由機關負擔費用。

(六)查驗、測試或檢驗結果不符合契約規定者，機關得予拒絕，廠商應免費改善、拆除、重作、退貨或換貨。

(七)廠商不得因機關辦理查驗、測試或檢驗，而免除其依契約所應履行或承擔之義務或責任，及費用之負擔。

(八)機關就廠商履約標的為查驗、測試或檢驗之權利，不受該標的曾通過其他查驗、測試或檢驗之限制。

(九)機關提供設備或材料供廠商履約者，廠商應於收受時作必要之檢查，以確定其符合履約需要，並作成紀錄。設備或材料經廠商收受後，其滅失或損害，由廠商負責。

第十條　保險

(一)廠商應於履約期間辦理下列保險(由機關擇定後於招標時載明；未載明者無)，其屬自然人者，應自行另投保人身意外險。

□與安裝財物有關之綜合保險。(例如安裝工程綜合保險；是否附加第三人意外責任險、鄰近財物險、雇主意外責任險，由機關擇定後於招標時載明)

□雇主責任險。

□機械保險、電子設備綜合保險或鍋爐保險。

□廠商應按進口財物契約價格(CIF/CIP 價款)之110%投保海/空運輸全險，包括協會貨物條款(海)／(空運)，協會貨物兵險條款，協會貨物罷工條款及偷竊、挖盜、未送達、漏失、破損、短缺、暴動險等(由機關於招標時載明)，並延伸至機關指定之地點，以涵蓋在中華民國境內之內陸保險。

□其他_____

(二)廠商依前款辦理之保險，其內容如下(由機關視保險性質擇定或調整後於招標時載明)：

1. 承保範圍：(由機關於招標時載明，包括得為保險人之不保事項)
2. 保險標的：履約標的。
3. 被保險人：以機關及廠商為共同被保險人。
4. 保險金額：含財物金額、運費及保險費之 110%。
5. 第三人意外責任險：(載明每一個人體傷或死亡之保險金額下限，每一事故體傷或死亡之保險金額下限，每一事故財物損害之保險金額下限，上述理賠合併單一事件之保險金額下限與保險期間最高累積責任上限。應含廠商、分包廠商、機關及其他任何人員，並包括鄰近財物險。)
6. 每一事故之自負額上限：(由機關於招標時載明)
7. 運輸險保險期間：自_____(地點)起至契約所定_____(地點)止。
8. 受益人：機關(不包含責任保險)。
9. 未經機關同意之任何保險契約之變更或終止，無效。但有利於機關者，不在此限。
10. 其他：_____

(三)保險單記載契約規定以外之不保事項者，其風險及可能之賠償由廠商負擔。

(四)採購進口財物以 CIF 或 CIP 條件簽約者，廠商應依契約規定條件辦理保險。保險單或保險證明書應於押匯時背書予機關。

(五)採購進口財物以 CFR/CPT 或 FOB/FCA 條件簽約者，廠商應於每批貨物裝運前將裝運資料書面通知機關，以便機關辦理保險。廠商如未及時通知，致機關未能辦妥貨物保險因而發生之一切損失或損害，應由廠商負責賠償。

(六)前款之書面資料應記載下列資料：招標案號、契約編號、財物名稱、數量、發票總金額、船名或機名(加註航次)、裝貨港口或機場、預定啟運時間、預定到達時間。

(七)廠商向保險人索賠所費時間，不得據以請求延長履約期限。

(八)廠商未依契約規定辦理保險、保險範圍不足或未能自保險人獲得足額理賠者，其損失或損害賠償，由廠商負擔。

(九)保險單正本 1 份及繳費收據副本 1 份，應於辦妥保險後即交機關收執。因不可歸責於廠商之事由致須延長履約期限者，因而增加之保費，由契

約雙方另行協議其合理之分擔方式。

(十)廠商應依中華民國法規為其員工及車輛投保勞工保險、就業保險、勞工職業災害保險、全民健康保險及汽機車第三人責任險。其依法免投保勞工保險、勞工職業災害保險者，得以其他商業保險代之。

(十一)海空運輸險之保險金額，得為包括內陸險在內之設備器材運抵機關場所金額之全險，並包括偷竊、挖盜、未送達、漏失、破損、短缺、戰爭、罷工及暴動險(由機關擇定後於招標時載明)。

(十二)安裝綜合保險之承保範圍，得包括山崩、地震、海嘯、火山爆發、颱風、豪雨、冰雹、水災、土石流、土崩、地層滑動、雷擊或其他天然災害、火災、爆炸、破壞、竊盜、搶奪、強盜、暴動、罷工、勞資糾紛或民眾非理性之聚眾抗爭等事項所生之損害(實際承保範圍，由機關於招標時載明)。

(十三)機關及廠商均應避免發生採購法主管機關訂頒之「常見保險錯誤及缺失態樣」所載情形。

第十一條　保證金

(一)保證金之發還情形如下(由機關擇定後於招標時載明)：

□預付款還款保證，依廠商已履約部分所占進度之比率遞減。

□預付款還款保證，依廠商已履約部分所占契約金額之比率遞減。

□預付款還款保證，於驗收合格後一次發還。

□履約保證金於履約驗收合格且無待解決事項後 30 日內發還。有分段或部分驗收情形者，得按比例分次發還。

□履約保證金依履約進度分_____期平均發還。

□履約保證金依履約進度分_____期發還，各期之條件及比率如下(由機關於招標時載明)：

□履約保證金於履約驗收合格且無待解決事項後 30 日內發還_____%(由機關於招標時載明)，其餘部分於_____(由機關於招標時載明)且無待解決事項後 30 日內發還。

■**履約保證金新臺幣壹拾玖萬元整，於履約驗收合格且無待解決事項後依機關付款程序發還。**

■**廠商於履約標的完成驗收付款前應繳納保固保證金新臺幣伍萬柒仟元整，於保固期滿且無待解決事項後依機關付款程序發還。**

□差額保證金之發還，同履約保證金。

□其他：

(二)因不可歸責於廠商之事由，致全部終止或解除契約，或暫停履約逾__個

月(由機關於招標時載明；未載明者，為 6 個月)者，履約保證金應提前發還。但屬暫停履約者，於暫停原因消滅後應重新繳納履約保證金。因可歸責於機關之事由而暫停履約，其需延長履約保證金有效期之合理必要費用，由機關負擔。

(三)廠商所繳納之履約保證金及其孳息得部分或全部不予發還之情形：

1. 有採購法第 50 條第 1 項第 3 款至第 5 款、第 7 款情形之一，依同條第 2 項前段得追償損失者，與追償金額相等之保證金。
2. 違反採購法第 65 條規定轉包者，全部保證金。
3. 擅自減省工料，其減省工料及所造成損失之金額，自待付契約價金扣抵仍有不足者，與該不足金額相等之保證金。
4. 因可歸責於廠商之事由，致部分終止或解除契約者，依該部分所占契約金額比率計算之保證金；全部終止或解除契約者，全部保證金。
5. 查驗或驗收不合格，且未於通知期限內依規定辦理，其不合格部分及所造成損失、額外費用或懲罰性違約金之金額，自待付契約價金扣抵仍有不足者，與該不足金額相等之保證金。
6. 未依契約規定期限或機關同意之延長期限履行契約之一部或全部，其逾期違約金之金額，自待付契約價金扣抵仍有不足者，與該不足金額相等之保證金。
7. 須返還已支領之契約價金而未返還者，與未返還金額相等之保證金。
8. 未依契約規定延長保證金之有效期者，其應延長之保證金。
9. 其他因可歸責於廠商之事由，致機關遭受損害，其應由廠商賠償而未賠償者，與應賠償金額相等之保證金。

(四)前款不予發還之履約保證金，於依契約規定分次發還之情形，得為尚未發還者；不予發還之孳息，為不予發還之履約保證金於繳納後所生者。

(五)廠商如有第 3 款所定 2 目以上情形者，其不發還之履約保證金及其孳息應分別適用之。但其合計金額逾履約保證金總金額者，以總金額為限。

(六)保固保證金及其孳息不予發還之情形，準用第 3 款至第 5 款之規定。

(七)廠商未依契約約定履約或契約經終止或解除者，機關得就預付款還款保證尚未遞減之部分加計年息__% （由機關於招標時合理訂定，如未填寫，則依機關撥付預付款當日中華郵政股份有限公司牌告一年期郵政定期儲金機動利率）之利息(於非可歸責廠商之事由之情形，免加計利息)，隨時要求返還或折抵機關尚待支付廠商之價金。

(八)保證金以定期存款單、連帶保證書、連帶保證保險單或擔保信用狀繳納者，其繳納文件之格式依採購法之主管機關於「押標金保證金暨其他擔保作業辦法」所訂定者為準。

(九)保證金之發還，依下列原則處理：

1. 以現金、郵政匯票或票據繳納者，以現金或記載原繳納人為受款人之禁止背書轉讓即期支票發還。
2. 以無記名政府公債繳納者，發還原繳納人；以記名政府公債繳納者，同意塗銷質權登記或公務保證登記。
3. 以設定質權之金融機構定期存款單繳納者，以質權消滅通知書通知該質權設定之金融機構。
4. 以銀行開發或保兌之不可撤銷擔保信用狀繳納者，發還開狀銀行、通知銀行或保兌銀行。但銀行不要求發還或已屆期失效者，得免發還。
5. 以銀行之書面連帶保證或保險公司之連帶保證保險單繳納者，發還連帶保證之銀行或保險公司或繳納之廠商。但銀行或保險公司不要求發還或已屆期失效者，得免發還。

(十)保證書狀有效期之延長：

廠商未依契約規定期限履約或因可歸責於廠商之事由，致有無法於保證書、保險單或信用狀有效期內完成履約之虞，或機關無法於保證書、保險單或信用狀有效期內完成驗收者，該保證書、保險單或信用狀之有效期應按遲延期間延長之。廠商未依機關之通知予以延長者，機關將於有效期屆滿前就該保證書、保險單或信用狀之金額請求給付並暫予保管，其所生費用由廠商負擔。其須返還而有費用或匯率損失者，亦同。

(十一)履約保證金或保固保證金以其他廠商之履約及賠償連帶保證代之或減收者，履約及賠償連帶保證廠商（以下簡稱連帶保證廠商）之連帶保證責任，不因分次發還保證金而遞減。該連帶保證廠商同時作為各機關採購契約之連帶保證廠商者，以 2 契約為限。

(十二)連帶保證廠商非經機關許可，不得自行申請退保。其經機關查核，中途失其保證能力者，由機關通知廠商限期覓保更換，原連帶保證廠商應俟換保手續完成經機關認可後，始能解除其保證責任。

(十三)機關依契約規定認定有不發還廠商履約保證金之情形者，除已洽由連帶保證廠商接續履約者外，該連帶保證廠商應於 5 日內向機關補繳該不發還金額中，原由連帶保證代之或減收之金額。

(十四)廠商為優良廠商或押標金保證金暨其他擔保作業辦法第 33 條之 6 所稱全球化廠商而減收履約保證金、保固保證金者，其有不發還保證金之情形者，廠商應就不發還金額中屬減收之金額補繳之。

(十五)契約價金總額於履約期間增減累計金額達新臺幣 100 萬元者(或機關於招標時載明之其他金額)，履約保證金之金額應依契約價金總額增

減比率調整之，由機關通知廠商補足或退還。

第十二條　驗收

(一)廠商履約所供應或完成之標的，應符合契約規定，無減少或滅失價值或不適於通常或約定使用之瑕疵，且為新品。

(二)驗收程序(由機關擇需要者於招標時載明)：

□廠商應於履約標的預定完成履約日前或完成履約當日，將完成履約日期書面通知機關。除招標文件另有規定者外，機關應於收到該書面通知之日起__日（由機關於招標時載明；未載明者，依採購法施行細則第 92 條規定，為 7 日）內會同廠商，依據契約核對完成履約之項目及數量，以確定是否完成履約。

□履約標的完成履約後有初驗程序者，廠商應於完成履約後__日（由機關於招標時載明；未載明者，依採購法施行細則第 92 條規定，為 7 日）內，將相關資料送請機關審核。機關應於收受全部資料之日起__日（由機關於招標時載明；未載明者，依採購法施行細則第 92 條規定，為 30 日）內辦理初驗，並作成初驗紀錄。初驗合格後，機關應於__日（由機關於招標時載明；未載明者，依採購法施行細則第 93 條規定，為 20 日）內辦理驗收，並作成驗收紀錄。廠商未依機關通知派代表參加初驗或驗收者，除法令另有規定外，不影響初驗或驗收之進行及其結果。如因可歸責於機關之事由，延誤辦理初驗或驗收，該延誤期間不計逾期違約金；廠商因此增加之必要費用，由機關負擔。

■無初驗程序者，機關應於接獲廠商通知備驗或可得驗收之程序完成後__日（由機關於招標時載明；未載明者，依採購法施行細則第 94 條規定，為 30 日）內辦理驗收，並作成驗收紀錄。廠商未依機關通知派代表參加驗收者，除法令另有規定外，不影響驗收之進行及其結果。如因可歸責於機關之事由，延誤辦理驗收，該延誤期間不計逾期違約金；廠商因此增加之必要費用，由機關負擔。

□其他(例如得依履約進度分期驗收，並得視案件情形採書面驗收)：_____。

(三)查驗或驗收有試車、試運轉或試用測試程序者，其內容（由機關於招標時載明，無者免填)：

廠商應就履約標的於____(場所)、_____(期間)及_____(條件)下辦理試車、試運轉或試用測試程序，以作為查驗或驗收之用。試車、試運轉或試用所需費用，由廠商負擔。但契約另有規定者，不在此限。

(四)查驗或驗收人對隱蔽部分拆驗或化驗者，其拆除、修復或化驗所生費用，拆驗或化驗結果與契約規定不符者，該費用由廠商負擔；與規定相符者，該費用由機關負擔。契約規定以外之查驗、測試或檢驗，亦同。

(五)履約標的完成履約後，廠商應對履約期間損壞或遷移之機關設施或公共設施予以修復或回復，並將現場堆置的履約機具、器材、廢棄物及非契約所應有之設施全部運離或清除，並填具完成履約報告，經機關勘驗認可，始得認定為完成履約。

(六)履約標的部分完成履約後，如有部分先行使用之必要，應先就該部分辦理驗收或分段查驗供驗收之用，並得就該部分支付價金及起算保固期。

(七)廠商履約結果經機關初驗或驗收有瑕疵者，機關得要求廠商於_____日內（機關未填列者，由主驗人定之）改善、拆除、重作、退貨或換貨(以下簡稱改正)。逾期未改正者依第 14 條規定計算逾期違約金。但逾期未改正仍在契約原訂履約期限內者，不在此限。

(八)廠商不於前款期限內改正、拒絕改正或其瑕疵不能改正，或改正次數逾_____次(由機關於招標時載明；無者免填)仍未能改正者，機關得採行下列措施之一：

1. 自行或使第三人改正，並得向廠商請求償還改正必要之費用。
2. 終止或解除契約或減少契約價金。

(九)因可歸責於廠商之事由，致履約有瑕疵者，機關除依前二款規定辦理外，並得請求損害賠償。

第十三條　保固

(一)**保固期：本履約標的自全部完成履約經驗收合格日之日起，由廠商保固一年**(由機關於招標時載明)。

(二)本條所稱瑕疵，包括損裂、坍塌、損壞、功能或效益不符合契約規定等。但屬第 14 條第 5 款所載不可抗力或不可歸責於廠商之事由所致者，不在此限。

(三)保固期內發現之瑕疵，應由廠商於機關指定之合理期限內負責免費無條件改正。逾期不為改正者，機關得逕為處理，所需費用由廠商負擔，或動用保固保證金逕為處理，不足時向廠商追償。但屬故意破壞、不當使用、正常零附件損耗或其他非可歸責於廠商之事由所致瑕疵者，由機關負擔改正費用。

(四)保固期內，採購標的因可歸責於廠商之事由造成之瑕疵致全部無法使用時，該無法使用之期間不計入保固期；致部分採購標的無法使用者，該部分採購標的無法使用之期間不計入保固期，並由機關通知廠商。

(五)為釐清發生瑕疵之原因或其責任歸屬，機關得委託公正之第三人進行檢驗或調查工作，其結果如證明瑕疵係因可歸責於廠商之事由所致，廠商應負擔檢驗或調查工作所需之費用。

(六)瑕疵改正後 30 日內，如機關認為可能影響本履約標的任何部分之功能與效益者，得要求廠商依契約原訂測試程序進行測試。該瑕疵係因可歸責於廠商之事由所致者，廠商應負擔進行測試所需之費用。

(七)機關得於保固期間及期滿前，通知廠商派員會同勘查保固事項。

(八)保固期滿且無待決事項後 30 日內，機關得應廠商要求簽發一份保固期滿通知書予廠商，載明廠商完成保固責任之日期。

第十四條　遲延履約

(一)逾期違約金，以日為單位，按逾期日曆天數，每日依契約價金總額 1 ‰（由機關於招標時載明比率；未載明者，為 1‰ ）計算逾期違約金。因可歸責於廠商之事由，致終止或解除契約者，逾期違約金應計算至終止或解除契約之日止。

