**資訊安全要求**

附件12

為建立資安防護機制，引導產業建立資安防護認知與制度，以保障我國製造業重要生產資訊，並提升製造業資安防護能量，本計畫資訊安全要求如下。

1. **共同規範：**
2. **施作項目**
3. 提案時應提出資安規劃地圖，包含功能、線路配置、產品規格等。
4. 資訊安全規劃，可包含內部系統資安防護(ERP、MES、CRM等)、網站服務資安、密碼安全性、應用程式資安(E-mail等)、連線系統資安、連網設備的資安防護(製造、檢測、控制器、邊緣運算等)。
5. 資安產品功能包含防毒軟體、防火牆、弱點掃描、資料傳輸加密、AI防毒監控、資安認驗證、資安情報、資安訓練、原始碼加密混淆器、伺服器安全監控等。
6. 物聯網相關產品如已有國家資安相關檢測標準，須採用通過資安驗證之產品。
7. 提案廠商應由高階管理階層指派具決策主管人員負責協調資訊安全專案之計畫執行及資源配置。
8. 資訊軟硬體不等同資安軟硬體，下列產品不可列入：虛擬主機、伺服器、雲端服務、路由器等資訊類產品。若資訊產品內含資安功能，可以從其功能百分比，依比例核列。
9. **注意事項**
10. 補助計畫簽約時，應提供與資安業者簽訂之「合作意願書」或「合約」等佐證資料。
11. 驗收時應提供支付資安廠商之給付證明、說明於該案中所提供之產品及服務、解決哪些資安需求等。
12. 資安業者不應有過度再外包的情形(不得超過資安經費的50%)。
13. 使用的資安軟、軔、硬體產品，不得為中國大陸生產或開發。
14. 計畫內資安軟、軔、硬體產品，非國內(台製)之資安產品佔比不得超過資安經費的50%；若有特殊情形，須於計畫書、審查會中明文說明。
15. 列入資安人力核銷項目，相關員工必須具備以下至少一項(1)取得資安證照、(2)碩博士論文與資安相關、(3)曾在資安專業公司/機構從事資安相關工程、服務等滿一年、(4)其他可資舉證之資安專業服務。(註：資安專業不同於資訊專業。)

**先期顧問規劃案：**

　　須盤點提案廠商與供應鏈間之資訊安全之現況，包含網路、應用及設備層的軟硬體，並進行問題分析與提出最佳調整方案之建議，需含教育訓練、機制建立、系統導入、導入後查驗、資安架構圖等規劃。

**系統建置導入案：**

須盤點提案廠商與供應鏈間之資訊安全之現況，包含網路、應用及設備層的軟硬體，並進行問題分析與提出最佳調整方案之建議，需含教育訓練、機制建立、軟硬體系統採購、系統導入、導入後查驗、資安架構圖，且建置及導入35%以上應為國內業者產品及服務，計畫驗收至少須達**二、必要要求**之條件。

並另敘明：

* 資訊安全組織：請指派公司之專責人員負責資訊安全計畫、執行、查核及改善，並由管理階層指派高階人員負責協調專案資源。
* 資訊安全計畫：請規劃資訊安全風險評估，可透過但不限於第三方單位執行原始碼檢測、黑箱檢測、滲透測試等，並針對重大威脅及脆弱性必須規劃資安防護解決方案。

1. **必要要求**
2. **企業網路層之安全要求**
3. 企業網路層、監控層及管理層之間，以及各層對外網路，採用資安防護設備，強化網路管控。

　　各層之間與各層對外網路應使用資安防護設備，包含但不限於IPS、VPN、URL Filter及APT偵測等。

1. 針對USB裝置進行管理與惡意程式掃描。
2. 各層對外網路應使用資安防護設備，功能包含但不限於IPS、VPN、URL Filter及APT偵測等。USB裝置除了不應提供自動執行功能外，設備開機時亦不可由USB裝置啟動。
3. 未經單位允許之USB設備及存放於該設備之程式與資料不應被啟動，且需定期針對設備進行惡意程式掃描。
4. 具備日誌與稽核機制，且須存查至少N+0.5年。

　　須具備事件記錄功能，確實記錄系統運作行為，得以提供發生異常時之事件檢視、查核未授權或異常的操作。其內容須包含完整時間戳記、使用者身份及操作行為等，且須至少保存N+0.5年之紀錄供後續查閱之用。

1. 各網路、系統、設備於上線前，須經弱點掃描確認，不可存在高風險等級之安全弱點。
2. 行動應用App須符合「行動應用App基本資安規範」之安全要求，並經合格實驗室測試通過。
3. 影像監控系統須符合「影像監控系統資安標準」之安全要求，並經合格實驗室測試通過。
4. **監控與管理層資訊安全要求**
5. 各個主機安裝資訊安全防護軟體。

