**111年度改善升級物流業物聯網資訊安全計畫**

**「國際物流業資訊安全現況調查」**

填表人姓名： 填表日期： 年 月 日

**一、廠商基本資料：**

1. 公司名稱：
2. 資本額： 萬元 營業額(110年)： 萬元
3. 公司地址：
4. 負責人： TEL： E-mail：
5. 聯絡人： 職稱： TEL：

E-mail：

1. 員工人數：共 人，資訊人員(含資安人員) 人，資安專職人員 人
2. 以何種方式管理資訊安全相關事宜：🞎正職資安人員 🞎資安約聘及約僱人員 🞎資安委外或其他人力(含職代) 🞎其他\_\_\_\_\_\_\_\_\_
3. 行業別(可複選)：🞎海運承攬運送業 🞎航空貨運承攬業 🞎貨櫃集散站經營業

🞎航空貨物集散站經營業 🞎報關業 🞎倉儲業 🞎汽車貨櫃貨運業 🞎自由貿易港區事業 🞎其他(主要服務類別： )

1. 已取得之資格認證/相關許可： 🞎AEO 🞎自由貿易港區事業營運許可 🞎IATA 🞎WCO 🞎ISO 9001 🞎ISO 9002 🞎ISO 27001 🞎CNS 27001

🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_

**二、資安管理：**

1. 請問公司是否已導入及通過CNS 27001或ISO 27001第三方驗證，並持續維持其驗證有效情形?

🞎是，符合系統包含：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (如:報關系統…)

🞎否

1. 請問公司無法導入及通過CNS 27001或ISO 27001第三方驗證之原因? (可複選，已導入及通過者可免填)

🞎尚未導入但已規劃辦理

🞎自行評估無需要導入

🞎經費不足

🞎軟硬體規格等級不足

🞎人力不足

🞎內部人員能力不足

🞎委外廠商能力不足

🞎其他業務單位反彈

🞎不受長官重視

🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 請問公司是否鼓勵員工參與資訊安全教育訓練，以提昇資訊安全認知?

🞎是，訓練內容：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

🞎否

1. 請問公司111年編列採購資安產品(含服務)預算經費(千元)?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. 請問公司目前是否已採購或預計將新增採購下列哪些資安產品(含服務)，及其廠牌規格?

| **內容** | | **已採購資安產品**  **(含服務)** | **111年新增採購的資安產品(含服務)** |
| --- | --- | --- | --- |
| (1) | **防毒**:由軟體或硬體來實作，用於偵測入侵電腦的病毒、蠕蟲、木馬與惡意程式，通常含有即時程序監控識別、惡意程式掃描與清除及自動更新病毒資料庫等功能。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (2) | **防火牆**：由軟體或硬體來實作，利用系統所建立的網路/應用程式安全性規則，有效的控制對內與對外的安全存取機制。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (3) | **郵件過濾裝置**：過濾垃圾郵件以達到資訊安全防護的裝置。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (4) | **入侵偵測/入侵防禦系統 (IDS/IPS)**  入侵偵測系統(IDS)：可以偵測外部及內部人員對未經授權之資訊系統做不正當的存取或攻擊，可提供紀錄以供審核及事後追蹤。  入侵防禦系統(IPS)：為入侵偵測系統的延伸，除了偵測外也能發揮主動防禦的功能，如刪除垃圾封包、擋掉入侵IP等等。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (5) | **網站應用程式防火牆(WEF)**：針對網站的常見攻擊進行防禦，諸如跨網站攻擊(cross-site scripting)以及SQL injection攻擊。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (6) | **進階持續性滲透攻擊(APT)防禦**：針對特定組織所作的複雜且多方位的網路攻擊防護。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (7) | **資料外洩防護(DLP)**：透過內容比對偵測技術，以管控資料的外洩防護。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (8) | **數位版權管理(DRM)**：用來保護數位內容使用的管理機制，透過加密認證等過程，確認是合法使用數位內容之使用者，可在文件上加浮水印、限制使用時間、使用載具限制、取得授權等方式來保護數位內容。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (9) | **日誌管理(Log Management)**：蒐集及分析資訊系統或設備在連線和運作時所產生的紀錄，讓IT人員能夠監控系統的運作狀態，了解資料存取行為和使用者的作業活動，以及是否有異常情況發生等項。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (10) | **資料庫監控(DAM)**：記錄所有資料庫的存取軌跡，以監控與稽核資料庫活動。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (11) | **行動裝置與應用管理(MDM/MAM)**：針對行動裝置，如手機、平板進行裝置功能的控管，或是資料儲存管理。前者例如鎖定照相功能、限定可安裝的應用程式，後者如電子郵件管理、聯絡人資訊、或是可存取的文件等。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (12) | **資安健診服務**：透過整合各項資通安全項目的檢視服務作業，提供受檢機關資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資訊系統安全防護能力。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (13) | **資安監控中心(SOC)**：由資安人員、管控系統平台、管控程序，三者加以整合而成。其中的系統平台即為資安事件管理平台，通常具備事件偵測、事件收集、知識庫、事件分析、回應與通報等基本功能。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (14) | **弱點掃瞄服務**：檢測系統潛在弱點，並依據檢測結果提出改善建議，協助受測目標提升系統安全防護。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (15) | **滲透測試服務**：IT人員透過模擬駭客的攻擊方式，進行滲透或穿透跳躍主機之入侵測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之情況。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (16) | **社交工程郵件測試服務**：模擬駭客寄送社交工程信件給受測對象，以信件之標題及內容引誘收件人「開啟信件」、「點閱連結」或「開啟附件」進而下載惡意程式的攻擊行為，進而統計分析。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (17) | **資安鑑識服務**：遭遇資安事件的後續處理，進行證據的收集與追蹤分析。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (18) | **行動化應用軟體資安檢測服務**：為了防範Mobile Application或Mobile App 被駭，所執行之安全檢測作業。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (19) | **物聯網(IoT)裝置安全威脅偵測：**採用非侵入式的監測分析設備之間的關聯性與日常正常行為，為每個類型IoT設備建立行為模型，並提供IoT裝置即時可見性和威脅偵測。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (20) | **物聯網(IoT)與營運科技(OT)安全與洞察解決方案：**針對IoT裝置網路OT架構能見度、提供關鍵基礎設施的威脅偵測和洞察解決方案，快速檢測關鍵狀態以確保IoT裝置網路安全性和可靠性。 | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | □是 □否  廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (21) | 其他：請加以論述 | 廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 廠牌規格：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**三、資安事件：**