1. 廠商如未依照契約所定履約期限完成履約標的之供應，自該期限之次日起算逾期日數。但未完成履約之部分不影響其他已完成部分之使用者（不以機關已有使用事實為限，亦即機關可得使用之狀態），按未完成履約部分之契約價金，每日依其 1‰（由機關於招標時載明比率；未載明者，為 3‰ ，但以每日依契約價金總額計算之數額為上限）計算逾期違約金。
2. 初驗或驗收有瑕疵，經機關通知廠商限期改正，自契約所定履約期限之次日起算逾期日數，但扣除以下日數：
   (1)履約期限之次日起，至機關決定限期改正前歸屬於機關之作業日數。
   (2)契約或主驗人指定之限期改正日數（機關得於招標時刪除此部分文字）。

(二)採部分驗收或分期驗收者，得就該部分或該分期之金額計算逾期違約金。

(三)逾期違約金之支付，機關得自應付價金中扣抵；其有不足者，得通知廠商繳納或自保證金扣抵。

(四)逾期違約金為損害賠償額預定性違約金，其總額（含逾期未改正之違約金）以契約價金總額之__%（由機關於招標時載明，但不高於 20%；未載明者，為 20%）為上限，且不計入第 15 條第 10 款之賠償責任上限金額內。

(五)因下列天災或事變等不可抗力或不可歸責於契約當事人之事由，致未能依時履約者，廠商得依第 7 條第 5 款規定，申請延長履約期限；不能履約者，得免除契約責任：

1. 戰爭、封鎖、革命、叛亂、內亂、暴動或動員。
2. 山崩、地震、海嘯、火山爆發、颱風、颶風、豪雨、冰雹、水災、土石流、土崩、地層滑動、雷擊或其他天然災害。
3. 墜機、沉船、交通中斷或道路、港口冰封。
4. 罷工、勞資糾紛或民眾非理性之聚眾抗爭。
5. 毒氣、瘟疫、火災或爆炸。
6. 履約標的遭破壞、竊盜、搶奪、強盜或海盜。
7. 履約人員遭殺害、傷害、擄人勒贖或不法拘禁。
8. 水、能源或原料中斷或管制供應。
9. 核子反應、核子輻射或放射性污染。
10. 非因廠商不法行為所致之政府或機關依法令下達停工、徵用、沒入、拆毀或禁運命令者。
11. 政府法令之新增或變更。
12. 我國或外國政府之行為。
13. 其他經機關認定確屬不可抗力者。

(六)前款不可抗力或不可歸責事由發生或結束後，其屬可繼續履約之情形者，應繼續履約，並採行必要措施以降低其所造成之不利影響或損害。

(七)廠商履約有遲延者，在遲延中，對於因不可抗力而生之損害，亦應負責。但經廠商證明縱不遲延給付，而仍不免發生損害者，不在此限。

(八)契約訂有分段進度及最後履約期限，且均訂有逾期違約金者，屬分段完成履約使用或移交之情形，其逾期違約金之計算原則如下：

1. 未逾分段進度但逾最後履約期限者，扣除已分段完成履約使用或移交部分之金額，計算逾最後履約期限之違約金。
2. 逾分段進度但未逾最後履約期限者，計算逾分段進度之違約金。
3. 逾分段進度且逾最後履約期限者，分別計算違約金。但逾最後履約期限之違約金，應扣除已分段完成履約使用或移交部分之金額計算之。
4. 分段完成履約期限與其他採購契約之進行有關者，逾分段進度，得個別計算違約金，不受前目但書限制。

(九)契約訂有分段進度及最後履約期限，且均訂有逾期違約金者，屬全部完成履約後使用或移交之情形，其逾期違約金之計算原則如下：

1. 未逾分段進度但逾最後履約期限者，計算逾最後履約期限之違約金。

2. 逾分段進度但未逾最後履約期限，其有逾分段進度已收取之違約金者，於未逾最後履約期限後發還。
3. 逾分段進度且逾最後履約期限，其有逾分段進度已收取之違約金者，於計算逾最後履約期限之違約金時應予扣抵。
4. 分段完成履約期限與其他採購契約之進行有關者，逾分段進度，得計算違約金，不受第 2 目及第 3 目之限制。

(十)廠商未遵守法令致生履約事故者，由廠商負責。因而遲延履約者，不得據以免責。

(十一)本條所稱「契約價金總額」為：□結算驗收證明書所載結算總價，並加計可歸責於廠商之驗收扣款金額；□原契約總金額（由機關於招標時勾選；未勾選者，為第 1 選項）。有契約變更之情形者，雙方得就變更之部分另為協議（例如契約變更新增項目或數量之金額）。

第十五條　權利及責任

(一)廠商應擔保第三人就履約標的，對於機關不得主張任何權利。

(二)廠商履約，其有侵害第三人合法權益時，應由廠商負責處理並承擔一切法律責任及費用，包括機關所發生之費用。機關並得請求損害賠償。

(三)廠商履約結果涉及智慧財產權（包含專利權、商標權、著作權、積體電路電路布局權、營業秘密、植物品種權等）者：（由機關於招標時載明，互補項目得複選，如僅涉及著作權者，請就第 4 目至第 12 目勾選。註釋及舉例文字，免載於招標文件）

註：在流通利用方面，考量資訊軟體系統開發之特性，如其內容包含機關與廠商雙方之創作智慧，且不涉及機關安全、專屬使用或其他特殊目的之需要，機關得允許此軟體著作權於機關外流通利用，以增進社會利益。機關亦宜考量避免因取得不必要之權利而增加採購成本。

□機關取得部分權利（內容由機關於招標時載明）。

■機關取得全部權利。

□機關取得授權（內容由機關於招標時載明）。

□機關有權永久無償利用該著作財產權。

例：採購已在一般消費市場銷售之套裝資訊軟體，機關依廠商或第三人之授權契約條款取得永久無償使用權。

□以廠商為著作人，並取得著作財產權，機關取得下列著作財產權授權，於該著作之著作財產權存續期間及約定授權範圍內，有在任何地點、任何時間、以任何方式利用該著作之權利，廠商不得撤銷此

項授權，且機關不須因此支付任何費用。（項目由機關於招標時勾選）

【1】□重製權　【2】□公開口述權　【3】□公開播送權
【4】□公開上映權　【5】□公開演出權　【6】□公開傳輸權
【7】□公開展示權　【8】□改作權　【9】□編輯權
【10】□出租權

例：採購一般共通性需求規格所開發之資訊應用軟體，如約定由廠商取得著作財產權，機關得就業務需要，為其內部使用之目的，勾選【1】重製權及【9】編輯權。如機關擬自行修改著作物，可勾選【8】改作權。如採購教學著作物，可勾選【2】公開口述權及【6】公開播送權。

□以廠商為著作人，其下列著作財產權於著作完成同時讓與機關，廠商並承諾不行使其著作人格權。（項目由機關於招標時勾選）

【1】□重製權　【2】□公開口述權　【3】□公開播送權
【4】□公開上映權　【5】□公開演出權　【6】□公開傳輸權
【7】□公開展示權　【8】□改作權　【9】□編輯權
【10】□出租權

例：採購一般共通性需求規格所開發之資訊應用軟體，機關得就業務需要，為其內部使用之目的，勾選【1】重製權及【9】編輯權。如機關擬自行修改著作物，可勾選【8】改作權。如採購教學著作物，可勾選【2】公開口述權及【3】公開播送權。

□以廠商為著作人，機關取得著作財產權，廠商並承諾對機關不行使其著作人格權。

例：採購機關專用或機關特殊需求規格所開發之資訊應用軟體，機關取得著作財產權之全部。

□以機關為著作人，並由機關取得著作財產權之全部。

□機關出資委託廠商設計之資訊應用軟體於開發或維護完成後，以機關為著作人，並由機關取得著作財產權之全部，廠商於開發或維護完成該應用軟體時，經機關同意：（項目由機關於招標時勾選）

【1】□取得機關之使用授權與再授權之權，於每次使用時均不需徵得機關之同意。

【2】□取得機關之使用授權與再授權之權，於每次使用均需徵得機關同意。

□機關與廠商共同享有著作人格權及著作財產權。

例：採購廠商已完成之資訊應用軟體，並依機關需求進行改作，且機關與廠商均投入人力、物力，該衍生之共同完成之著作，其著作

人格權由機關與廠商共有，其著作財產權享有之比例、授權範圍、後續衍生著作獲利之分攤內容，由機關於招標時載明。

□機關取得授權，於利用著作財產權存續期間，有轉授權他人利用該著作之權利。上開他人包括：＿＿＿＿＿＿（由機關於招標時載明）

□其他。（內容由機關於招標時載明）

例：機關得就其取得之著作財產權，允許廠商支付對價，授權廠商使用。

(四)訂約機關為政府機關者，以政府機關所屬公法人為權利義務主體。

(五)廠商保證對於其受雇人或受聘人職務上完成之著作，依著作權法第 11 條第 1 項但書及第 12 條規定，與其受雇人或受聘人約定以廠商為著作人，享有著作人格權及著作財產權。惟此一約定僅止於廠商與其受雇人或受聘人間。廠商與機關間之權利及責任，仍以本契約為準。

(六)除另有規定外，廠商如在契約使用專利品，或專利性施工方法，或涉及著作權時，其有關之專利及著作權益，概由廠商依照有關法令規定處理，其費用亦由廠商負擔。

(七)機關及廠商應採取必要之措施，以保障他方免於因契約之履行而遭第三人請求損害賠償。其有致第三人損害者，應由造成損害原因之一方負責賠償。

(八)機關對於廠商、分包廠商及其人員因履約所致之人體傷亡或財物損失，不負賠償責任。對於人體傷亡或財物損失之風險，廠商應投保必要之保險。

(九)廠商依契約規定應履行之責任，不因機關對於廠商履約事項之審查、認可或核准行為而減少或免除。

(十)因可歸責於一方之事由，致他方遭受損害者，一方應負賠償責任，其認定有爭議者，依照爭議處理條款辦理。

1. 損害賠償之範圍，依民法第 216 條第 1 項規定，以填補他方所受損害及所失利益為限。

□但非因故意或重大過失所致之損害，契約雙方所負賠償責任不包括「所失利益」（得由機關於招標時勾選）。

2. 除第 14 條規定之逾期違約金外，損害賠償金額上限為：（機關欲訂上限者，請於招標時載明）

■契約價金總額。

□契約價金總額之__倍。

□契約價金總額之__%。

□固定金額__元。

3. 前目訂有損害賠償金額上限者，於法令另有規定(例如民法第 227 條第 2 項之加害給付損害賠償)，或一方故意隱瞞工作之瑕疵、故意或重大過失行為，或對第三人發生侵權行為，對他方所造成之損害賠償，不受賠償金額上限之限制。

(十一)連帶保證廠商應保證得標廠商依契約履行義務，如有不能履約情事，即續負履行義務，並就機關因此所生損失，負連帶賠償責任。

(十二)連帶保證廠商經機關通知代得標廠商履行義務者，有關廠商之一切權利，包括尚待履約部分之契約價金，一併移轉由該連帶保證廠商概括承受，本契約並繼續有效。得標廠商之保證金及已履約而尚未支付之契約價金，如無不支付或不發還之情形，得依原契約規定支付或發還該得標廠商。

(十三)廠商與其連帶保證廠商如有債務等糾紛，應自行協調或循法律途徑解決。

第十六條　契約變更及轉讓

(一)機關於必要時得於契約所約定之範圍內通知廠商變更契約(含新增項目)，廠商於接獲通知後，除雙方另有協議外，應於__天（由機關於招標時載明；未載明者，為 10 天）內向機關提出契約標的、價金、履約期限、付款期程或其他契約內容須變更之相關文件。契約價金之變更，其底價依採購法第 46 條第 1 項之規定。

契約原有項目，因機關要求契約變更，如變更之部分，其價格或履約條件改變，得就該等變更之部分另行議價。新增工作中如包括原有契約項目，經廠商舉證依原單價履約顯失公平者，亦同。

(二)廠商於機關接受其所提出須變更之相關文件前，不得自行變更契約。除機關另有請求者外，廠商不得因前款之通知而遲延其履約期限。

(三)機關於接受廠商所提出須變更之事項前即請求廠商先行施作或供應，其後未依原通知辦理契約變更或僅部分辦理者，應補償廠商所增加之必要費用。

(四)契約約定之採購標的，其有下列情形之一者，廠商得敘明理由，檢附規格、功能、效益及價格比較表，徵得機關書面同意後，以其他規格、功能及效益相同或較優者代之。但不得據以增加契約價金。其因而減省廠商履約費用者，應自契約價金中扣除。

1. 契約原標示之廠牌或型號不再製造或供應。
2. 契約原標示之分包廠商不再營業或拒絕供應。
3. 較契約原標示者更優或對機關更有利。

4. 契約所定技術規格違反採購法第 26 條規定。

屬前段第三目情形，而有增加經費之必要，其經機關綜合評估其總體效益更有利於機關者，得不受前段序文但書限制。

(五)廠商提出前款第 1 目、第 2 目或第 4 目契約變更之文件，其審查及核定期程，除雙方另有協議外，為該書面請求送達之次日起__天（由機關於招標時載明；未載明者，為 10 天）內。但必須補正資料者，以補正資料送達之次日起__天（由機關於招標時載明；未載明者，為 10 天）內為之。因可歸責於機關之事由逾期未核定者，得依第 7 條第 5 款申請延長履約期限。

(六)廠商依前款請求契約變更，應自行衡酌預定履約時程，考量檢(查、試)驗所需時間及機關受理申請審查及核定期程後再行適時提出，並於接獲機關書面同意後，始得依同意變更情形施作。除因機關逾期未核定外，不得以資料送審為由，提出延長履約期限之申請。

(七)契約之變更，非經機關及廠商雙方合意，作成書面紀錄，並簽名或蓋章者，無效。

(八)廠商不得將契約之部分或全部轉讓予他人。但因公司分割或其他類似情形致有轉讓必要，經機關書面同意轉讓者，不在此限。

廠商依公司法、企業併購法分割，受讓契約之公司（以受讓營業者為限），其資格條件應符合原招標文件規定，且應提出下列文件之一：

1. 原訂約廠商分割後存續者，其同意負連帶履行本契約責任之文件；
2. 原訂約廠商分割後消滅者，受讓契約公司以外之其他受讓原訂約廠商營業之既存及新設公司同意負連帶履行本契約責任之文件。

第十七條　契約終止解除及暫停執行

(一)廠商履約有下列情形之一者，機關得以書面通知廠商終止契約或解除契約之部分或全部，且不補償廠商因此所生之損失：

1. 有採購法第 50 條第 2 項前段規定之情形者。
2. 有採購法第 59 條規定得終止或解除契約之情形者。
3. 違反不得轉包之規定者。
4. 廠商或其人員犯採購法第 87 條至第 92 條規定之罪，經判決有罪確定者。
5. 因可歸責於廠商之事由，致延誤履約期限，有下列情形者（由機關於招標時勾選；未勾選者，為第 1 選項）：

■履約進度落後　%(由機關於招標時載明，未載明者為 20%)以上，且日數達十日以上。

百分比之計算方式：

(1)屬尚未完成履約而進度落後已達百分比者，機關應先通知廠商限期改善。屆期未改善者，如機關訂有履約進度計算方式，其通知限期改善當日及期限末日之履約進度落後百分比，分別以各該日實際進度與機關核定之預定進度百分比之差值計算；如機關未訂有履約進度計算方式，依逾期日數計算之。

(2)屬已完成履約而逾履約期限，或逾最後履約期限尚未完成履約者，依逾期日數計算之。

□其他：　　。

6. 偽造或變造契約或履約相關文件，經查明屬實者。

7. 擅自減省工料情節重大者。

8. 無正當理由而不履行契約者。

9. 查驗或驗收不合格，且未於通知期限內依規定辦理者。

10 有破產或其他重大情事，致無法繼續履約者。

11. 廠商未依契約規定履約，自接獲機關書面通知之次日起 10 日內或書面通知所載較長期限內，仍未改正者。

12. 違反環境保護或勞工安全衛生等有關法令，情節重大者。

13. 違反法令或其他契約規定之情形，情節重大者。

(二)機關未依前款規定通知廠商終止或解除契約者，廠商仍應依契約規定繼續履約。

(三)契約經依第 1 款規定或因可歸責於廠商之事由致終止或解除者，機關得依其所認定之適當方式，自行或洽其他廠商完成被終止或解除之契約；其所增加之費用及損失，由廠商負擔。無洽其他廠商完成之必要者，得扣減或追償契約價金，不發還保證金。機關有損失者亦同。

(四)契約因政策變更，廠商依契約繼續履行反而不符公共利益者，機關得報經上級機關核准，終止或解除部分或全部契約，並與廠商協議補償廠商因此所生之損失。但不包含所失利益。

(五)依前款規定終止契約者，廠商於接獲機關通知前已完成且可使用之履約標的，依契約價金給付；僅部分完成尚未能使用之履約標的，機關得擇下列方式之一洽廠商為之：

1. 繼續予以完成，依契約價金給付。

2. 停止製造、供應或施作。但給付廠商已發生之製造、供應或施作費用及合理之利潤。

(六)非因政策變更而有終止或解除契約必要者，準用前 2 款規定。

(七)廠商未依契約規定履約者，機關得隨時通知廠商部分或全部暫停執行，至情況改正後方准恢復履約。廠商不得就暫停執行請求延長履約期限或

增加契約價金。

(八)因可歸責於機關之情形，機關通知廠商部分或全部暫停執行：

1. 致廠商未能依時履約者，廠商得依第 7 條第 5 款規定，申請展延履約期限；因此而增加之必要費用（例如但不限於管理費），由機關負擔。
2. 暫停執行期間累計逾__個月（由機關於招標時合理訂定，如未填寫，則為 2 個月）者，機關應先支付已依機關指示由機關取得所有權之履約標的之價金。
3. 暫停執行期間累計逾__個月（由機關於招標時合理訂定，如未填寫，則為 6 個月）者，廠商得通知機關終止或解除部分或全部契約，並得向機關請求賠償因契約終止或解除而生之損害。因可歸責於機關之情形無法開始履約者，亦同。

