114 年資訊安全報告

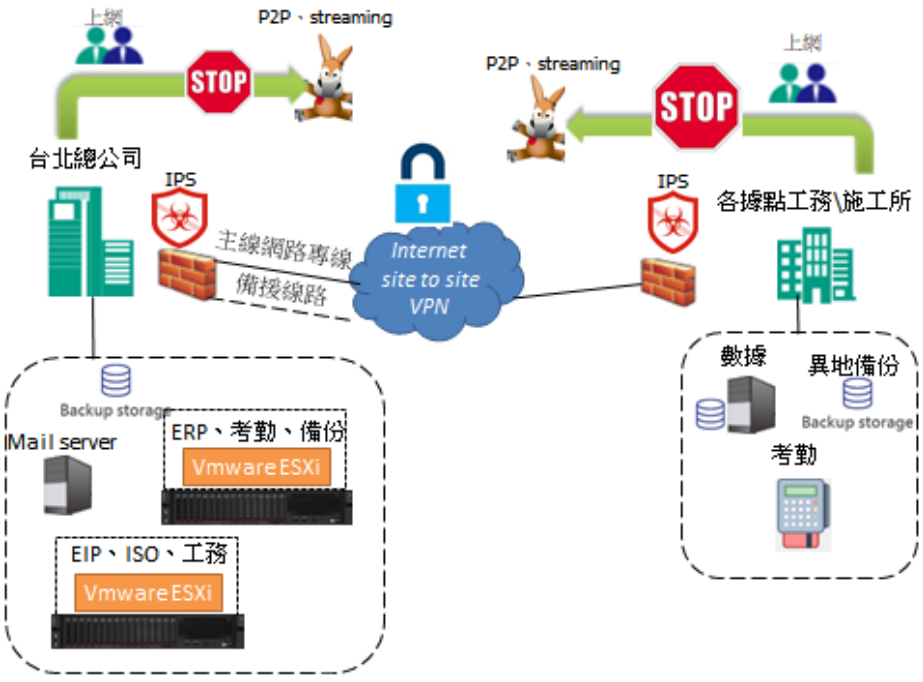
經檢視「資訊安全政策」尚符合公司之需求，得繼續沿用，本(114)年度資安政策與執行情形請參閱下方說明。

(一)資訊架構檢視

1. 網路架構與備援線路機制

本公司各據點的連線架構是採用 VPN 加密連線架構，

總公司主線路使用數據專線，並建立備援線路。



2. 網路存取管控

連線方向	服務	管控方式
外對內連線	網頁服務	IPS 入侵防禦監控與紀錄
內對外連線	上網	使用 UTM 進行應用程式管控與紀錄
	各據點連線	VPN 加密連線

3. 網路活動分析

各點防火牆設備使用 UTM 系統進行防護與紀錄，透過集中化安全記錄分析設備對內部電腦或設備進行流量、事件分析紀錄，並定期輸出分析報告。

Application Traffic

Top 30 Applications by Bandwidth and Sessions

#	Application	Bandwidth	Sent	Received	Sessions
1	Stream.Media		5.41 TB		111,515
2	SMB		4.43 TB		436,516
3	HTTPS		4.04 TB		13,209,513
4	tcp/873		1.39 TB		74
5	HTTPS.BROWSER		1.36 TB		10,334,369
6	443/udp		1.21 TB		2,787,317
7	QUIC		1.02 TB		2,488,258
8	YouTube		919.12 GB		256,867
9	HTTP		888.52 GB		3,568,386
10	Naver.Line		570.86 GB		1,097,698
11	Yahoo.Services		531.84 GB		2,011,591
12	HTTP.Video		525.27 GB		557,747
13	Facebook		372.75 GB		701,223
14	MS.Windows.Update		259.68 GB		638,458
15	SSL		235.76 GB		298,457
16	udp/443		233.95 GB		294,369
17	tcp/8888		173.38 GB		792
18	Google.Services		146.00 GB		1,248,220
19	HTTP.BROWSER		140.99 GB		6,269,821
20	183/tcp		76.96 GB		218

P2P	36.00%
Remote.Access	32.00%
Proxy	28.00%
Video/Audio	4.00%

Figure 1: Breakdown of High Risk Applications

High Risk Applications

Top 20 high risk applications are listed below. These applications have the risk rating of 5 (critical risk) or 4(high risk). Each application is listed with its respective category, technology, number of users, bandwidth and sessions.