請問過去曾遭遇哪些資安事件的威脅? (複選)

| **資安事件** | | **發生來源** | **造成損失** | **復原時間** | **復原方式** |
| --- | --- | --- | --- | --- | --- |
| (1) | 惡意程式  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (2) | 釣魚攻擊  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (3) | 勒索軟體  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (4) | 垃圾郵件  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (5) | 商業電子郵件詐騙  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (6) | 系統老舊所產生的資安事件  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (7) | 過時的資安控管與架構所產生的漏洞攻擊  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (8) | 使用未具防護之電子裝置所產生的資安事件  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (9) | 使用雲端服務所產生的資安事件  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (10) | 未即時軟體更新所產生的資安事件  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (11) | 密碼共用且無其他認證機制所產生的資安事件  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (12) | 缺乏資安意識所造成的資料外洩  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (13) | 資料庫遭受入侵  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (14) | 未經授權的存取  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (15) | 零時差攻擊(零日攻擊)  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (16) | 其他：請加以論述  □有  □無 | 🞎外部攻擊(駭客)  🞎內部人員疏失  🞎離職人員或內部犯罪  🞎委外/IT供應商  🞎外國國家級攻擊  🞎上下游供應鏈合作夥伴  🞎競爭對手  🞎顧客  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎沒有損失  🞎業務中斷  🞎個資或資料外洩  🞎財務損失，損失金額(千元)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_  🞎信譽損失  🞎智慧財產權的損失  🞎無法估計  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎1小時內  🞎1天內  🞎1周內  🞎2周內  🞎1個月內  🞎半年內  🞎不知道  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 🞎還原系統  🞎重新安裝系統  🞎安裝修補程式  🞎其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**111年度改善升級物流業物聯網資訊安全計畫**

**「國際物流資安問題分析與技術評估檢視表」**

　　　　　　　　　　　　　　　　　　　　　　　　　　　版本：ITRI 1.2

|  |  |
| --- | --- |
| **公司名稱：** |  |
| **填表人：** |  |
| **填表日期：** | 民國 　年 月 日 |
| **檢核項目：** | 一、技術類別  二、設備類別  三、作業類別  四、公司政策類別  五、人員類別 |