各個主機應安裝資訊安全防護軟體，包含但不限於防毒軟體與惡意程式防護軟體。

1. 採用白名單管控方式如下：
2. 建立作業系統控管執行程式白名單
3. 建立連線控管白名單
4. 具備日誌與稽核機制，且存查至少N+0.5年。

　　須具備事件記錄功能，確實記錄系統運作行為，得以提供發生異常時之事件檢視、查核未授權或異常的操作。其內容須包含完整時間戳記、使用者身份及操作行為等，且須至少保存N+0.5年之紀錄供後續查閱之用。

1. 建立安全的軟/韌體與組態更新機制。
2. 更新方式
3. 離線手動更新

更新檔須加密保護以確保機密，且須採用FIPS 140-2 Annex A所核可之加密演算法，抑或是須於產品之身份鑑別因子、加解密用之金鑰(不含非對稱加解密用之公鑰)及敏感性資料，不應出現於軟/韌體之程式碼與安裝檔內其它檔案中。

1. 線上更新

須驗證下載來源，且其更新路徑須通過安全通道，且安全通道須使用SSL/TLS，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)。

1. 更新前必須驗證軟/韌體之正確性及完整性的功能。
2. 支援備援更新功能，即發生更新失敗時，系統能回復正常運作。
3. **控制層資訊安全要求**

建立軟/韌體與組態更新機制。

1. **實體層資訊安全要求**
2. 遵循國際通用規範或原廠規格的通訊協定存取資料。

自行發展之通訊協定與實作恐造成後續維護之困難性，稽核人員將查核受稽單位選擇之理由及日後維護之能力，並確認相關設計資料之保存機制。

1. **備份機制要求**
2. 程式碼與設定檔須定期備份。
3. 開發過程應遵循安全開發流程。
4. 根據資安政策制定備份流程與週期。
5. 資料分級後，重要資料定期備份。
6. 依據資料用途進行風險評估，並設定風險等級。
7. 風險等級高之重要資料，應依據資安政策定期進行備份。
8. **加解密認證安全建議**
9. 若使用密碼管理，須有以下機制：

* 更改初始密碼
* 要求密碼強度
* 密碼失效鎖定機制
* 密碼加密保存
* 密碼定期更改

1. 以密碼進行身分鑑別已被認定為不安全之作法，宜避免繼續使用密碼鑑別。若情非得已，應述明理由，且規劃長期汰換計畫，短期應另有控制措施，以避免密碼遭竊外洩，造成身分鑑別功能喪失之風險。
2. **中階要求(非必要項目，由提案廠商視需要導入)**
3. **企業網路層之安全要求**
4. 在企業網路層安全防護架構或措施，參考如下：

* IPS (介於IT與OT環境)
* Secure Tunnel VPN (介於IT與OT環境)
* 裝置網路能見度管理 (介於IT與OT環境)
* IP白名單 (介於IT與OT環境)
* 惡意程式掃描
* 垃圾郵件掃描
* URL過濾
* APT偵測
* 重要的資料視設備之環境及安全要求等級決定各種資料加密演算法強度及金鑰儲存方式
* 針對外部伺服器請採用Webtrust SSL憑證
* 伺服器端受資安防護設備保護
* 系統特權帳號管理，特權帳號僅授予執行業務及職務所必要為限
* 系統特權帳號存取，系統均留有完整紀錄
* 提供自動異常偵測機制，發送告警通知，並產出稽核報表
* 智慧手機具有足夠的演算能力，登入採用雙因子認證機制

1. 企業網路層與其他廠區之網路連線，參考如下：

* 資料傳輸建立安全的加密通道
* 遠端連線應透過加密通道，登入系統採用安全的身分鑑別機制
* 避免使用專屬網路協定，若有其必要且不可取代性，請另行表述
* 僅開放網路連線必要之服務與連接埠，其餘皆關閉

1. **監控與管理層資訊安全要求**
2. 建立校時機制。
3. 須建置NTP伺服器，維持設備時間一致性與系統日誌時間正確性，以確保鐘訊同步。
4. 建立防毒軟體版本及病毒碼更新機制。

　　防毒軟體與病毒碼更新機制應包含版本檢查更新、確認更新來源、安裝更新、移除已安裝更新及更新失敗回復，共5個流程。

1. 採標準的安全加解密機制。

　　加解密機制應採用尚未被破解且已具強固加密等級之加密技術，可參考FIPS 140-2 Annex A所核可之加密演算法。

1. 建作之機制立當監控管理設備遺失或脫管時，可立即阻斷與防止再操作。
2. 建立信任監控管理裝置列表與雙重認證註冊機制，以白名單方式進行設備存取管控。
3. 設置各別裝置可存取位址來源之管制措施。
4. 設備註冊後預建議載入代理軟體(Agent)，可透過遠端派送命令或更新至受管制設備，使其可鎖定、註銷及移除相關監控內容與功能。
5. **實體層資訊安全要求**
6. 若透過外加模組方式存取資料，請提供所採用的通訊協定及設備認證相關資料。

　　通訊方法通常可透過外加模組方式添加新通訊方式。稽核人員將確認受稽單位選用外加模組之設計能力、維護能力與第三方供應商管理能力，並稽核受稽單位是否理解其通訊堆疊之實作方式與內建之協定、是否開啟適當之通訊加密功能、是否具備軟韌體更新機制與是否存有硬體後門，並確認廠商其產品安全應變機制，以界定受稽單位其資安規劃能力可達到中階要求，高於行業水準。