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	5	Cloudflare.1.1.1.1.VPN	Proxy	Client-Server	30	75.18 MB	26,464
2	5	SurfEasy.VPN	Proxy	Client-Server	1	0 B	1,661
3	5	Proxy.HTTP	Proxy	Network-Protocol	18	1.40 MB	456
4	5	DNS.TXT.Records.Tunneling	Proxy	Client-Server	1	9.30 KB	19
5	5	Psiphon	Proxy	Client-Server	4	2.23 MB	12
6	5	OKHTTP.Library.VPN	Proxy	Client-Server	1	3.34 KB	1
7	5	Your.Freedom	Proxy	Client-Server	1	76 B	1
8	4	BitTorrent	P2P	Peer-to-Peer	5	23.72 MB	120,087
9	4	Chrome.Remote.Desktop	Remote.Access	Client-Server	6	171.62 MB	22,477
10	4	TeamViewer	Remote.Access	Client-Server	54	4.32 GB	14,044
11	4	VeryCD	P2P	Browser-Based	1	34.29 MB	10,922
12	4	QVOD	P2P	Peer-to-Peer	2	61.03 KB	10,200
13	4	PPStream	P2P	Peer-to-Peer	9	10.93 MB	4,798
14	4	AnyDesk	Remote.Access	Client-Server	19	518.06 MB	4,328
15	4	Thunder.Xunlei	P2P	Peer-to-Peer	2	4.44 MB	1,378
16	4	Baidu.Music	P2P	Peer-to-Peer	2	1.59 MB	466
17	4	TeamViewer_CallReceive	Remote.Access	Client-Server	35	113.74 MB	180
18	4	Telnet	Remote.Access	Client-Server	5	52.03 MB	131
19	4	TeamViewer_CallRequest	Remote.Access	Client-Server	3	25.68 MB	73
20	4	KKBOX	P2P	Peer-to-Peer	2	166.21 KB	47

Figure 2: High risk applications (rating of 4 or 5) that are traversing the network.

4.實體設備管理

電腦主機及其相關儲存與網路連結設備設置於專用機房，該機房設有空調系統並使用不斷電系統供應電力，以避免電壓不穩定或瞬間斷電造成損害。機房由資訊室負責管理，未經授權不可隨意進入。

(二)伺服器、用戶端設備檢測

營運設備	風險事件	已存在控制措施
EIP、ISO、工務、財會等服務伺服器	系統異常、服務中斷	系統虛擬化並建立還原機制
	資料損毀	採用硬碟與異地備份
	駭客入侵	建置防火牆，進行 IPS、網路行為管控、防毒軟體安裝
	系統漏洞	定期進行系統安全性更新
郵件主機	廣告、病毒、釣魚信件	多重垃圾信件掃描、流量清洗、IPS 入侵防禦、APT 攻擊防禦、BEC 滲透防禦
	系統漏洞	定期進行系統安全性更新
個人電腦	電腦中毒	安裝防毒軟體監視病毒事件及事件排除。
	系統漏洞	定期進行系統安全性更新