| **編號** | **檢核結果** | | **檢視項目** | **備註**  **NIST Compliance** |
| --- | --- | --- | --- | --- |
| **YES** | **NO** |
| **一、技術類別** | | | | |
|  |  |  | 是否安裝防毒軟體。 | NIST SP 800-26 11.1 |
|  |  |  | 是否定期更新防毒軟體病毒碼。 | NIST SP 800-26 11.1.1 |
|  |  |  | 是否安裝防火牆系統。 | NIST SP 800-26 16.2.10 |
|  |  |  | 是否建立電子郵件過濾機制。 | NIST SP 800-26 16.2.10 |
|  |  |  | 是否建立電子郵件內容防護安全檢查。 | NIST SP 800-26 16.2.1 |
|  |  |  | 是否定期執行資訊系統弱點掃描測試。 | NIST SP 800-26 1.1.6 |
|  |  |  | 是否建立網路瀏覽內容防護安全檢查。 | NIST SP 800-26 16.3.1 |
|  |  |  | 是否定期執行防火牆設定檢視。 | NIST SP 800-26 16.2.11 |
|  |  |  | 是否安裝惡意程式偵測系統。 | NIST SP 800-26 11.2.5 |
|  |  |  | 是否定期執行資訊系統滲透測試。 | NIST SP 800-26 11.2.8 |
|  |  |  | 是否定期執行網路架構安全性檢視。 | NIST SP 800-26 16.2 |
|  |  |  | 是否定期檢測網路運作環境之安全漏洞。 | NIST SP 800-26 16.2 |
|  |  |  | 遠端系統管理是否僅開放特定網路地址。 | NIST SP 800-26 16.2.4 |
|  |  |  | 是否依據使用需求開放不同的目錄存取權限。 | NIST SP 800-26 15.2/16.1/16.1.2 |
|  |  |  | 帳號目錄系統是否有日誌紀錄保存。 | NIST SP 800-26 17.1 |
|  |  |  | 是否安裝網路入侵偵測系統(IDS)。 | NIST SP 800-26 2.1.4/11.2.5 |
|  |  |  | 是否定期更新入侵偵測系統(IDS)之特徵資料庫。 | NIST SP 800-26 11.2.5 NIST SP 800-26 11.2.6 |
|  |  |  | 是否安裝網路入侵防禦系統(IPS)。 | NIST SP 800-26 11.2.7 |
|  |  |  | 是否定期更新入侵防禦系統(IPS)之特徵資料庫。 | NIST SP 800-26 11.2.7 |
|  |  |  | 自行開發之系統是否執行原始碼安全檢測。  (如未開發可免填；本公司使用\_\_\_\_\_\_\_\_\_\_\_\_產品) | ─ |
|  |  |  | 資訊系統監控工具是否可識別異常的資訊系統存取活動。 | NIST SP 800-26 16.1.10 |
|  |  |  | 資訊系統監控工具是否可識別未經授權的資訊系統存取活動。 | NIST SP 800-26 16.1.1/16.1.2/16.2.4/16.2.7 |
|  |  |  | 資訊系統監控工具是否設置外界與內部網路之資料傳輸及資源存取控管。 | NIST SP 800-26 7.2 / 7.2.2 |
|  |  |  | 資訊系統監控工具是否設置重要伺服器與內部網路之資料傳輸及資源存取控管。 | NIST SP 800-26 16.2 |
|  |  |  | 資訊系統監控工具是否具有即時事件記錄的功能。 | NIST SP 800-26 16.2.5 |
|  |  |  | 自動監測工具是否具有警示的功能。 | ─ |
|  |  |  | 是否定期檢查開放存取之目錄有無存在異常程式。 | NIST SP 800-26 17.1 |
| **二、設備類別** | | | | |
|  |  |  | 是否建立資訊設備清冊。 | NIST SP 800-26 12.1 |
|  |  |  | 是否定期盤點資訊設備。 | NIST SP 800-26 2.1.1 |
|  |  |  | 各網域電腦主機與個人電腦設備在接入網路前是否移除預設帳號及密碼。 | NIST SP 800-26 16.2.3 |
|  |  |  | 各網域是否移除非必要之所有帳號。 | NIST SP 800-26 16.1.5 |
|  |  |  | 是否定期檢討資訊設備的安全防護機制。 | NIST SP 800-26 12.2.1 |
|  |  |  | 機房及重要區域是否建立人員進出管控管理措施。 | NIST SP 800-26 7.1.11 |
|  |  |  | 可攜式行動裝置(例如: USB、筆記型電腦) 若連接至內部裝置與資訊系統時，是否已通過病毒測試。 | NIST SP 800-26 7.3/16.2.11 |
|  |  |  | 各網域電腦主機與個人電腦設備配置是否定期檢測。 | NIST SP 800-26 16.2.4 |
|  |  |  | 無線網路服務是否有對訪客設置安全防護機制。 | NIST SP 800-26 16.2.12 |