(九)因非可歸責於廠商之事由，機關有延遲付款之情形：

1. 廠商得向機關請求加計年息__%（由機關於招標時合理訂定，如未填寫，則依機關簽約日中華郵政股份有限公司牌告一年期郵政定期儲金機動利率）之遲延利息。
2. 廠商得於通知機關__個月後（由機關於招標時合理訂定，如未填寫，則為 1 個月）暫停或減緩履約進度、依第 7 條第 5 款規定，申請展延履約期限；廠商因此增加之必要費用，由機關負擔。
3. 延遲付款達__個月（由機關於招標時合理訂定，如未填寫，則為 3 個月）者，廠商得通知機關終止或解除部分或全部契約，並得向機關請求賠償因契約終止或解除而生之損害。

(十)除契約另有約定外，履行契約需機關之行為始能完成，而機關不為其行為時，廠商得定相當期限催告機關為之。機關不於前述期限內為其行為者，廠商得通知機關終止或解除契約，並得向機關請求賠償因契約終止或解除而生之損害。

(十一)因契約規定不可抗力之事由，致全部契約暫停執行，暫停執行期間持續逾__個月（由機關於招標時合理訂定，如未填寫，則為 3 個月）或累計逾__個月（由機關於招標時合理訂定，如未填寫，則為 6 個月）者，契約之一方得通知他方終止或解除契約。。

(十二)廠商不得對本契約採購案任何人要求、期約、收受或給予賄賂、佣金、比例金、仲介費、後謝金、回扣、餽贈、招待或其他不正利益。分包廠商亦同。違反規定者，機關得終止或解除契約，並將 2 倍之不正利益自契約價款中扣除。未能扣除者，通知廠商限期給付之。

(十三)本契約終止時，自終止之日起，雙方之權利義務即消滅。契約解除時，

溯及契約生效日消滅。雙方並互負保密義務。

第十八條　爭議處理

(一)機關與廠商因履約而生爭議者，應依法令及契約規定，考量公共利益及公平合理，本誠信和諧，盡力協調解決之。其未能達成協議者，得以下列方式處理之：

1. 依採購法第 85 條之 1 規定向採購申訴審議委員會申請調解。
2. 經契約雙方同意並訂立仲裁協議書後，依本契約約定及仲裁法規定提付仲裁。
3. 依採購法第 102 條規定提出異議、申訴。
4. 提起民事訴訟。
5. 依其他法律申(聲)請調解。
6. 契約雙方合意成立爭議處理小組協調爭議。
7. 依契約或雙方合意之其他方式處理。

(二)依前款第 2 目提付仲裁者，約定如下：

1. 由機關於招標文件及契約預先載明仲裁機構。其未載明者，由契約雙方協議擇定仲裁機構。如未能獲致協議，由機關指定仲裁機構。上開仲裁機構，除契約雙方另有協議外，應為合法設立之國內仲裁機構。
2. 仲裁人之選定：
   (1)當事人雙方應於一方收受他方提付仲裁之通知之次日起 14 日內，各自從指定之仲裁機構之仲裁人名冊或其他具有仲裁人資格者，分別提出 10 位以上(含本數)之名單，交予對方。
   (2)當事人之一方應於收受他方提出名單之次日起 14 日內，自該名單內選出 1 位仲裁人，作為他方選定之仲裁人。
   (3)當事人之一方未依(1)提出名單者，他方得從指定之仲裁機構之仲裁人名冊或其他具有仲裁人資格者，逕行代為選定 1 位仲裁人。
   (4)當事人之一方未依(2)自名單內選出仲裁人，作為他方選定之仲裁人者，他方得聲請□法院；□指定之仲裁機構（由機關於招標時勾選；未勾選者，為指定之仲裁機構）代為自該名單內選定 1 位仲裁人。
3. 主任仲裁人之選定：
   (1)二位仲裁人經選定之次日起 30 日內，由□雙方共推；■雙方選定之仲裁人共推(由機關於招標時勾選)第三仲裁人為主任仲裁人。
   (2)未能依(1)共推主任仲裁人者，當事人得聲請□法院；□指定之仲

裁機構（由機關於招標時勾選；未勾選者，為指定之仲裁機構）為之選定。

4. 以■機關所在地；□其他：_____為仲裁地（由機關於招標時載明；未載明者，為機關所在地）。

5. 除契約雙方另有協議外，仲裁程序應公開之，仲裁判斷書雙方均得公開，並同意仲裁機構公開於其網站。

6. 仲裁程序應使用■國語及中文正體字；□其他語文：_____。（由機關於招標時載明；未載明者，為國語及中文正體字）

7. 機關□同意；■不同意（由機關於招標時勾選；未勾選者，為不同意）仲裁庭適用衡平原則為判斷。

8. 仲裁判斷書應記載事實及理由。

(三)依第 1 款第 6 目成立爭議處理小組者，約定如下：

1. 爭議處理小組於爭議發生時成立，得為常設性，或於爭議作成決議後解散。

2. 爭議處理小組委員之選定：

(1)當事人雙方應於協議成立爭議處理小組之次日起 10 日內，各自提出 5 位以上(含本數)之名單，交予對方。

(2)當事人之一方應於收受他方提出名單之次日起 10 日內，自該名單內選出 1 位作為委員。

(3)當事人之一方未依(1)提出名單者，為無法合意成立爭議處理小組。

(4)當事人之一方未能依(2)自名單內選出委員，且他方不願變更名單者，為無法合意成立爭議處理小組。

3. 爭議處理小組召集委員之選定：

(1)二位委員經選定之次日起 10 日內，由雙方或雙方選定之委員自前目(1)名單中共推 1 人作為召集委員。

(2)未能依(1)共推召集委員者，為無法合意成立爭議處理小組。

4. 當事人之一方得就爭議事項，以書面通知爭議處理小組召集委員，請求小組協調及作成決議，並將繕本送達他方。該書面通知應包括爭議標的、爭議事實及參考資料、建議解決方案。他方應於收受通知之次日起 14 日內提出書面回應及建議解決方案，並將繕本送達他方。

5. 爭議處理小組會議：

(1)召集委員應於收受協調請求之次日起 30 日內召開會議，並擔任主席。委員應親自出席會議，獨立、公正處理爭議，並保守秘密。

(2)會議應通知當事人到場陳述意見，並得視需要邀請專家、學者或

其他必要人員列席，會議之過程應作成書面紀錄。

(3)小組應於收受協調請求之次日起 90 日內作成合理之決議，並以書面通知雙方。

6. 爭議處理小組委員應迴避之事由，參照採購申訴審議委員會組織準則第 13 條規定。委員因迴避或其他事由出缺者，依第 2 目、第 3 目辦理。

7. 爭議處理小組就爭議所為之決議，除任一方於收受決議後 14 日內以書面向召集委員及他方表示異議外，視為協調成立，有契約之拘束力。惟涉及改變契約內容者，雙方應先辦理契約變更。如有爭議，得再循爭議處理程序辦理。

8. 爭議事項經一方請求協調，爭議處理小組未能依第 5 目或當事人協議之期限召開會議或作成決議，或任一方於收受決議後 14 日內以書面表示異議者，協調不成立，雙方得依第 1 款所定其他方式辦理。

9. 爭議處理小組運作所需經費，由契約雙方平均負擔。

10. 本款所定期限及其他必要事項，得由雙方另行協議。

(四)依採購法規定受理調解或申訴之機關名稱：_____

地址：_____

電話：_____

(五)履約爭議發生後，履約事項之處理原則如下：

1. 與爭議無關或不受影響之部分應繼續履約。但經機關同意無須履約者不在此限。

2. 廠商因爭議而暫停履約，其經爭議處理結果被認定無理由者，不得就暫停履約之部分要求延長履約期限或免除契約責任。

(六)本契約以中華民國法律為準據法，並以機關所在地之地方法院為第一審管轄法院。

第十九條　其他

(一)廠商對於履約所僱用之人員，不得有歧視性別、原住民、身心障礙或弱勢團體人士之情事。

(二)廠商履約時不得僱用機關之人員或受機關委託辦理契約事項之機構之人員。

(三)廠商授權之代表應通曉中文或機關同意之其他語文。未通曉者，廠商應備翻譯人員。

(四)機關與廠商間之履約事項，其涉及國際運輸或信用狀等事項，契約未予載明者，依國際貿易慣例。

(五)機關及廠商於履約期間應分別指定授權代表，為履約期間雙方協調與契約有關事項之代表人。

(六)依據「政治獻金法」第7條規定，與政府機關（構）有巨額採購契約，且在履約期間之廠商，不得捐贈政治獻金。

(七)廠商內部揭弊者保護制度及機關處理方式：

1. 廠商人員（包括勞工及其主管）針對本採購案發現其雇主、所屬員工或機關人員（包括代理或代表機關處理採購事務之廠商）涉有違反採購法、本契約或其他影響公共安全或品質，具名揭弊者，廠商應保障揭弊人員之權益，不得因該揭弊行為而為不利措施（包括但不限解僱、資遣、降調、不利之考績、懲處、懲罰、減薪、罰款〈薪〉、剝奪或減少獎金、退休〈職〉金、剝奪與陞遷有關之教育或訓練機會、福利、工作地點、職務內容或其他工作條件、管理措施之不利變更、非依法令規定揭露揭弊者之身分）。但若發生違法或違約之行為（例如無故曠職、洩漏公司機密等），不在此限。

2. 廠商人員之揭弊內容有下列情形之一者，仍得受前目之保護：

(1)所揭露之內容無法證實。但明顯虛偽不實或揭弊行為經以誣告、偽證罪緩起訴或判決有罪者，不在此限。

(2)所揭露之內容業經他人檢舉或受理揭弊機關已知悉。但案件已公開或揭弊者明知已有他人檢舉者，不在此限。

3. 廠商內部訂有禁止所屬員工揭弊條款者，該約定於本採購案無效。

4. 為兼顧公益及採購效率，機關於接獲揭弊內容後，應積極釐清揭弊事由，立即啟動調查；除經調查後有具體事證，依契約及法律為必要處置外，廠商及機關仍應依契約約定正常履約及估驗。

(八)本契約未載明之事項，依採購法及民法等相關法令。

立契約書人:

機　　關：臺北醫學大學
校　　長：吳麥斯 校長
地　　址：台北市信義區吳興街250號
電　　話：02-2736-1661

廠商名稱：泰瑩科技股份有限公司
負 責 人：董事長 賴 銘 德
統一編號：28208184
地　　址：台北市松山區南京東路四段130號四樓
電　　話：02-2578-1133

中　華　民　國　113　年　11　月 28　日

保密同意書

茲緣於簽署人 黃政寬 （簽署人姓名，以下稱簽署人）參與**泰瑩科技股份有限公司** （廠商名稱，以下稱廠商）得標**臺北醫學大學**（機關名稱）（以下稱機關）資訊業務委外案**防火牆日誌紀錄器**（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第1條　簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第2條　簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第3條　簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第4條　簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第5條　簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第6條　本同意書一式四份，機關執存三份、**泰瑩科技股份有限公司**（廠商）執存一份，簽屬人自行影印留存一份。

簽署人姓名及簽章：黃政寬

身分證字號：F126890958

聯絡電話：0963371832

戶籍地址：新北市板橋區成功路6巷5號3樓

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：[redacted]

所屬廠商地址：台北市105松山區南京東路四段130號4F

中　華　民　國 113 年 11 月 28 日

保密同意書

茲緣於簽署人 張堅邦 （簽署人姓名，以下稱簽署人）參與**泰瑩科技股份有限公司** （廠商名稱，以下稱廠商）得標**臺北醫學大學**（機關名稱）（以下稱機關）資訊業務委外案**防火牆日誌紀錄器**（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第1條　簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第2條　簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第3條　簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第4條　簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第5條　簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第6條　本同意書一式四份，機關執存三份、**泰瑩科技股份有限公司**（廠商）執存一份，簽屬人自行影印留存一份。

簽署人姓名及簽章：張堅邦

身分證字號：F129314310

聯絡電話：0982913143

戶籍地址：新北市淡水區自強路20巷18號2樓

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：趙銘德

所屬廠商地址：台北市105松山區南京東路四段130號4F

中　華　民　國 113 年 11 月 28 日

保密同意書

茲緣於簽署人 闕子翔 （簽署人姓名，以下稱簽署人）參與**泰瑩科技股份有限公司** （廠商名稱，以下稱廠商）得標**臺北醫學大學**（機關名稱）（以下稱機關）資訊業務委外案**防火牆日誌紀錄器**（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第1條　簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第2條　簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第3條　簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第4條　簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第5條　簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第6條　本同意書一式四份，機關執存三份、**泰瑩科技股份有限公司**（廠商）執存一份，簽屬人自行影印留存一份。

簽署人姓名及簽章：闕子翔

身分證字號：A130517162

聯絡電話：0930999999

戶籍地址：台北市松山區三民路110巷10號3樓

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：

所屬廠商地址：台北市105松山區南京東路四段130號4F

中　華　民　國 113 年 11 月 28 日

保　密　切　結　書

立切結書人 張聖邦/關子翔（簽署人姓名）等，受**泰瑩科技股份有限公司**（廠商名稱）委派至**臺北醫學大學**（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。

1、 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。

2、 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。

3、 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。

4、 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。

5、 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。

6、 本保密切結書不因立切結書人離職而失效。

7、 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	聯絡電話及戶籍地址
張聖邦	F124314310	0982413143，新北市淡水區自強路20巷18號2樓
關子翔	A130517162	0930999777，台北市松山區三民路110巷10號3樓

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
泰瑩科技股份有限公司	張聖邦	02-2578-1133
		台北市105松山區南京東路四段130號4F

填表說明：

1、 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。

2、 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。

中　華　民　國 113 年 11 月 28 日

保　密　切　結　書

立切結書人黃政棠（簽署人姓名）等，受**泰瑩科技股份有限公司**（廠商名稱）委派至**臺北醫學大學**（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。

1、 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。
2、 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。
3、 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。
4、 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。
5、 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。
6、 本保密切結書不因立切結書人離職而失效。
7、 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	聯絡電話及戶籍地址
黃政棠	F126689098	0963911832 新北市板橋區武功路6巷5號3樓

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
泰瑩科技股份有限公司	趙銘德	02-2578-1133
		台北市105松山區南京東路四段130號4F

填表說明：

1、 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。
2、 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。

中　華　民　國 113 年 11 月 26 日

同意書

本人同意任職**泰瑩科技股份有限公司**（廠商名稱）期間內在職務上所為之著作，以職務所屬廠商為著作人。本人同意對上開著作，職務所屬廠商享有著作財產權及著作人格權。

簽署人姓名及簽章：黃政熹

身分證字號：F126689098

戶籍地址：新北市板橋區成功路6巷5號3樓

聯絡電話：0963371832

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：

所屬廠商地址：台北市105松山區南京東路四段130號

中　華　民　國 113 年 11 月 28 日

同意書

本人同意任職**泰瑩科技股份有限公司**（廠商名稱）期間內在職務上所為之著作，以職務所屬廠商為著作人。本人同意對上開著作，職務所屬廠商享有著作財產權及著作人格權。

簽署人姓名及簽章：張堅邦

身分證字號：F129314310

戶籍地址：新北市淡水區自強路201巷18號2樓

聯絡電話：0982913143

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：賴金玉

所屬廠商地址：台北市105松山區南京東路四段130號4F

中　華　民　國 113 年 11 月 28 日

同意書

本人同意任職**泰瑩科技股份有限公司**（廠商名稱）期間內在職務上所為之著作，以職務所屬廠商為著作人。本人同意對上開著作，職務所屬廠商享有著作財產權及著作人格權。

簽署人姓名及簽章：閻子翔

身分證字號：A130517162

戶籍地址：台北市松山區三民路110巷10號3樓

聯絡電話：0930999777

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：

所屬廠商地址：台北市105松山區南京東路四段130號4F

中　華　民　國 113 年 11 月 28 日

廠商人員接受適任性查核同意書

本人因任職**泰瑩科技股份有限公司**（廠商名稱）受**臺北醫學大學**(機關)之委託，執行**防火牆日誌紀錄器**（業務），涉及該機關之重要業務及國家機密，依資通安全管理法第九條及資通安全管理法施行細則第四條之規定，同意**臺北醫學大學**(機關)以下列事項進行適任性查核：