(三) 安全設定檢視

設備	**設定原則**
網路設備	密碼須符合複雜性並定期更新密碼
伺服器	
個人電腦	

(四)資安風險預防措施

- 系統與文件皆採取每日、每週及每月之本地備份且定期將備份與異地保存。
- 資訊系統架構依其風險等級將逐步建立高可用性之備援，以確保服務不中斷，以確保符合預期系統復原目標時間。
- 大多數的資安事件來自於內部員工的疏忽及欠缺資安意識，並定期強化員工資安觀念及社交工程演練。
- 定期檢測設備並更新未達現代資安要求之設備設施。

(五)資安教育訓練與資源投入

本公司重視資訊安全治理與員工資安意識之建立，於 114 年度持續推動資訊安全相關教育訓練及資源投入，強化全體同仁對資安風險之認知與防護能力。

在資安教育訓練與宣導方面，本年度共辦理及報告資訊安全相關會議計 5 次，就資安政策、風險防範、系統使用安全及資安事件應變等議題進行說明與宣導；並不定期透過公司 EIP 公佈欄及討論區發布資訊安全相關訊息與學習資料，提供同仁持續學習與即時掌握資安趨勢，藉以提升整體資安意識。

在資源投入方面，本公司於 114 年度投入資訊安全相關之設備、系統及資源經費合計新臺幣 3,791,957 元，以強化資訊系統之可用性、完整性與機密性。另在人力配置上，已設置資訊安全主管一名及資訊人員一名，專責辦理資訊安全政策規劃、系統維運、風險控管及資安事件應變等作業，確保資安管理制度之有效運作。

為因應營運發展及潛在資安風險，本公司並規劃於次一年度持續精進資安防護措施，重點包括：

1. 優化總公司辦公室網路架構，將無線網路與實體網路進行隔離，以提升網路效能並降低未授權存取之風險。
2. 建置各工地資料儲存設備之異地備援機制，強化資料保護及災害復原能力，以確保營運資料之安全與持續性。

透過持續之教育訓練推動與資安資源投入，本公司有效提升員工資安意識及整體防護水準，並落實資訊安全治理、風險管理與法令遵循要求，以降低資安事件對公司營運之影響。

工信工程股份有限公司

資訊安全政策

一、目的

為增進本公司資訊作業安全及穩定之運作，確保資訊資產之機密性、完整性及可用性，並順利推展本公司各項業務，以符合資通安全管理法及其子法之規範，特制定本公司資訊安全政策(以下簡稱本政策)做為本公司資訊安全管理最高指導方針。

二、範圍

本政策適用於本公司同仁、接觸本公司業務資訊或提供服務之廠商及第三方人員。

三、目標

(一)確保本公司業務相關資訊之機密性，保障個人資料。

(二)確保本公司業務相關資訊之完整性及可用性，提高行政效能與品質。

四、策略

(一)應考量相關法律規章及營運要求，評估資訊作業安全需求，建立相關程序，以確保資訊資產之機密性、完整性及可用性。

(二)建立本公司資訊安全組織(資訊室)，俾利推行資訊安全作業。

(三)建立資訊安全事件通報應變機制，以確保資安事件妥善回應、控制及處理。

(四)定期執行資通安全稽核作業，以確保資通安全管理落實執行。

五、審查

本政策由行政部經理及稽核室主任共同核定，每年至少評估一次，或於組織有重大變更時（如組織調整、業務重大異動等）重新評估。依評估結果、相關法令、技術及業務等最新發展現況，予以適當修訂。