1. **加解密認證安全建議**
2. 針對資訊系統的重要性進行分級。
3. 利用威脅建模方法論，盤點風險，分類系統等級，並產生應對措施與投入資源。
4. 資訊系統之重要性應以業務目標相互契合，將資安問題作為一個商業風險問題而非技術問題，並取得關係人上下一致共識。
5. 由於無法完全遏止所有資安事件發生，建議受稽單位能明智地接受一些風險，利用持續觀測之數據證明，部分風險是可接受的，且不致造成業務發展之阻礙。稽核人員將查核受稽單位之各項管制作為。
6. 以CIS controls top 20為查核基準，並查核是否有用預設值直接上線使用情事發生。
7. 關鍵系統採用尚未被破解且具強健加密等級的加密技術。

　　關鍵系統其身分鑑別、資料倉儲與通訊傳輸應該利用強建等級之密碼學技術搭配管制措施加以保護，強健性以美國NIST、德國BSI或ECRYPT-CSA最新建議皆可接受，須建立與時俱進之機制，提出如何與世界密碼研究進度保持同步(如sha1碰撞該如何應變)之說明。

1. 一般系統採用適當安全等級之加密技術。

　　一般系統雖不影響業務目標，但也應考慮成本效益比相當合適之加密技術與管制措施，以確保身分鑑別、資料倉儲與通訊傳輸三項功能安全。

1. **進階要求(非必要項目，由提案廠商視需要導入)**
2. **企業網路層之安全要求**
3. 定期執行滲透測試。
4. 企業網路層的資訊設備應定期執行滲透測試，以提升安全性，建議至少半年執行乙次。滲透測試執行後若發現漏洞，必須執行漏洞修補，並出示相關紀錄或報告，以確保企業網路層之資訊設備安全。
5. 各網路、系統於上線後，應定期(至少每半年)執行弱點掃描，可存在高風險等級之安全弱點。
6. 各網路、系統於上線後，應定期(至少每年)須經過第三方單位滲透測試確認，不可存在高風險等級之安全弱點。
7. **監控與管理層資訊安全要求**
8. 採用工控協定防火牆進行指令過濾或進行流量偵測分析(如：Port Mirror)。
9. 工控協定防火牆應能支援各種多元化的通訊協定標準，以確保工控指令或資料封包之合法性。
10. 若設備採用金鑰管控，請導入金鑰管理機制。
11. 金鑰管理機制的基本條件至少須完成金鑰生命週期之每個功能項。
12. 工控協定防火牆於上線前，須經過第三方單位滲透測試。
13. 不可存在高風險等級之安全弱點。
14. 針對中風險等級之安全弱點，須提出補償措施。
15. **控制層資訊安全要求**
16. 應建立軟/韌體安全更新機制。
17. 建立安全更新機制，以確保軟/韌體完整性，可達到系統安全啟動與安全功能檢查，防止被植入惡意程式。
18. **加解密認證安全建議**
19. 安全要求較高的設備或服務，採用雙因子認證、生物識別等功能。
20. 採雙因子、生物識別等憑證方式可避免人為選擇密碼之缺失。原則上不允許未經外界檢驗而自行實作之機制，特別是認證套件與整合實作。
21. 導入安全的金鑰管理機制(包含金鑰產生、儲存、使用、備份、銷毀、更新、復原及稽核等，且金鑰具備可供稽核的安全存放及使用歷程紀錄的機制)，避免被竊取或盜用。
22. 若未採業界認可之金鑰管理產品，而採自行開發方式，則受稽單位應提出其設計與實作之安全性證明，至少包含密鑰、證書、協議參數配置、加密套件參數配置、伺服器架構與參數配置，搭配常見實作之問題(如證書校驗缺陷、隨機數生成方式、降級攻擊、截斷攻擊、部署弱點、協議攻擊、性能下降與DoS攻擊)應具安全性之實作與管理。
23. 若採用對稱式金鑰，請另採用非對稱金鑰加以保護。
24. 對稱式金鑰缺點在於雙方共享同一密鑰，故無法用於身分鑑別與不可否認性，須另有機制進行保護。受稽單位應提出完整之設計機制與風險論述，同時實作過程與細節可被檢驗，至少包含密鑰、證書、協議參數配置、加密套件參數配置、伺服器架構與參數配置，搭配常見實作之問題(如證書校驗缺陷、隨機數生成方式、降級攻擊、截斷攻擊、部署弱點、協議攻擊、性能下降與DoS攻擊)應具安全性之實作與管理
25. 軟/軔體更新時使用電子簽章技術以驗證資料的正確性與完整性。
26. 該電子簽章技術應用於軟/韌體更新應具備完善機制，包含可信任根、被檢驗過之演算法實作等。原則上，不接受未經外界檢驗而自行實作之機制，特別是加密套件與整合實作。