1、是否曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

2、是否曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

3、是否曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

4、其他與國家機密保護相關之具體項目。

簽署人姓名及簽章：黃政憲

身分證字號：F126689098

通訊地址：新北市板橋區成功路6巷5號3樓

聯絡電話：0963321832

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：賴銘德

所屬廠商地址：台北市105松山區南京東路四段130號4F

中　華　民　國 113 年 11 月 28 日

廠商人員接受適任性查核同意書

本人因任職**泰瑩科技股份有限公司**（廠商名稱）受**臺北醫學大學**(機關)之委託，執行**防火牆日誌紀錄器**（業務），涉及該機關之重要業務及國家機密，依資通安全管理法第九條及資通安全管理法施行細則第四條之規定，同意**臺北醫學大學**(機關)以下列事項進行適任性查核：

1、是否曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

2、是否曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

3、是否曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

4、其他與國家機密保護相關之具體項目。

簽署人姓名及簽章：張聖邦

身分證字號：F129314310

通訊地址：新北市 淡水區 自強路 201巷 18號 2樓

聯絡電話：0982913143

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：

所屬廠商地址：台北市105松山區南京東路四段130號4F

中　華　民　國 113 年 11 月 28 日

廠商人員接受適任性查核同意書

本人因任職**泰瑩科技股份有限公司**（廠商名稱）受**臺北醫學大學**(機關)之委託，執行**防火牆日誌紀錄器**（業務），涉及該機關之重要業務及國家機密，依資通安全管理法第九條及資通安全管理法施行細則第四條之規定，同意**臺北醫學大學**(機關)以下列事項進行適任性查核：

1、是否曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

2、是否曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

3、是否曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

4、其他與國家機密保護相關之具體項目。

簽署人姓名及簽章：關子翔

身分證字號：A130517162

通訊地址：台北市松山區[illegible]10號3樓

聯絡電話：0930999777

所屬廠商名稱及蓋章：泰瑩科技股份有限公司

所屬廠商負責人姓名及簽章：賴銘德

所屬廠商地址：台北市105松山區[illegible]4F

中　華　民　國 113 年 11 月 28 日

泰瑩科技股份有限公司 參與 臺北醫學大學 辦理
防火牆日誌紀錄器
之相關資安管理作業自我評估表

日期：113 年 11 月 28 日

評估項目	辦理情形
1. 管理面	
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	□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_____ □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) ■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	■本專案之資安負責人(專案主管)為黃政憲 □本專案之資安人員為____ □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	■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) □未就本專案進行資安風險評估 備註：本案設備無機密性、完整性、可用性風險
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	■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_附件_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_4_小時內向甲方等相關利害關係人通報，通報對象包含_陳韋伸_ □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	■過去3年無發生因管理議題肇因之資安事件

	□是，共__次，事件發生主要根因為____ 備註：_____
2. 技術面	
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需使用之業務、行政相關資通系統，辦理安全性檢測	□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：_____ ■未就本專案範圍內之資通系統規劃安全性檢測 備註：本專案並未含相關系統之業務
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護措施	□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：_____ ■本專案受託業務之環境及設備未導入相關資通安全防護措施 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	□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：____ ■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：本專案設備不包含機敏性
3. 認知訓練面	
3.1 本專案直接履約相關人員之資安教育訓練	■本專案直接履約相關人員之資安教育訓練包含 1 小時之資安通識教育訓練，對象包含本專案直接履約相關人員；__小時之資安專業教育訓練，對象包含 □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	■本專案具資安證照之團隊成員有：1 位 □本專案團隊人員未具備資通安全專業證照 備註：_____

廠商用印：_____

制定 / 修訂記錄

日期	章節	內容摘要	版次	公告日期	備註
2023.02.01	1-7	新制定	1.0	2023.02.20	
2023.10.26	5.1.1	原定:...並於每週例行性會議進行提報。 修訂:...如有不正常之情況時，向權責單位主管進行提報。	1.1	2023.10.30	
2023.10.26	5.1.2	原定:...於每週例行性會議中針對防毒伺服器的結果進行提報。 修訂:...向權責單位主管進行提報。	1.1	2023.10.30	
2023.12.13	5.3.3.2	原定:一般資安事件：凡非屬 6.5.2.1 所述重大事件之資安事件稱之。 修訂:一般資安事件：凡非屬 5.3.3.1 所述重大事件之資安事件稱之。	1.2	2023.12.14	
2023.12.13	5.3.4.1	原定:綠色資安事件：資安事件發生時即備定義成一般資安事件。 修訂:綠色資安事件：資安事件發生時即被定義成一般資安事件。	1.2	2023.12.14	
2024.02.05	5.3.3 5.3.4	原定:資訊安全事件等級分為-重大資安事件(紅色資安事件)、一般資安事件(綠色資安事件) 修訂:資訊安全事件等級分為四級	1.3	2024.02.23	
2024.02.05	5.7.3	原定:若為綠色資安事件... 修訂:若為一、二級事件...	1.3	2024.02.23	
2024.02.05	5.7.4	原定:若為紅色資安事件... 修訂:若為三、四級事件...	1.3	2024.02.23	

1. 目的：

確保於資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害。

2. 範圍：

本公司系統之相關資訊資產之資訊安全事件管理。

3. 權責：

3.1 發現人員：所有人員（含：本單位人員、約聘僱人員與委外駐點人員），發現疑似資訊安全事件時，皆負有即時通報之責任。

3.2 資訊單位：資訊安全事件處理之權責單位，須執行資訊安全事件之分析及處理。

3.3 管理代表：督導資訊安全事件通報、處理及分析作業。

4. 名詞釋義：

4.1 資訊安全事件：凡於作業環境中，導致資訊資產之機密性、完整性、可用性遭受影響之事件。

4.2 內部危安事件：發現（疑似）遭人為惡意破壞毀損、作業不慎等事件。

4.3 外力入侵事件：發現（疑似）電腦病毒感染事件、駭客攻擊（非法入侵）等事件。

4.4 天然災害：颱風、水災、地震等。

4.5 突發事件：火災、爆炸、重大建築災害及資訊網路系統骨幹中斷事件等。

5. 作業內容：

5.1 弱點通報作業

5.1.1 資訊單位每日檢視防火牆異常事件，記錄於每日工作紀錄，如有不正常之情況時，向權責單位主管進行提報。

5.1.2 資訊單位需每週對防毒監控之情形進行確認，如有不正常之情況時，向權責單位主管進行提報。

5.2 事件通報作業

5.2.1 為建全通報體系，應建立並維護相關服務廠商之「委外廠商服務人員名冊」。

5.2.2 當系統異常事件發生時，需依 5.3.3" 事件分級" 要求進行通報作業。

5.2.3 若異常事件需尋求外部支援時，依「委外廠商服務人員名冊」進行通報。

5.2.4 資訊安全事件造成同仁生命安全或設備遭到破壞等涉及民事或刑事案件時，應通報檢調單位請求支援並協助處理。

5.2.5 每次異常事件發生時， 須將異常事件記錄於「資安事件記錄處理單」。

5.3 事件辨識作業

5.3.1 記錄人員應紀錄異常事件發生狀況、異常事件處理方式及發生原因。

5.3.2 由記錄人員根據異常事件影響程度不同，進行分級、通報。

5.3.3 資訊安全事件等級分為四級：

5.3.4 事件等級：

5.3.4.1 有下列情形之一者，為第一級資通安全事件：

一、非核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成公司日常作業影響。

5.3.4.2 有下列情形之一者，為第二級資通安全事件：

一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

5.3.4.3 有下列情形之一者，為第三級資通安全事件：

一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

5.3.4.4 有下列情形之一者，為第四級資通安全事件：

一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

5.3.5 事件負責人員應依資訊安全事件狀況協調設備(系統)管理人員辦理事件辨識作業，並將辨識結果紀錄在「資安事件記錄處理單」之資安事件辨識作業欄位中。

5.4 事件緊急應變作業

5.4.1 處理事件負責人應依資訊安全事件辨識結果，針對異常狀況協調資訊單位採取緊急應變措施，並將應變方法與注意事項紀錄在「資安事件記錄處理單」。

5.4.2 緊急應變措施應以隔離或停止事件發生之設備、系統、環境及存取權限或連線為原則。

5.5 事件排除作業

5.5.1 負責人應依資訊安全事件發生之原因，協調資訊單位進行事件排除作業。

5.5.2 為避免事件排除作業造成重要資料或鑑識證據之遺失，應於事件排除作業前完成重要設定檔、資料與鑑識記錄檔之備份。

5.5.3 備份作業完成後，應確認備份資料之有效性與可用性，以避免備份失敗導致資料毀損。

5.5.4 事件排除作業除需移除資訊安全事件原因外，應依事件發生原因加強防護，並將加強防護的措施紀錄在「資安事件記錄處理單」作為往後資訊安全日常管理的參考，以避免相同事件再次發生。

5.6 系統復原作業

5.6.1 資訊安全事件排除後，若有需要應由資訊單位或負責人員進行系統復原作業。

5.6.2 資訊單位應於系統復原 3 天內，加強監視系統運作，確認系統屬於正常作業。

5.7 事故矯正措施

5.7.1 採取矯正措施時，應使用適切的資料來源，以分析檢討異常情況發生之原因，針對應改善事項確實檢討改進，並期能避免相同異常事件的再發生。

5.7.2 單位主管審閱異常事件發生狀況及影響程度，依情況嚴重度給予處理。

5.7.3 若為一、二級事件，可即時解決，且影響程度不大，記錄異常事件處理情形，呈請管理代表簽名結案。

5.7.4 若為三、四級事件，可能造成法律訴訟、或影響公司營運及形象，或長期重複發生之異常事件，需進行後續處理及改善追蹤，應依「資訊安全矯正措施管理程序」研擬預防與矯正對策。

5.8 事件檢討與學習

5.8.1 資訊安全事件處理過程應由資訊單位填寫「資安事件記錄處理單」，並保存所有事件分析及處理紀錄。

5.8.2 資訊安全事件處理結果，應定期彙整，描述事件發生原因、過程、處理方式、改善與注意事項等，做為內部資安宣導及事件預防之參考資訊，原則上，由資訊單位每半年以郵件公告方式進行宣導。

5.8.3 若具有標準化之需要時，須採取適當的管制措施，如新增或變更作業程序。

6. 相關文件：

6.1 資訊安全矯正措施管理程序(ISM-2-004)

7. 使用表單：

7.1 資安事件記錄處理單(ISM-2-017-01)

7.2 委外廠商服務人員名冊(ISM-2-011-02)

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY **投標標價清單:(第一次公告)** 標號：TMU113-103

標價清單

※請列出分項價格

採購名稱：防火牆日誌紀錄器

項目	數量	單價	總價
甲、 功能需求內容說明	2台		
1. 獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構（Hardware Appliance）。 2. 系統日誌接收效能可達 6,000 logs/sec（含）以上。 3. 系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。 4. 系統儲存容量可達 16 TB（含）以上，支援磁碟陣列 RAID 0/1, 1s/5, 5s/10 規範。 5. 具備防火牆日誌（Logging）匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。 6. 具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。 7. 具備報表（Reporting）管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。 8. 具備即時性（Real-time）與歷史（Historical）日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。 9. 具備事件監看與告警功能，可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。 10. 具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。 11. 具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。 12. 具備資安維運中心（SOC）檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。 13. 具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服		NT$1,944,900. NT$389,800	

項目	數量	單價	總價

器或 Common Event Format (CEF) 伺服器，以利與既有日誌系統整合。

14. 具備管理區域 (Administrative Domain) 分割功能，並可針對不同管理人員賦予不同的管理權限。

15. 具備 REST API，以利與既有資安環境整合。採購項目說明

乙、 維護標的資訊一覽表

1. 維護等級5x8_設備清單

項次	設備型號	數量	維護期間
1	防火牆日誌紀錄器	1台	驗收日次日起算一年

2. 上述硬體設備得標廠商應提供自驗收次日起 1 年(5*8)人力到場維護保固服務及原廠經銷授權證明。

3. 得標廠商須提供原設備參數轉移與配合網路架構優化相關技術服務。

4. 為確保本案日後維護之保障，廠商須提供網路設備之原廠授權經銷商證明。

★本招標案件不得使用大陸廠牌資通訊產品(含軟體、硬體及服務)

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY

廠商投標議比價單

議價日期	中華民國一一三年十一月二十八日
議價地點	本校醫學綜合大樓前棟三樓第一會議室
議價會議	一一三學年度採購委員會第九次會議
請購單位	資訊處
採購名稱	防火牆日誌紀錄器
交貨期	依投標須知及標單相關規定
備註	※標價需含營業稅額。 ※標價含開狀手續費、報關費、提貨、倉租及將貨運至本校請購單位指定地點等所需之一切費用並需含安裝、裝機完成。 ※結匯金額以所議定之新臺幣金額為上限，期間若因匯率變動致結匯金額超過概由乙方補足，若另有議定條件則不在此限。

議比價記錄

開標價格	優先減價	第一次比減價	第二次比減價	第三次比減價
NT$2,389,800	NT$2,300,000 ※「開標價格」最低者可享有優先減價權。	NT$2,280,000 ※需低於優先減價，否則請註明「無法再減」字樣。	NT$2,230,000	NT$2,190,000

決標價格：新台幣 壹佰玖拾 ~~萬 仟 佰 拾~~ 元整。(含稅)

※附加條件：

1. _____。
2. _____。
3. _____。
4. _____。

投標廠商資料

投標廠統編：28208184

投標廠名稱：泰瑩科技股份有限公司

投標代表人：陳好嘉

投標商電話：0908590641

投標商地址：台北市南京東路四段130號4F

投標廠商蓋章

臺北醫學大學 TAIPEI MEDICAL UNIVERSITY 投標標價清單:(第一次公告) 標號：TMU113-103

請購單位：資訊處，請購人：陳暐傑 先生，聯絡電話：2736-1661 轉 2626

合　　計	新臺幣 貳佰 參拾捌萬 玖仟捌佰 ~~拾~~ ~~元~~整(含稅)			
型　　號	FAZ-810G	原 產 地	美國	Maker Fortinet
交 貨 期	廠商須於 113 年 12 月 13 日前，將採購標的送達請購單位指定地點，安裝測試完畢，且測試結果符合投標須知及標單、契約等規定。			
備　　註	※保固期至少為一年(或依原廠保固期較長為主)，請務必列出分項價格及廠牌。			

廠商資料		投標廠商及負責人章：
	投標商名稱：秦譽科技股份有限公司	
	投標商統編：28208184	
	投標商地址：台北市南京東路四段130號4F	
	投標聯絡人：陳小姐	
	聯絡人電話：0908590611　　手機：0908590611	投標日：113年11月25日

泰瑩科技股份有限公司

「防火牆日誌紀錄器」
決標單價分析表(含稅)

單位： 新台幣元

編號	品項	單價	數量	單位	小計
1	防火牆日誌紀錄器	NT$950,000	2	台	NT$1,900,000
				總計	NT$1,900,000

得標廠商(大小章)：

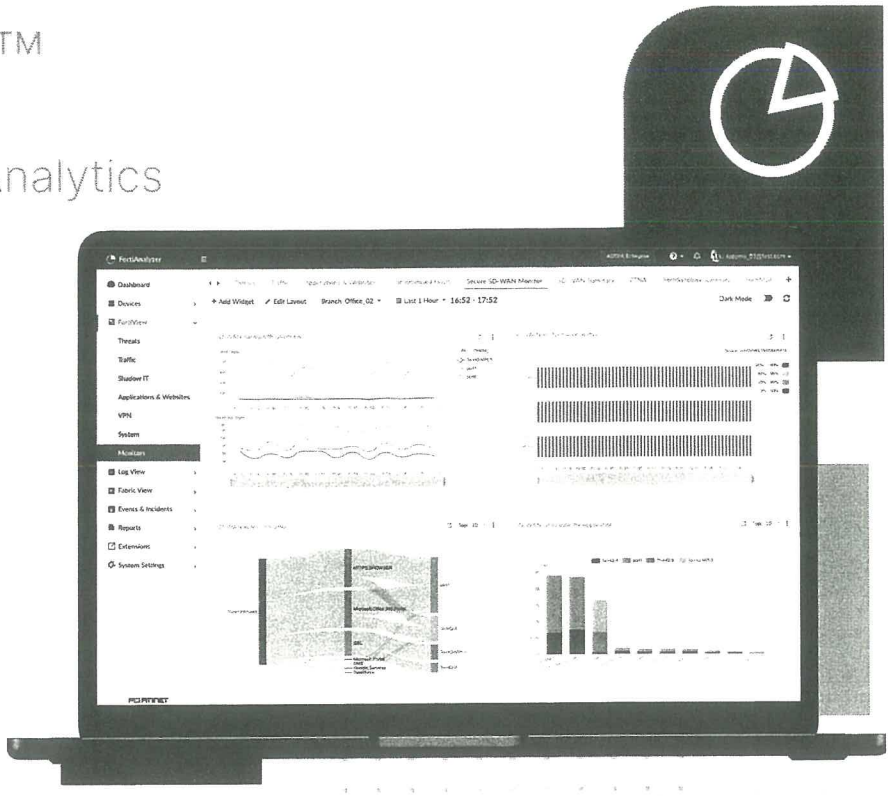
設備規格答覆及資料佐證索引

防火牆日誌紀錄器 (FortiAnalyzer-810G)		符合	不符合	佐證資料
1.	獨立主機採硬體式設備並使用嵌入式或專屬作業系統架構 (Hardware Appliance)。	符合		附件 Page. 5
2.	系統日誌接收效能可達 6,000 logs/sec (含)以上。	符合		附件 Page. 7
3.	系統提供 4 埠(含)以上 GE 介面、 2 埠(含)以上 GE SFP 介面。	符合		附件 Page. 7
4.	系統儲存容量可達 16 TB (含)以上，支援磁碟陣列 RAID 0/1,1s/5,5s/10 規範。	符合		附件 Page. 7
5.	具備防火牆日誌 (Logging) 匯集功能，須能將本校防火牆(FortiGate)的日誌統一集中管理。	符合		附件 Page. 5
6.	具備與本校防火牆(FortiGate)通訊傳輸資料加密功能。	符合		附件 Page. 12
7.	具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF、HTML、CSV、XML。	符合		附件 Page. 22 附件 Page. 23
8.	具備即時性 (Real-time) 與歷史 (Historical) 日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、系統管理事件，查看並提供摘要資訊。	符合		附件 Page. 13 附件 Page. 14 附件 Page. 15 附件 Page. 17
9.	具備事件監看與告警功能，可從日誌中擷取過濾資訊來形成事件並觸發告警，告警可以 Email、SNMP、Syslog 的方式發送。	符合		附件 Page. 18
10	具備 SD-WAN 線路 SLA 資訊收集能力，可記錄線路 SLA 狀態包括 Jitter、Latency 與 Packet Loss 等。	符合		附件 Page. 16
11.	具備以圖表方式顯示 SD-WAN 語音通話的 MOS 分數值。	符合		附件 Page. 16