資訊安全之管理與風險因應

管理項目	執行情形
明確規範資訊部門之功能與使用單位之職責劃分，透過資訊系統之協助，落實公司之計劃。	1. 公司部門組織設立資訊室，制定資訊室功能職掌表且確切執行。 2. 內控制度明訂資訊部門人員不得有使用應用系統權限從事資料之輸入與修正。而系統程式撰寫單位亦不得擔任系統安全管理員與應用系統使用者。
藉由專業人士之評估，確保公司電腦設備得以系統化及具效益性。	1. 每日檢測電腦運作並記載於系統機房工作日誌上。 2. 與協力廠商訂定軟、硬體系統維護合約。
確保公司電腦化作業之軟體符合企業及使用單位需求。	1. 重大資訊系統採購，經資訊室進行策略規劃並考量資訊系統所提供之功能，呈書面報告予總經理簽核。 2. 系統開發前系統使用者應告知使用需求，並於維護合約書中記錄需求內容。
確保公司軟硬體之書面操作資料適當保存與管理，需要參考時即可獲得。	1. 系統文件由資訊室負責保管，並建立「電腦文件列管清冊」及「電腦軟體列管清冊」。 2. 軟體程式更改或新購時，其相關之電腦文書皆同時予以更新。
規範各使用者對系統程式及資料存取之權限及範圍，確保程式及資料之存取安全。	1. 內控制度明訂資訊部門人員不得有使用應用系統權限從事資料之輸入與修正。而系統程式撰寫單位亦不得擔任系統安全管理員與應用系統使用者。 2. 系統程式、財會薪資兩大應用程式皆有「權限設定」之控制。一般應用系統使用者並無權限存取主機重要之系統公用程式、工具及指令(只有系統管理員有此權限)。 3. 使用者名稱(帳號)之新增、修改、刪除均以「電腦用戶申請單」經適當核准，由系統管理員執行。 4. 系統管理員可檢視「電腦用戶申請單」或系統工具之「使用者管理員」檢視帳戶實用性以確定每位使用者皆有個別之使用帳戶及密碼，並可檢查

	其定期更換密碼週期及最少字元要求。 5. 系統管理員每日檢視日誌檔紀錄事項，遇系統軟體發生故障、初次載入系統軟體及應用軟體、重新開機及復原、緊急狀況和任何不尋常狀況時，應登錄於「系統機房工作日誌」，並呈報主管核示。 6. 已建置防毒軟體於 SERVER 上，個人電腦一開機連上區域網路，主機自動進行防毒軟體更新及病毒偵測。
確保資料檔案及各項電腦設備之安全。	制訂備份排程，定期由專人備份重要之系統檔案、程式及資料檔案，每月將所有主機作一次完整備份，依據「備份檔案管理原則」記錄於「備份檔案儲存登記簿」。
避免電腦危機造成公司業務的衝擊。	1. 備份資料統一由資訊室集中送公司第三地留存保管，配合系統復原計劃作回存測試。 2. 備份資料存於獨立之第三地。 3. 系統伺服器置於獨立之機房，上鎖予以保護，並製作「系統機房工作日誌」以進行門禁管制及非經授權人員進、出管制。 4. 電腦主機連接不斷電系統並設置消防設備，裝置溫、濕度監測器。 5. 主機及工作站皆裝有防毒軟體，定期偵測病毒並有資訊廠商提供定期偵測病毒軟體。
確保資通安全檢查控制處理之正確性。	1. 資訊室對網路作業系統隨時清查並及時作系統漏洞修補；且全面清查使用之電腦(含伺服器、個人電腦)均安裝防毒軟體，除定期作病毒掃描並定期更新病毒碼。 2. 本公司對外開放資訊系統，重要資料及軟體均定期作備份且定期回復測試，以確定其可用性並存於第三地。 3. 隨時檢查網路系統、伺服器、網路芳鄰、交換器等，使用者權限均依照「程式及資料存取控制作業」規定辦理。

配合電子化政府之政策與資訊充分揭露之原則，冀期公司各項公開資訊得以完整、快速地透過網際網路提供給投資人。	1. 使用者權限均依其業務範圍、權責分別設定使用者之帳號及密碼，並經適當核准，由系統管理員執行；且使用者一旦離開原職務，即立即撤銷該使用者之帳號及權限。 2. 應申報之公開資訊、重大訊息等項目，均依相關法令辦理，並於規定時限內申報完成。 3. 上傳申報之各項資料，承辦人員均確認上傳成功且經證期局所接受。