|  |  |  | 可攜式行動裝置(例如: USB、筆記型電腦) 若連接至內部裝置與資訊系統時，是否已經過授權使用。 | NIST SP 800-26 7.3/16.2.4/16.2.11 |
| **三、作業類別** | | | | |
|  |  |  | 是否建立並遵循使用者密碼管理之作業規定。 | NIST SP 800-26 11.2.3/15.1 |
|  |  |  | 是否對機敏性資訊(如:帳號與密碼)訂定權限管理機制。 | NIST SP 800-26 17.1.5 |
|  |  |  | 是否建立電子郵件申請帳號及使用方法安全管理作業之規定。 | **—** |
|  |  |  | 是否建立電子郵件密碼長度設定之管理規定。 | NIST SP 800-26 11.2.3 |
|  |  |  | 是否定期執行電子郵件安全檢查作業。 | **—** |
|  |  |  | 是否訂定資料備份程序。 | NIST SP 800-26 9.1/9.1.1/9.2/9.3 |
|  |  |  | 是否將儲存於資料庫之機敏性資訊(如:帳號與密碼)以編碼或加密方式處理。 | NIST SP 800-26 16.2.15 |
|  |  |  | 機敏性資訊傳輸過程是否採取資訊加密保護措施。 | NIST SP 800-26 16.2.14 |
|  |  |  | 聯盟或供應鏈成員間資訊交換是否採取資訊加密保護措施。 | NIST SP 800-26 11.2 |
|  |  |  | 是否定期修補資料庫系統漏洞。 | NIST SP 800-26 11.2.5/11.2.6 |
|  |  |  | 是否定期修補軟體漏洞。 | NIST SP 800-26 11.2.8 |
|  |  |  | 是否訂定資料還原程序。 | NIST SP 800-26 9.2.3 |
|  |  |  | 是否定期備份作業系統及紀錄檔案。 | NIST SP 800-26 9.1/9.2/9.3 |
|  |  |  | 聯盟或供應鏈成員間重要機敏資料傳遞是否有軌跡紀錄。 | NIST SP 800-26 16.2.5 |
|  |  |  | 是否建立並遵循媒體及可攜式儲存媒體使用安全管理作業規定。 | NIST SP 800-26 7.3 |
| **四、公司政策類別** | | | | |
|  |  |  | 是否對核心系統制定業務持續運作計畫。 | NIST SP 800-26 9.1 |
|  |  |  | 是否對核心系統定期辦理業務持續運作演練。 | NIST SP 800-26 9.3 |
|  |  |  | 員工和委外廠商在被允許存取資訊前是否有簽署機密性或保密協議。 | NIST SP 800-26 6.2.2/6.2.3 |
|  |  |  | 是否訂定「資訊安全政策」之管理程序文件及管制措施。 | NIST SP 800-26 1.1 |
|  |  |  | 是否定期審查檢討「資訊安全政策」之管理程序文件及管制措施。 | NIST SP 800-26 1.1.1/1.1.2 |
|  |  |  | 是否訂定「資料保護管理」之管理程序文件及管制措施。 | NIST SP 800-26 1.1.3 |
|  |  |  | 是否定期審查檢討「資料保護管理」之管理程序文件及管制措施。 | NIST SP 800-26 1.1.3 |
|  |  |  | 對於系統侵犯者之違規行為，是否訂有適當懲處規定。 | NIST SP 800-26 11.2.6 |
|  |  |  | 是否審查委外廠商，以確保網路安全符合要求。 | NIST SP 800-26 7.1.11 |
| **五、人員類別** | | | | |
|  |  |  | 是否加強開啟郵件、點閱郵件附件或連結等員工之資安意識教育訓練。 | NIST SP 800-26 13.1.5 |
|  |  |  | 是否加強會計同仁收到詐騙電子郵件資安意識教育訓練。 | NIST SP 800-26 13.1.5 |
|  |  |  | 是否指定專人或專責單位負責資訊安全政策、計畫與管理之工作事項。 | NIST SP 800-26 13.1 |
|  |  |  | 是否每年對員工施予教育訓練並作成紀錄。 | NIST SP 800-26 13.1.3 |
|  |  |  | 是否指定核心人員負責資訊技術系統和操作技術系統的日常維護和網路攻擊的偵測。 | NIST SP 800-26 14.1.4 |
|  |  |  | 是否要求資訊同仁對遠距工作落實執行加密連線到公司的系統。 | NIST SP 800-26 16.2.4 |
|  |  |  | 是否適當培訓核心人員，確保核心人員瞭解網路安全措施方面的責任，包含：及時回應、及時上報的責任。 | NIST SP 800-26 14.1.5 |
|  |  |  | 是否要求資訊同仁安全管控USB。 | **—** |
|  |  |  | 是否建立資訊安全管理小組，當事故發生時能啟動緊急應變。 | NIST SP 800-26 14.1 |
|  |  |  | 對於人員職務調整及調動是否限期調整其系統存取權限。 | NIST SP 800-26 15.2.2 |