12.	具備資安維運中心（SOC）檢視功能，可自訂儀錶板將重要的資安與系統訊息匯集在單一檢視畫面，方便中央監看、顯示資安威脅、深入追蹤與採取行動。	符合		附件 Page. 15 附件 Page. 19 附件 Page. 20 附件 Page. 21
13.	具備日誌轉發功能，可將日誌發送給其他 Syslog 伺服器或 Common Event Format（CEF）伺服器，以利與既有日誌系統整合。	符合		附件 Page. 24
14.	具備管理區域（Administrative Domain）分割功能，並可針對不同管理人員賦予不同的管理權限。	符合		附件 Page. 25
15.	具備 REST API，以利與既有資安環境整合。	符合		附件 Page. 11

FortiAnalyzer™

Security Fabric Network Analytics



Highlights

- Centralized network monitoring and visibility
- Advanced threat and vulnerability detection with event and log data correlation
- Augmented NOC/SOC operations for real-time response, analytics, and reporting
- Automation to save time, reduce errors, and improve efficiency
- Multi-tenancy solution with quota management
- Administrative domains for operational effectiveness and compliance
- 70+ reports and 2000+ ready-to-use datasets, charts, and macros

Analytics, Reports, and Compliance Across the Security Fabric

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

Capabilities

Incident Detection and Response

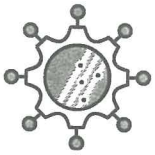
Centralized NOC/SOC Visibility for the Attack Surface

FortiAnalyzer provides Security Fabric Analytics across all device logs with event correlation and real-time detection of Advanced Persistent Threats (APTs), vulnerabilities and Indicators of Compromise (IOC) for FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail and other Fortinet products, for deep visibility and critical network insights. Simplified orchestration and automated workflows provide Network Security Operations teams with real-time notifications, reports, and dashboards for single-pane visibility and actionable results.

Incidents and Events Management

Security teams can monitor and manage alerts and event logs from Fortinet devices, with events processed and correlated in a format that analysts can easily understand. Investigate suspicious traffic patterns and search using filters in predefined or custom event handlers to generate real-time notifications and monitoring for NOC and SOC operations, SD-WAN, SSL VPN, wireless, Shadow IT, IPS, network recon, FortiClient, and more.

The Incidents component enables analysts to manage incident handling and life cycle, with incidents generated by events that show affected assets, endpoints, users and timelines.



Fabric Automation

FortiAnalyzer Playbooks boost an organization's security team abilities to simplify investigation efforts through automated incident response, freeing up resources and allowing analysts to focus on critical tasks. Out-of-the-box playbook templates enable SOC analysts to quickly customize their use cases, define custom processes, interact with other Security Fabric devices like FortiOS and EMS, edit playbooks and tasks in the visual playbook editor and use the Playbook Monitor for investigation of compromised hosts, infections and critical incidents, data enrichment for Assets and Identity views, blocking malware, C&C IPs, and more.

Security Fabric Analytics

Analytics and Reporting

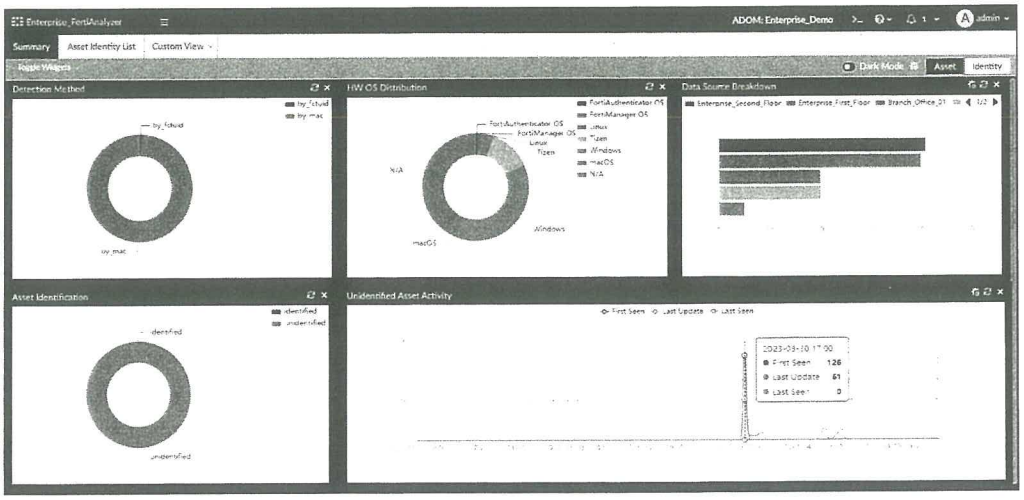
FortiAnalyzer automation driven analytics empowers network security operations teams to complete a fast assessment of network devices, systems, and users, with correlated log data and FortiGuard threat intelligence for analysis of real-time and historical events.

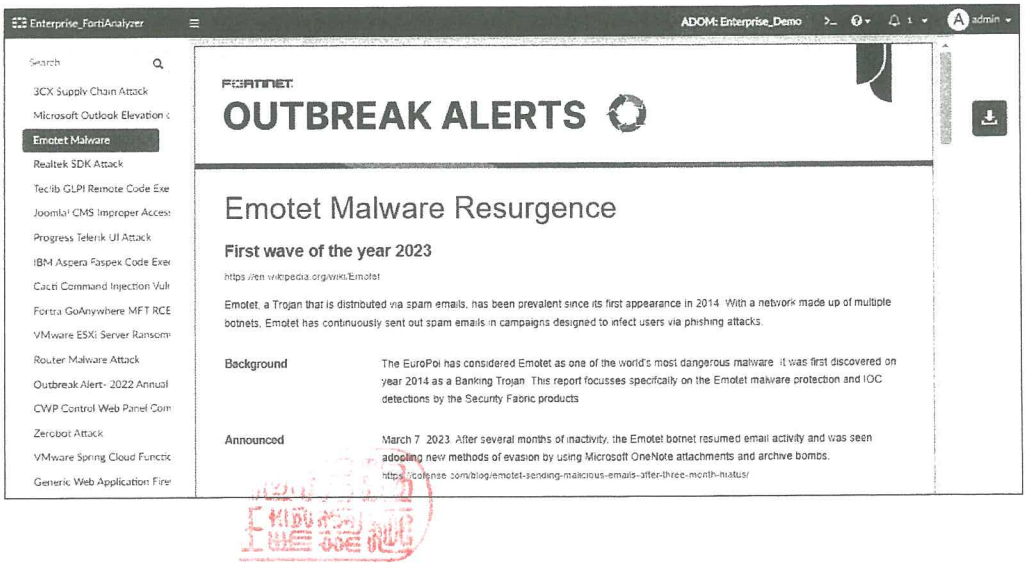
- **FortiView** Monitors and Views provide deep insights with context and meaning of network activity, risks, vulnerabilities, attack attempts, indicators of compromise and anomalies, sanctioned and unsanctioned user activity.
- **Log View** enables analysts to expand their investigation and utilize search filters on managed device logs, drill down on logs, with custom views and log groups, including a SIEM database with normalized logs for Fortinet devices in Fabric ADOMs.
- **Reports** provide comprehensive analysis of your Security Posture, including reports for Operational Technology (OT), security rating, security rating for PCI, Secure SD-WAN, VPN, FortiNDR network anomaly detection, cyber threat assessments, 360 Security Reviews, situational awareness, compliance, auditing, and more.

Capabilities

Assets and Identity

FortiAnalyzer Fabric View with Assets and Identity monitoring provides SOC teams with elevated awareness and visibility into an organization's endpoints and users with dashboards and correlated device and UEBA information, vulnerability detections, EMS tagging, and asset classifications through telemetry with EMS, NAC, Fortinet Fabric Agent, and an OT Dashboard View.





Subscriptions and Extensions

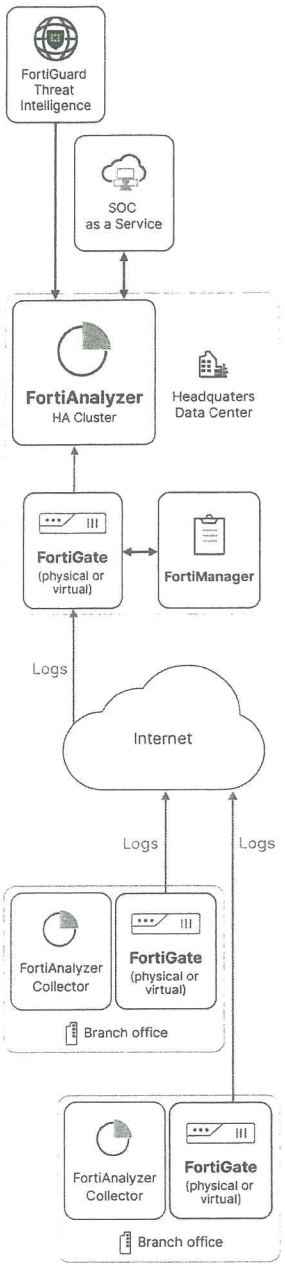
Subscription Licenses and FortiGuard Security Services

- **FortiGuard Outbreak Detection Service** delivers automated content package download for detecting the latest malware, including a summary of outbreaks and kill chain mapping for how the malware works. The package includes a FortiGuard Report for the outbreak, Event Handler, and a Report Template to detect outbreaks.
- **FortiGuard Indicators of Compromise Service** empowers security teams with forensic data from 500 000 IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system, that have been determined with high confidence to be malicious infections or intrusions, and historical rescan of logs for threat hunting.
- **Shadow IT Monitoring Service** provides continuous monitoring of unapproved devices, resources, unsanctioned accounts and unauthorized use of SaaS and IaaS, API integration, and third party apps. The service identifies rogue users using personal accounts for managing company assets, using correlated FortiOS and FortiCASB data with a FortiCASB account subscribed for SaaS features.
- **OT Security Service** provides security teams with advanced OT analytics, risk and compliance reports, OT event handlers, and use-case correlation rules.
- **Security Rating and Compliance Service** helps security teams design, implement, and maintain their security posture, and provides actionable configuration recommendations as well as key performance and risk indicators.
- **Security Automation Service** subscription enables further automation for incident response with enhanced monitoring and escalation, built-in incident management workflows, connectors, playbooks and more.

Management Extension Applications (MEAs)

The Management Extensions pane allows you to enable licensed applications that are released and signed by Fortinet, which can be installed and run on FortiAnalyzer, including the FortiSIEM and FortiSOAR.

Deployments



Deploying FortiAnalyzer

FortiAnalyzer can be deployed as a physical hardware appliance, virtual machine (VM) and virtual machine subscription (VM-S), as well as private or public cloud instance, with scalability, redundancy and backup, and high availability capabilities.

FortiAnalyzer High Availability (HA)

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

Multi-Tenancy with Flexible Quota Management

FortiAnalyzer provides the ability to manage multiple sub-accounts with each account having its own administrators and users. The time-based archive/analytic log data policy, per Administrative Domain (ADOM), allows automated quota management based on the defined policy, with trending graphs to guide policy configuration and usage monitoring.

Analyzer Collector Modes

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

FortiAnalyzer Fabric

FortiAnalyzer Fabric allows SOC Administrators to configure two operation modes - Supervisor and Member. This allows viewing of member devices, ADOMs and authorized logging devices, as well as incidents and events created on members. Admins get access to Reports and FortiView across all member FortiAnalyzers, and can perform global search in Log View of logs collected across FortiAnalyzer Fabric members with pre-defined device filters and log drill down for each Member and Member ADOMs.

Log Forwarding for Third-Party Integration

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

Cloud Services

FortiAnalyzer Cloud

FortiAnalyzer Cloud offers customers a PaaS-based delivery option for automation-driven, single pane analytics, providing log management, analytics, and reporting for Fortinet NGFW and SD-WAN with an easily accessible cloud-based solution. FortiAnalyzer Cloud delivers reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture. Customers can easily access their FortiAnalyzer Cloud from their FortiCloud single sign-on portal.

Virtual Offerings

FortiAnalyzer VM Subscription

The FortiAnalyzer VM Subscription license model consolidates into one single SKU: VM product SKU, FortiCare Support SKU, FortiGuard IOC and Outbreak Detection Service, Security Automation services, to simplify the product purchase, upgrade, and renewal. FortiAnalyzer-VM S provides organizations with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet and third party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer-VM S series SKUs come in stackable 5, 50, and 500 GB/ day logs licenses, so that multiple units of this SKU can be purchased together providing organizations with the ability and cost-efficiencies to scale and meet their logging needs.

FortiAnalyzer VM

Fortinet offers the FortiAnalyzer-VM licensing in a stackable perpetual license model with a-la-carte technical support and subscription services.

This software-based version of the FortiAnalyzer hardware appliance is designed to run on many virtualization platforms, which allows you to expand your virtual solution as your environment expands.

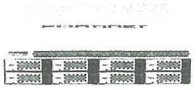
FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity						
GB/ day of Logs *	+1	+5	+25	+100	+500	+2000
Devices/VDOMs Maximum	10 000	10 000	10 000	10 000	10 000	10 000
FortiGuard IOC Service			✓			
Security Automation Service			✓			
Hypervisor Support	Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit https://docs.fortinet.com/product/fortianalyzer/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"					
vCPU Support (Minimum / Maximum)	4 / Unlimited					
Network Interface Support (Min / Max) **	1 / 12					
Memory Support (Minimum / Maximum)	16 GB / Unlimited for 64-bit					

* Unlimited GB/ day when deployed in collector mode.

** VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms

Specifications



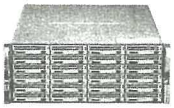
FORTIANALYZER APPLIANCES	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000G
Capacity and Performance				
GB/ day of Logs	25	100	200	660
Analytic Sustained Rate (logs/ sec)*	500	2000	4000	20 000
Collector Sustained Rate (logs/ sec)*	750	3000	6000	30 000
Devices/VDOMs (Maximum)	50	180	800	2000
Max Number of Days Analytics**	90	50	50	60
Options				
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓	✓
Security Automation Service	✓	✓	✓	✓
Enterprise Bundle	✓	✓	✓	✓
Hardware Bundle	✓	✓	✓	✓
OT Security Service	✓	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓	✓
Hardware Specifications				
Form Factor (supports EIA/non-EIA standards)	Desktop	1 RU Rackmount	1 RU Rackmount	2 RU Rackmount
Total Interfaces	2x RJ45 GE	4x RJ45 GE	4x RJ-45 2x GE SFP	2× 2.5GbE RJ45 + 2× 25GbE SFP28
Storage Capacity	4TB (2× 2TB)	8 TB (2× 4 TB)	16TB (4× 4TB) 3.5 in SAS HDDs	32 TB (8 × 4TB) 3.5 in SAS SED HDD
Usable Storage (After RAID)	2 TB	4 TB	8 TB	24 TB
Removable Hard Drives	No	No	✓	✓
RAID Levels Supported	0/1	RAID 0/1	RAID 0/1,1s/5,5s/10	RAID 0/1/5/6/10/50/60
RAID Type	Software	Software	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	1	1	10	50
Redundant Hot Swap Power Supplies	No	Optional	Optional	✓
Trusted Platform Module (TPM) ***	Gen 2	Gen 2	✓	✓
Dimensions				
Height x Width x Length (inches)	9.5 × 3.5 × 8	1.73 × 17.24 × 16.38	1.73 × 17.32 × 21.65	3.46 × 17.24 × 24.41
Height x Width x Length (cm)	24.1 × 8.9 × 20.55	4.4 × 43.8 × 41.6	4.4 × 44.0 × 55.0	8.8 × 43.8 × 62.0
Weight	9.35 lbs (4.24 kg)	22.5 lbs (10.2 kg)	25.75 lbs (11.68 kg)	49.6 lbs (22.5 kg)
Environment				
AC Power Supply	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100-240Vac, 50~60Hz, 4A max	100-240Vac, 50~60Hz, 4A max
Power Consumption (Average / Maximum)	36 W / 43 W	90.1 W / 99 W	115W / 150W	251.36W / 302W
Heat Dissipation	147.4 BTU/h	337.8 BTU/h	433 BTU/h	857.73 BTU/h
Operating Temperature	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)
Storage Temperature	-4°F to 167° F (-20°C to 75° C)	-13°F to 167° F (-25°C to 75° C)	-4°F to 167° F (-20°C to 75° C)	-40°F to 158° F (-40°C to 70° C)
Humidity	5% to 95% non-condensing	20% to 90% non-condensing	5% to 95% non-condensing	5% to 95% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 16 404 ft (5000 m)
Compliance				
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

Specifications


FORTIANALYZER APPLIANCES	FAZ-3100G	FAZ-3510G	FAZ-3700G
Capacity and Performance			
GB/ day of Logs	3000	5000	8300
Analytic Sustained Rate (logs/sec)*	42 000	60 000	100 000
Collector Sustained Rate (logs/sec)*	60 000	90 000	150 000
Devices/VDOMs (Maximum)	4000	10 000	10 000
Max Number of Days Analytics**	30	35	60
Options			
FortiGuard IOC and Outbreak Detection Service	✓	✓	✓
Security Automation Service	✓	✓	✓
Enterprise Bundle	✓	✓	✓
Hardware Bundle	✓	✓	✓
OT Security Service	✓	✓	✓
Security Rating and Compliance Service	✓	✓	✓
Hardware Specifications			
Form Factor (supports EIA/non-EIA standards)	3 RU Rackmount	4 RU Rackmount	4 RU Rackmount
Total Interfaces	2x GE RJ45, 2× 25GE SFP28	2× 10GbE RJ45, 2× 25GbE SFP28	2× 10GE RJ-45 + 2× 25GE SFP28
Storage Capacity	64 TB (16 × 4TB) 3.5" SAS SED HDD + 3.84 (2× 1.92TB) 2.5" NVMe SSD	24× 4TB (96TB) + 2× 3.84TB (7.68TB)	240TB (60× 4TB) 3.5 in HDD + 19.2TB (6× 3.2TB) NVMe SSD
Usable Storage (After RAID)	56 TB	84 TB	224 TB
Removable Hard Drives	✓	✓	✓
RAID Levels Supported	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60
RAID Type	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	50	50	50
Redundant Hot Swap Power Supplies	✓	✓	✓
Trusted Platform Module (TPM) ***	✓	✓	✓
Dimensions			
Height x Width x Length (inches)	5.2 × 17.2 × 25.5	7 × 17.2 × 27.5	7.0 × 17.2 × 30.2
Height x Width x Length (cm)	13.0 × 44.0 × 65.0	17.8 × 43.7 × 69.9	17.8 × 43.7 × 76.7
Weight	69.6 lbs (31.57 kg)	65 lbs (29.5 kg)	118 lbs (53.5 kg)
Environment			
AC Power Supply	100-127V~/10A, 200-240V~/5A	100-127V~/10A, 200-240V~/5A	2000W AC****
Power Consumption (Average/Max)	395 W / 510 W	983 W / 1278 W	850 W / 1423.4 W
Heat Dissipation	1740.19 BTU/h	3424 BTU/h	4858 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	50°F to 95°F (10°C to 35°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)	-4°F to 167°F (-20°C to 75°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	5% to 95% (non-condensing)	5% to 95% (non-condensing)	8% to 90% (non-condensing)
Forced Airflow	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 13 123 ft (4000 m)	Up to 10 000 ft (3048 m)	Up to 7400 ft (2250 m)
Compliance			
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB

* Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

** is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

*** Gen2 refers to hardware that has been upgraded since initial release.

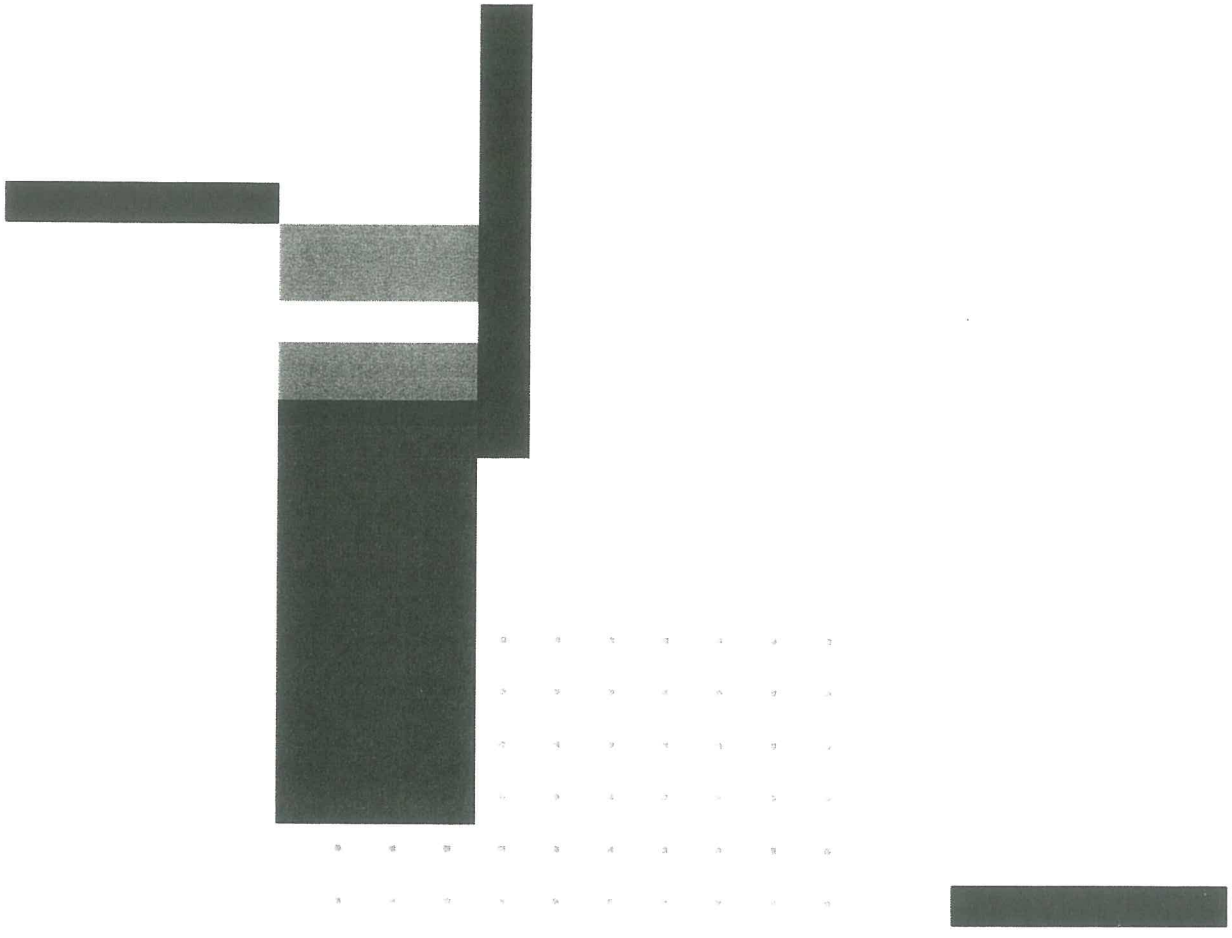
****3700G must connect to a 200V - 240V power source.

Ordering Information

Product	SKU	Description
FortiAnalyzer	FAZ-150G	Centralized log and analysis appliance — 2x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.
	FAZ-300G	Centralized log and analysis appliance — 4x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.
	FAZ-810G	Centralized log and analysis appliance — 4x GE, 2x SFP, 16 TB self-encrypting storage, up to 200 GB/ day of logs.
	FAZ-1000G	Centralized logging and analysis appliance - 2× 2.5GbE RJ45 + 2× 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs.
	FAZ-3100G	Centralized log and analysis appliance — 2x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3000 GB/ day of logs.
	FAZ-3510G	Centralized log and analysis appliance — 2× 10GbE RJ45, 2× 25GbE SFP28, 96 TB storage, up to 5000 GB/ day of logs.
	FAZ-3700G	Centralized log and analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 240TB HDD + 19.2TB NVMe SSD storage, up to 8300 GB/ day of Logs.
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-465-01-DD	Subscription license for 5 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC2-10-AZVMS-465-01-DD	Subscription license for 50 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC3-10-AZVMS-465-01-DD	Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
FortiAnalyzer-VM	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of Logs.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs.
FortiAnalyzer Cloud Storage Subscription	FC1-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
	FC2-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
	FC3-10-AZCLD-463-01-DD	Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
FortiAnalyzer - Backup to Cloud Service	FC-10-FAZ00-286-02-DD	One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.
FortiAnalyzer Cloud with SOCaaS	FC-10-[Model Code]-464-02-DD	FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.
FortiAnalyzer Cloud	FC-10-[Model Code]-585-02-DD	FortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service.
Security Automation Service	FC-10-[Model Code]-335-02-DD	Subscription license for Security Automation Service - Appliance.
	FC[GB Day Code]-10-LV0VM-335-02-DD	Subscription license for Security Automation Service - Virtual Machine.
FortiGuard IOC and Outbreak Detection Service	FC-10-[Model Code]-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.
	FC[GB Day Code]-10-LV0VM-661-02-DD	Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.
OT Security Service	FC-10-[Model Code]-159-02-DD	OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules.
FortiAnalyzer Security Rating and Compliance Service	FC-10-[Model Code]-175-02-DD	Subscription license for FortiAnalyzer Security Rating and Compliance Service.
Enterprise Protection Bundle	FC-10-[Model Code]-466-02-DD	Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).
Hardware Bundle	FAZ-[Hardware Model]-BDL-466-DD	Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Avatars

When FortiClient sends logs to FortiAnalyzer, an avatar for each user can be displayed in the *Source* column in the *FortiView* and *Log View* panes. FortiAnalyzer can display an avatar when FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiAnalyzer enabled.

15

- When FortiClient Telemetry connects to FortiGate, FortiClient sends logs (including avatars) to FortiGate, and the logs display in FortiAnalyzer under the FortiGate device as a sub-type of security.
  The avatar is synchronized from FortiGate to FortiAnalyzer by using the FortiOS REST API.
- When FortiClient Telemetry connects to FortiClient EMS, FortiClient sends logs (including avatars) directly to FortiAnalyzer, and logs display in a FortiClient ADOM.

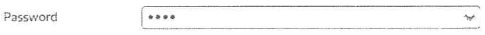
If FortiAnalyzer cannot find the defined picture, a generic, gray avatar is displayed.

You can also optionally define an avatar for FortiAnalyzer administrators. See Creating administrators on page 351.

Showing and hiding passwords

In some cases you can show and hide passwords by using the toggle icon. When you can view the password, the *Toggle show password* icon is displayed:

When you can hide the password, the *Toggle hide password* icon is displayed:



Target audience and access level

This guide is intended for administrators with full privileges, who can access all panes in the FortiAnalyzer GUI, including the *System Settings* pane.

In FortiAnalyzer, administrator privileges are controlled by administrator profiles. Administrators who are assigned profiles with limited privileges might be unable to view some panes in the GUI and might be unable to perform some tasks described in this guide. For more information about administrator profiles, see Administrator profiles on page 358.

If you logged in by using the `admin` administrator account, you have the *Super_User* administrator profile, which is assigned to the *admin* account by default and gives the `admin` administrator full privileges.

Initial setup

This topic provides an overview of the tasks that you need to do to get your FortiAnalyzer unit up and running.

ADOMs must be enabled to support FortiCarrier, FortiClient EMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox logging and reporting. See Administrative Domains (ADOMs) on page 296.

Logs

Logs in FortiAnalyzer are in one of the following phases.

- Real-time log: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file.
- Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline.
- Analytics logs or historical logs: Indexed in the SQL database and online.

In order for FortiAnalyzer to accept logs, the sending device must be registered in FortiAnalyzer. You can add devices to FortiAnalyzer by specifying the serial number and other details, or you may point the device's log settings to the FortiAnalyzer. If initiated by the remote device, the device must be authorized before logs can be received on FortiAnalyzer. See Adding devices on page 41.

For more information on the types of logs collected for each device, see Types of logs collected for each device on page 88.

Log encryption

Beginning in FortiAnalyzer 6.2, all logs from Fortinet devices (using Fortinet's proprietary protocol: OFTP) must be encrypted. FortiAnalyzer encryption level must be equal or less than the sending device's level. For example, when configuring logging from a FortiGate, FortiAnalyzer must have the same encryption level or lower than FortiGate in order to accept logs from FortiGate.

To configure the encryption level on FortiAnalyzer:

1. In the FortiAnalyzer CLI, enter the following commands:

```
config system global
    set enc-algorithm {high | low | medium}
```

To configure the encryption level on FortiGate:

1. In the FortiGate CLI, enter the following commands:

```
config log fortianalyzer setting
    set enc-algorithm {high-medium | high | low}
```

See also Appendix B - Log Integrity and Secure Log Transfer on page 405.

Log storage

Logs and files are stored on the FortiAnalyzer disks. Logs are also temporarily stored in the SQL database.

FortiView dashboards for FortiGate and FortiCarrier devices

Category	View	Description
Threats	Top Threats	Lists the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus.
	Threat Map	Displays a map of the world that shows the top traffic destinations starting at the country of origin. Threats are displayed when the threat score is greater than zero and either the source or destination IP is a public IP address. The *Threat Window* below the map, shows the threat, source, destination, severity, and time. The color gradient of the lines indicate the traffic risk. A yellow line indicates a high risk and a red line indicates a critical risk. This view does not support filtering and *Day*, *Night*, and *Ocean* themes. See also Viewing the threat map on page 58.
	Compromised Hosts	Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats. To use this feature: 1. UTM logs of the connected FortiGate devices must be enabled. 2. The FortiAnalyzer must subscribe to FortiGuard to keep its threat database up-to-date.
	FortiSandbox Detection	Displays a summary of FortiSandbox related detections. The following information is displayed: Filename, End User and/or IP, Destination IP, Analysis (Clean, Suspicious or Malicious rating), Action (Passthrough, Blocked, etc.), and Service (HTTP, FTP, SMTP, etc.). Select an entry to view additional information in the drilldown menu. Clicking a FortiSandbox action listed in the *Process Flow* displays details about that action, including the *Overview*, *Indicators*, *Behavior Chronology Chart*, *Tree View*, and more. Information included in the *Details* and *Tree View* tab is only available with FortiSandbox 3.1.0 and above.

Category	View	Description
Traffic	Top Sources	Displays the highest network traffic by source IP address and interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Source Addresses	Displays the top source addresses by source object, interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Destinations	Displays the highest network traffic by destination IP addresses, the applications used to access the destination, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Destination Addresses	Displays the top destination addresses by destination objects, applications, sessions, and bytes. If available, click the icon beside the IP address to see its WHOIS information.
	Top Country/Region	Displays the highest network traffic by country in terms of traffic sessions, including the destination, threat score, sessions, and bytes.
	Policy Hits	Lists the policy sessions by policy, device name, VDOM, number of hits, bytes, and last used time and date.
	DNS Logs	Summarizes the DNS activity on the network. Double click an entry to drill down to the specific details about that domain.
	ZTNA Servers	ZTNA servers by bytes.
Shadow IT	Top Cloud Applications	Displays the top cloud applications used on the network. When viewing information about an application, FortiAnalyzer will first check the Shadow IT database, and if no results are found, it will use the metadata.
	Top Cloud Users	Displays the top cloud users on the network.
Applications & Websites	Top Applications	Displays the top applications used on the network including the application name, category, risk level, and sessions blocked and allowed. Bytes sent and received can also be enabled through the widget settings. Top Applications can be viewed as a stackbar, bar, table, or bubble chart. For a usage example, see Finding application and user information on page 68.
	Top Website Domains	Displays the top allowed and blocked website domains on the network.
	Top Website Categories	Displays the top website categories.
	Top Browsing Users	Displays the top web-browsing users, including source, group, number of sites visited, browsing time, and number of bytes sent and received.

Category	View	Description
VPN	SSL & Dialup IPsec	Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec). You can view VPN traffic for a specific user from the top view and drilldown views. In the top view, double-click a user to view the VPN traffic for the specific user. In the drilldown view, click an entry from the table to display the traffic logs that match the VPN user and the destination.
	Site-to-Site IPsec	Displays the names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network.
System	Admin Logins	Displays the users who logged into the managed device.
	System Events	Displays events on the managed device.
	Resource Usage	Displays device CPU, memory, logging, and other performance information for the managed device. Resource Usage includes two widgets: *Resource Usage Average* and *Resource Usage Peak*.
	Failed Authentication Attempts	Displays the IP addresses of the users who failed to log into the managed device.

Using FortiView

When ADOMs are enabled, *FortiView* displays information for each ADOM. Please ensure you are in the correct ADOM. See Switching between ADOMs on page 26.

- Viewing FortiView dashboards on page 57
- Filtering FortiView on page 59
- Viewing related logs on page 59
- Exporting filtered summaries on page 59
- Monitoring resource usage of devices on page 60
- Long-lived session handling on page 60

Viewing FortiView dashboards

When viewing FortiView dashboards, use the controls in the toolbar to select a device, specify a time period, refresh the view, and switch to full-screen mode.

Many widgets on FortiView dashboards let you drill down to view more details. To drill down to view more details, click, double-click, or right-click an element to view details about different dimensions in different tabs. You can continue to drill down by double-clicking an entry. Click the close icon in the widget's toolbar to return to the previous view.

Many FortiView widgets support multiple chart types such as table view, bubble view, map view, tile view, etc.

- In widgets that support multiple views, select the settings icon in the top-right corner of the widget to choose another view.

SD-WAN Bandwidth Overview	The bandwidth of the SD-WAN network over time. This widget displays a line chart of the sent/received rate (bps) in the selected time period for SD-WAN members interfaces.
SD-WAN Performance Status	The SD-WAN performance status comparison with interfaces. Mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check. Click on a scatter chart to view additional details.
SD-WAN Rules Utilization	The SD-WAN rule traffic utilization by interface and application.
SD-WAN Utilization by Application	The share of bandwidth utilization by application for each WAN link.
一、10 **Top SD-WAN SLA Issues**	The top SD-WAN SLA issues.
Health Check Status	This widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.
SD-WAN Events	This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.
Application Bandwidth Utilization	The total bandwidth from all applications as well as the bandwidth per-SD-WAN interface. This widget can be viewed in a sanky chart or table chart format.
Per-Application Performance	The performance for the selected application based on chosen metric. You can select an application in the widget's *Application* dropdown menu. *Latency*, *Jitter*, *Packet Loss*, and *Bandwidth* metrics are available.
Global-Application Performance	The global application performance for the selected metric. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
SD-WAN Interfaces	The information for SD-WAN interfaces and ADVPN shortcut interfaces. *Latency*, *Jitter*, and *Packet Loss* metrics are available.
一、11 **Audio MOS Score**	The MOS score by interface. Mousing over the chart displays a summary of the MOS score and VoIP quality at that point. The interface must have a performance SLA with MOS enabled to display in the chart.

To update the *Refresh Interval*, click the settings icon at the top of the widget, and then select a value from the dropdown.

To filter a chart, click a key in the legend.

SD-WAN Summary

SD-WAN Summary monitor includes the following widgets:

SD-WAN Health Overview	The SD-WAN devices' status.

device(s) and time frame for the event logs.

The *Total Events* widget on this dashboard displays a line chart of event logs by level. You can hover your cursor over the line chart to display a summary of the count and time at that point.

The other widgets on this dashboard list the event names for the displayed event types. These widgets can be toggled on/off from the *Toggle Widgets* dropdown. By clicking an event name in the widget, you can open a list view of those event logs filtered by the devices and time frame you selected on the dashboard.

Viewing historical and real-time logs

By default, *Log View* displays historical logs. *Custom View* and *Chart Builder* are only available in historical log view.

To view real-time logs, in the log message list view toolbar, click *Tools* > *Real-time Log*.

To switch back to historical log view, click *Tools* > *Historical Log*.

Viewing raw and formatted logs

By default, *Log View* displays formatted logs. The log view you select affects available view options. You cannot customize columns when viewing raw logs.

To view raw logs, in the log message list view toolbar, click *Tools* > *Display Raw*.

To switch back to formatted log view, click *Tools* > *Formatted Log*.

For more information about FortiGate raw logs, see the *FortiGate Log Message Reference* in the Fortinet Document Library. For more information about raw logs of other devices, see the *Log Message Reference* for the platform type.

Option	Description
	• *Match Criteria*: Select an operator from the dropdown. • *Value*: Select the event type from the dropdown. To delete a condition, click the *delete* icon next to the condition.
Generic Text Filter	(Optional) Enter a filter string. For more information, see Using the Generic Text Filter on page 177.

Creating notification profiles

Notification profiles are used to send alert notifications when an event is generated by an event handler. You can configure the notification profile to send the alert to an email address, SNMP community, and/or syslog server. You can also configure the notification profile to send the alert through a fabric connector.

You can create, edit, clone, and delete notification profiles in *FortiSoC/Incidents & Events* > *Handlers* > *Notification Profile List*.

To assign a notification profile to a basic event handler, see Creating a custom event handler on page 168.

To assign a notification profile to a correlation handler, see Creating a custom correlation handler on page 171.

To create a notification profile:

1. Go to *FortiSoC/Incidents & Events* > *Handlers* > *Notification Profile List*.
2. Click *Create New*.
   The *Add New Notification Profile* pane displays.
3. Configure the following options, and click *OK* to save the notification profile.

Option	Description
Name	Enter a name for the notification profile.
Send Alert through Fabric Connectors	Send an alert through one or more fabric connectors selected from the dropdown. Click the plus (+) to add fabric connectors. For more information, see Fabric Connectors on page 112.
Send Alert Email	Send an alert to one or more email addresses. Specify the email parameters, including the mail server. For more information, see Mail Server on page 333.
To	Enter the email address(es) to send the alert to. Use a semicolon (;) to separate multiple email addresses.
From	Enter a from address for the alert email.
Subject	Enter a subject line for the alert email.
Email Server	Select the mail server for the alert email.
Send SNMP(...) Trap	Send an alert to an SNMP community or user selected from the dropdown. For more information, see SNMP on page 324.

FortiSoC

FortiSoC is a subscription service that enables playbook automation for security operations on FortiAnalyzer.

FortiAnalyzer's SIEM capabilities parse, normalize, and correlate logs from Fortinet products and the security event log of Windows and Linux hosts (with Fabric Agent integration). Parsing is predefined by FortiAnalyzer and does not require manual configuration by administrators. SIEM logs are displayed as *Fabric logs* in *Log View* and can be used when generating reports. See Types of logs collected for each device on page 88.

FortiSoC provides incident management capabilities with playbook automation to accelerate incident response. When FortiAnalyzer has a valid subscription license, the FortiSoC module is activated and administrators are able access playbook automation features. Task automation can be configured by SOC analysts using playbooks which consist of a trigger and sequence of automated actions. Playbooks can be created from scratch or by using one of the predefined templates. Fabric connectors further enhance FortiSoC functionality by allowing playbooks to perform tasks using connected devices, including FortiOS and FortiClient EMS.

FortiSoC includes a trial with a limited capacity allowing up to five playbooks per day. A SOC subscription is required to run at full capacity. For additional information about licensing, please see support.fortinet.com.

For information about FortiSoC incidents and events, see Incident and Event Management on page 135.

Viewing FortiSoC dashboards

一、12

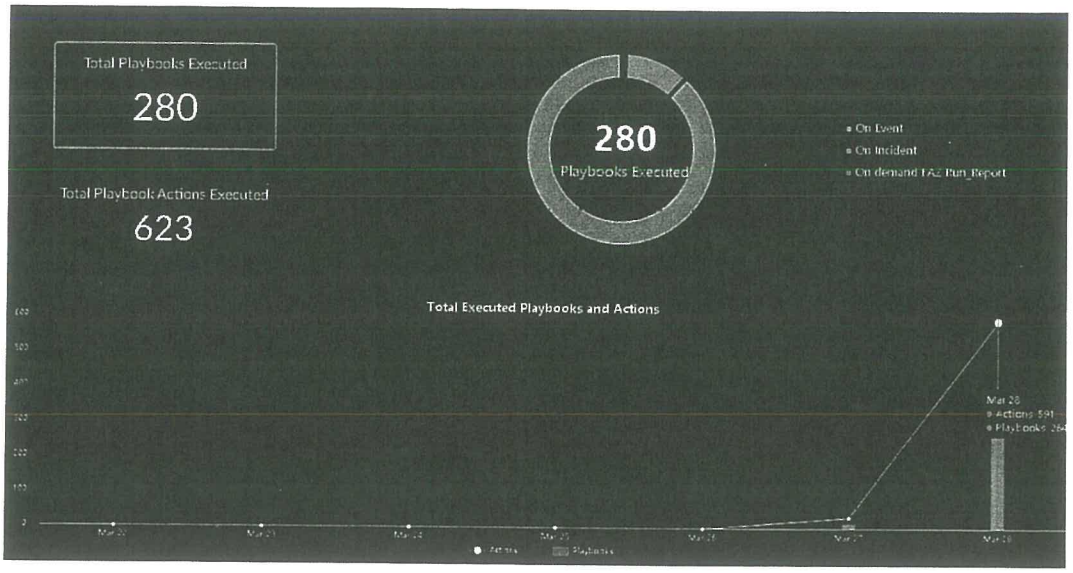
FortiSoC includes multiple dashboards for viewing information about playbooks, incidents, and events.

There is a toolbar available for each dashboard, providing the following options:

Dark Mode	Enable/disable dark mode. Dark mode shows a black background for the dashboard.
Refresh	From the *Refresh* dropdown in the toolbar, you can select a frequency for the dashboard to automatically refresh the information. If you need to manually refresh the dashboard before it is done automatically, click *Refresh* in the toolbar. By default, the refresh frequency is set to *Manual Refresh*. Click *Refresh* in the toolbar to refresh the dashboard when needed.

Playbooks

一、12

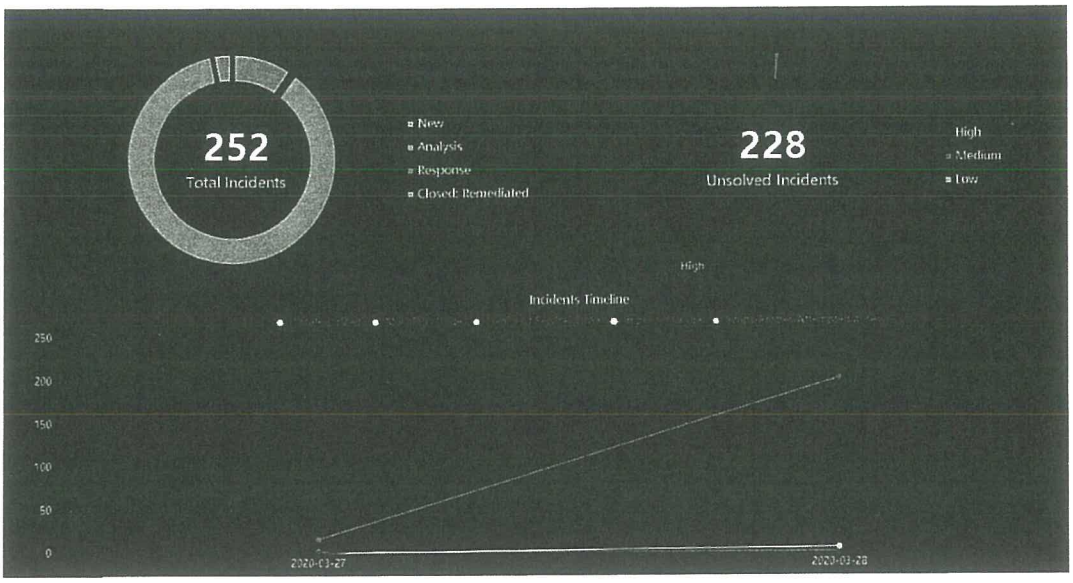


The *Playbooks* dashboard includes:

Total Playbooks Executed	The total number of playbooks executed.
Total Playbook Actions Executed	The total number of playbook actions (tasks) executed.
Playbooks Executed	The number of times each playbook has been run.
Overall Time Saved	The estimated time saved by administrators resulting from FortiSoC automation.
Total Executed Playbooks and Actions	A timeline of the number of playbooks and actions run for each day. Both actions and playbooks can be toggled on or off in the graph by clicking the corresponding name below the graph.

Incidents

一、12

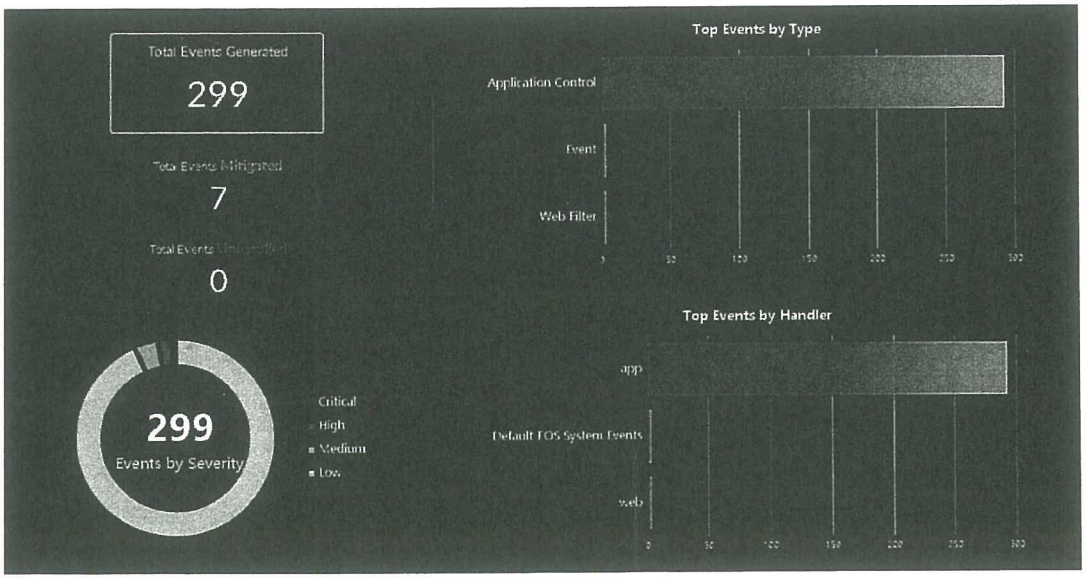


The *Incidents* dashboard includes:

Total Incidents	Displays the total number of incidents created by their status.
Unsolved Incidents	Displays the total number of unsolved (not closed) incidents by severity.
Incidents Timeline	Total incidents breakdown by category trend by day.

Events

一、12



The *Events* dashboard includes:

Outbreak Alerts

The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows FortiAnalyzer administrators to view outbreak alerts and automatically download related event handlers and reports from FortiGuard.

When FortiAnalyzer has a valid license for the Outbreak Detection Service, outbreak alerts from Fortinet are displayed in the *FortiSoC* > *Outbreak Alerts* pane. Outbreak alerts can be viewed from any ADOM. You can navigate between outbreak alerts by clicking on the corresponding tab at the top of the pane, and click the download icon to download a copy of the outbreak alert.

Outbreak event handlers and reports are created in real-time by Fortinet to detect and respond to emerging outbreaks. Outbreak reports and event handlers are automatically downloaded so that they are available in your environment. See Viewing imported event handlers and reports on page 212.

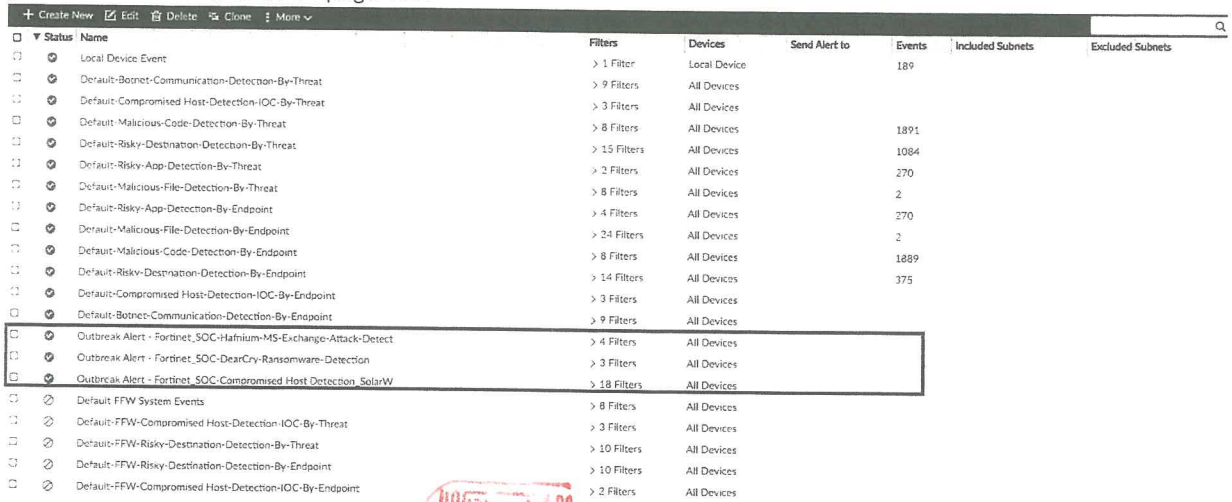
Without a valid license for the Outbreak Detection Service, *Outbreak Alerts* displays a default alert page, and outbreak event handlers and reports are not available from FortiGuard. To obtain a valid license for FortiAnalyzer Outbreak Detection Service, contact Fortinet FortiCare.

Viewing imported event handlers and reports

With a valid license, the FortiAnalyzer Outbreak Detection Service automatically downloads event handlers and reports created by Fortinet in response to known outbreaks. This section includes information on how to view downloaded outbreak event handlers and reports.

To view outbreak event handlers and reports:

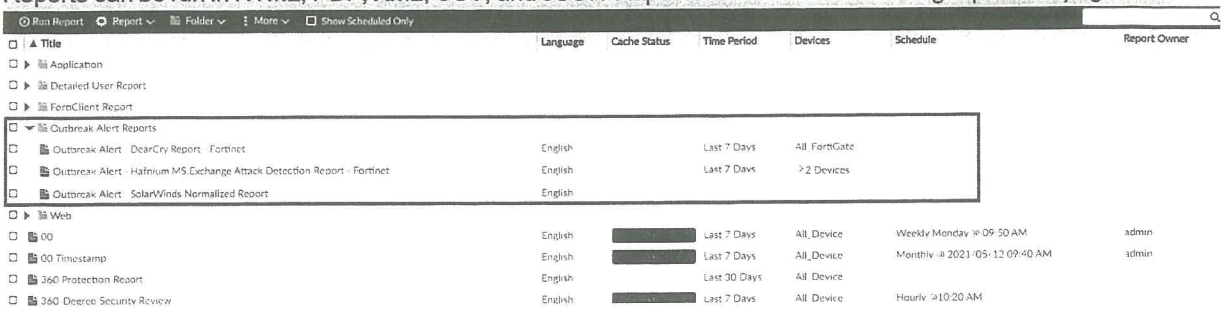
1. Go to *FortiSoC* > *Handlers* > *Event Handler List*.
   Event handlers created by the FortiAnalyzer Outbreak Detection Service are displayed with the Outbreak Alert prefix. See Event handlers on page 135.



2. Go to *Reports* > *All Reports*.
   The *Outbreak Alert Reports* folder includes available reports from the FortiAnalyzer Outbreak Detection Service.

一、7

Reports can be run in HTML, PDF, XML, CSV, and JSON output formats. See Generating reports on page 215.



Viewing a CRL

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *Result* page opens.
4. Click *OK* to return to the CRL list.

Deleting a CRL

To delete a CRL or CRLs:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL or CRLs you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

Log Forwarding

一、13

You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server when you use the default forwarding mode in log forwarding.

The *client* is the FortiAnalyzer unit that forwards logs to another device. The *server* is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs.

In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. See Log storage on page 33 for more information.

To see a graphical view of the log forwarding configuration, and to see details of the devices involved, go to *System Settings* > *Logging Topology*. For more information, see Logging Topology on page 285.

Modes

FortiAnalyzer supports two log forwarding modes: forwarding (default), and aggregation.

Forwarding

Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

This mode can be configured in both the GUI and CLI.

Force this administrator to change password upon next log on.	Force the administrator to change their password the next time that they log in to the FortiAnalyzer. This option is only available if *Password Policy* is enabled in *Admin Settings*. See Password policy on page 382.
FortiToken Cloud	Enable or disable two-factor authentication with FortiToken Cloud, then select the token delivery method from the following options: • *FortiToken Mobile*: Use the FortiToken Mobile app to get tokens. The administrator is sent an email with a link to activate their token in the FortiToken Mobile app on their mobile device. • *Email*: Receive the token by email. • *SMS*: Receive the token by SMS message. This option is not available if Admin Type is set to *PKI* or *SSO*. See Two-factor authentication on page 385.
Administrative Domain	Choose the ADOMs this administrator will be able to access. • *All ADOMs*: The administrator can access all the ADOMs. • *All ADOMs except specified ones*: The administrator cannot access the selected ADOMs. • *Specify*: The administrator can access the selected ADOMs. Specifying the ADOM shows the *Specify Device Group to Access* check box. Select the *Specify Device Group to Access* check box and select the Device Group this administrator is allowed to access. The newly created administrator will only be able to access the devices within the Device Group and sub-groups. If the *Admin Profile* is *Super_User*, then this setting is *All ADOMs*. This field is available only if ADOMs are enabled. See Administrative Domains (ADOMs) on page 296.
Admin Profile	Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features. See Administrator profiles on page 358.
JSON API Access	Select the permission for JSON API Access. Select *Read-Write*, *Read*, or None. The default is *None*.
Trusted Hosts	Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added. See Trusted hosts on page 349 for more information.
Theme Mode	Select *Use Global Theme* to apply a theme to all administrator accounts. Select *Use Own Theme* to allow administrators to select their own theme.
Meta Fields	Optionally, enter the new administrator's email address and phone number.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced options, see the *FortiAnalyzer CLI Reference*.

核准日期:民國49年6月1日
核准文號:教育部台(49)高第6598號

地址:台北市吳興街250號
No. 250, WuXing Street, Taipei 11031 Taiwan, R.O.C
統一編號Company Tax ID: 03724606

財團法人臺北醫學大學收款收據

日期 Date : 2024/12/06

Taipei Medical University Receipt

收據號碼 Receipt NO : AA11301632

繳款人姓名或單位名稱 Payer Name or Payer Department	泰瑩科技股份有限公司
身分證字號或統一編號 ID Card Number or Company Tax	28208184

收費項目 Charge Item	金額 Amount	收費項目 Charge Item	金額 Amount
存入保證金(履保.保固)	190,000		
以下空白			

總計金額 Total Amount	新臺幣 壹拾玖萬元整 (NTD$190,000)
用途說明 Instructions	防火牆日誌紀錄器

備註 Remark [票號]:KB2232932 [到期日]:2024/12/05

主辦人員 Handler : 出納組 113 12 06 許文嘉

主辦出納 Chief Cashier : 專用收辦章據出納主

主辦會計 Chief Accountant : 專用收辦章據會計主

1080801 136396

校長 President : 專用校長收據章 臺北醫學大學

*本收據若經塗改或無經辦人員章無效
Invalid if Altered or Altered Without Handler's Signature

收執聯

臺北醫學大學　功能驗收紀錄單

1091215 版

採購案號	1130203887	請購單位	網路通訊組		
請 購 人	陳暐傑	保 管 人	陳韋伸	Email	Jack355111@tmu.edu.tw
購案名稱	防火牆日誌紀錄器				
成交廠商	泰瑩科技股份有限公司			成交金額	1,900,000
到貨日期	113 年 12 月 13 日	履約有無逾期		□逾期	☑未逾期

● **功能測試：**

1. 本設備/軟體，安裝於 信義校區醫學綜合大樓前棟五樓網通組機房。
2. 本設備/軟體於 113 年 12 月 13 日起進行功能測試，至 113 年 12 月 13 日完成。

● **功能測試結果：**

☑標的物功能正常，安裝、規格、功能效益經測試與規範規定皆符合。

□標的物經測試後發現異常，狀況如下（請確實填寫）：

廠商於____年____月____日到校進行修復／更換，於____年____月____日____時____分完成，標的物異常狀況已排除／修復，全部測試於____年____月_____日完成。

● **教育訓練：**

1. □是，設備/軟體於__年_月__日起進行教育訓練，至__年__月__日完成。（人員訓練紀錄詳如附件）。
2. ☑否，設備/軟體不須進行教育訓練。

單位使用保管人（簽章及日期）：陳暐傑 12/13　　**分機：2626**

注意事項

1. **功能測試紀錄單請使用保管人功能測試填寫及簽章。**
2. **請購單位應於廠商到貨後二週內完成功能驗收，並通知保管組辦理會驗。若測試驗收不通過，本校得要求整批退貨重新交貨或解約。功能測試如需較長時間，應於訂約時述明或於驗收作業註明貴時較長原因。**
3. **10 萬元以上之儀器設備請購案，除本單之外，尚須加附詳細逐項測驗報告。**
4. **功能測試紀錄單於填寫完成後，請購單位使用保管人簽署後，上傳 ERP 系統之驗收文件(PDF 檔)，隨案結報。**

序號	採購品項				標的物安裝、規格、功能效益經測試與規範規定
	品名	規格及說明	數量	單位	
1	防火牆日誌紀錄器	FAZ-810G	2	台	☑相符□不相符
2					□相符□不相符
3					□相符□不相符

註:本表單所定格式僅供參考，單位得視實際需要自行調整及附相關人員簽署之詳細資料。

「防火牆日誌紀錄錄器」測試報告

測試日期：2024/12/13

廠商：泰瑩科技股份有限公司

驗收人(保管人)：陳韋伸 12/13

項目	測試項目	合格	不合格	備註
1	廠牌型號產地是否符合	✓		廠牌：FortiAnalyzer-810G 產地：美國
2	開關機是否正常	✓		
3	規格是否符合	✓		
4	數量是否符合	✓		2台

泰瑩科技股份有限公司

出　貨　單 第1/1頁

中華民國113 年 12 月 13 日

客戶名稱：	台北醫學大學	出貨號碼：	2211-20250102004
電　　話：	02-27361661*2629	訂單/報價單號碼：	TMU113-035W
聯 絡 人：	陳韋伸	業務人員：	陳妤嘉
送貨地址：			

項次	品名規格	數量	序號
1	防火牆日誌紀錄器 FAZ-810G	2	FAZ81GT224000116 FAZ81GT224000123

客戶簽章：陳曉傑 12/13　　領貨人：　　製單人：

地　址 ： 台北市南京東路四段130號四樓　　電　話：02-2578-1133

臺北醫學大學　財物及勞務類　驗收紀錄表

採購案號	1130203887	請購單位	資訊處
請購人	陳暐傑	保管人	陳韋伸
採購名稱	防火牆日誌紀錄器		
成交廠商	泰瑩科技股份有限公司	成交金額	NT$1,900,000
履約期限	113/12/13	履約有無逾期	☑未逾期　☐逾期
到貨日期	113/12/13	排驗日期	113/12/17

【驗收經過】

- 本案設備於113年12月13日到貨，113年12月13日完成功能驗收，113年12月17日辦理正式驗收。
- 抽驗防火牆日誌紀錄器1台，儲存容量16TB(含)以上、可匯集logging並集中管理、具報表功能可支援pdf、csv格式，與採購規格書相符，符合。

【驗收結果】

☑ 與契約、圖說、貨樣規定相符。

☐ 與契約、圖說、貨樣規定不符及其情形：

【備註】：

廠商	請購單位	保管組	事務組	財務處	總務長
12/17	12/17	113.12.17	12/17	113.12.17	113.12.17
（簽章及日期）	（簽章及日期）	（簽章及日期）	（簽章及日期）	（簽章及日期）	（簽章及日期）

註：用印完成資料請送回保管組

臺北醫學大學　財務/勞務 結算驗收證明

填發日期：113/12/19

案號及契約號	1130203887		廠商名稱	泰瑩科技股份有限公司	
標的名稱及數量 摘　　要	防火牆日誌紀錄器				
採購金額	□未達公告金額 ☑公告金額以上未達查核金額 □查核金額以上未達巨額 □巨額				
履約期限	113/12/13	履約地點	醫綜前棟RF1		
完成履約日期	113/12/13	開始驗收日期	113/12/13	驗收完畢/驗收合格日期	113/12/19
履約逾期總天數	0	不計違約金天數	0	應計違約金天數	0
逾期違約金	NT$0		其他違約金	NT$0	
契約金額	NT$1,900,000				

增減價款	次別 / 類別	第 1 次		第 2 次		合　計
		金　額	簽准日期或核准文號	金　額	簽准日期或核准文號	
	增加金額					
	減少金額					

驗收扣款		（不包括逾期違約金及其他違約金）
結算總價 （金額中文大寫）	新台幣	壹佰玖拾萬 元整
驗收意見	◦與契約規定相符，驗收合格。	

承辦單位主管及人員簽章	本機關監驗人員簽章	上級機關監驗人員簽章或授權自辦文號（未達查核金額者免）	主驗人員簽章	
簡郁芳	113.12.19			（機關印信）

說明：

一、本證明書已含有結算內容者，得免附具「結算明細表」，以資簡化；依實做數量或自行購料經工clear理者，應附具「結算明細表」。

二、本證明書份數請各機關自行依需要備具，例如由主辦機關自存、送主(會)計單位製作憑證之用、報上級機關備查、交廠商收執。

三、「驗收完畢/驗收合格日期」，指政府採購法第73條所定「驗收完畢」之日期，亦即參加驗收人員於驗收紀錄會同簽認廠商履約與契約、圖說、貨樣規定相符時之日期。惟其屬減價收受者，指依政府採購法第72條第2項報經上級機關核准(查核金額以上)或經機關首長或其授權人核准(未達查核金額)之日期。

四、「逾期違約金」及「其他違約金」以預算外或營業外收入處理，不必扣抵結算總價；「其他違約金」，指例如政府採購法施行細則第 98條第2項所定之減價收受懲罰性違約金。

五、「結算總價」之計算方式為「契約金額」加「增加金額」減「減少金額」減「驗收扣款」。至主辦機關供給材料及管理費或作業費等契約以外之各項支出均不必合併結算。

六、本證明書所定欄位如不夠使用，得新增其他欄位或增補續頁。

七、本證明書原則不得塗改，並應檢公文處理程序簽核後加蓋驗收機關印信；供機關自存者，得免加蓋機關印信。

泰瑩科技股份有限公司
TAI WIN TECHNOLOGY CORPORATION
Tel:886-2-25781133 Fax:886-2-25780334

保固書證明

致：臺北醫學大學

保固編號：2211-20250102004
契約編號：TMU113-035W
日期：113年12月23日

泰瑩科技股份有限公司保證以下產品均為原廠新品，並符合貴公司需求之規格，保固期間若發生任何因品質不良之損壞，本公司將轉送原廠維修或免費更換良品，但因下列原因導致損壞時，保證自動失效。

*一切人為因素造成之損壞
*不當之使用
*因意外造成之損壞
*不適當之重新安裝
*天災地變造成之損壞

項次	保固內容	數量
1	防火牆日誌紀錄器 FAZ-810G 保固期間：自113年12月24日起至114年12月23日止保固一年	2

泰瑩科技股份有限公司
負責人：賴銘德

中華民國 113 年 12 月 23 日

核准日期:民國49年6月1日
核准文號:教育部台(49)高第6598號

地址:台北市吳興街250號
No. 250. WuXing Street, Taipei 11031 Taiwan, R. O. C
統一編號Company Tax ID: 03724606

財團法人臺北醫學大學收款收據

收執聯

日期 Date : 2024/12/25

Taipei Medical University Receipt

收據號碼 Receipt NO : AA11301800

繳款人姓名或單位名稱 Payer Name or Payer Department	泰瑩科技股份有限公司
身分證字號或統一編號 ID Card Number or Company Tax	28208184

收費項目 Charge Item	金額 Amount	收費項目 Charge Item	金額 Amount
存入保證金(履保.保固)	57,000		
以下空白			

總計金額 Total Amount	新臺幣 伍萬柒仟元整 (NTD$57,000)
用途說明 Instructions	防火牆日誌紀錄器

備註 Remark [票號]:KB2232948 [到期日]:2024/12/24

主辦人員 Handler 出納組 113.12.25 許文嘉

主辦出納 Chief Cashier : 主辦出納專用收據章

主辦會計 Chief Accountant : 主辦會計專用收據章 1080801 136187

校長 President : 臺北醫學大學校長收據專用章

*本收據若經塗改或未蓋主辦人員章無效
Invalid if Altered or Altered Without Handler's Signature

113125624

臺北醫學大學付款憑單

會1

財務處承辦人:施千代

預算編號	113-3600-001-212		計畫編號(名稱)	113-3600-001-2124151B-(113)教補款(資本門)-資訊安全資本門設備		採購案號	113020388700	序號	
計畫期間	113/10/01~113/12/31								
請款單位	請款人	計畫主持人	單位主管	一級主管	會計審核	主辦會計	副校長	校長	
資訊處	李清萬 李清萬		李彥蓉	張正恆 113.12.25 張正恆	施千代 財務處 113.12.27 施千代	113.12.30 許淑群	依財務系統簽核權限辦理	依財務系統簽核權限辦理	

會計科目	用途及說明	金額
機械儀器及設備	防火牆日誌紀錄器	1,900,000
本款支付	泰瑩科技股份有限公司	1,900,000

學年度	會計編號	會計項目	沖預付款	摘要	傳票號碼	附件
113	113125624	134101	0		C1131227005、	原始憑證 0 件 簽呈 0 件 其他 0 件

支出憑證一式一份，正本憑證另冊保存

113/12/30付款

電子發票證明聯

2024 年 12 月 23 日

號碼：HF61953097

格　式：25

方：台北醫學大學

編號：03724606

址：

品名	數量	單價	金額	備註
體日誌紀錄器	2	904,762	1,809,524	契約編號:TMU113-035W
銷售額合計			1,809,524	營業人蓋統一發票專用章
兌 應稅 V 零稅率 免稅			90,476	賣　方：泰瑩科技股份有限公司
		計	1,900,000	統一編號：28208184
新臺幣 大寫)	壹佰玖拾萬元整			地　址： 台北市松山區南京東路四段130號

臺北醫學大學
分錄轉帳傳票

傳票日期：2024/12/27　　傳票編號：C11131227005

	會計項目	摘要	借方金額	貸方金額
1	134101 機械儀器及設備	防火牆日誌紀錄器	1,900,000	
2	212401 應付設備款	防火牆日誌紀錄器		1,900,000
Page 1 of 1		合計：	1,900,000	1,900,000

製票	施千代 2024/12/27	複核	林靜怡 2024/12/27	主辦會計	許淑群 2024/12/27	校長(或授權代簽人)	依核決權限授權決行

臺北醫學大學
分錄轉帳傳票明細表

傳票編號：C11131227005　　承辦人：施千代

傳票序號	會計項目/名稱		專帳/單位/摘要/備註	借方金額	貸方金額
	立沖帳	對象名稱	分錄備註		
1	134101 機械儀器及設備		113-3600-001-2124151B-(113)教補款(資本門)-資訊安全資本門設備 C0800資訊處 防火牆日誌紀錄器	1,900,000	
2	212401 應付設備款		C0800資訊處 防火牆日誌紀錄器		1,900,000
	立帳	泰瑩科技股份有限公司			
			合計：	1,900,000	1,900,000