研華資訊安全政策
Advantech Information Security Policy

一. 資訊安全政策方針
Guidelines

- 建立專責的資安組織與適當的管理程序, 以確保公司資訊資產之機密性、完整性與可用性, 並重視與保障使用者與客戶資料隱私，完善安全措施，提高系統可用度與信任度。
  Establish a dedicated information security organization and appropriate management procedures to ensure the confidentiality, integrity, and availability of company information assets, and protect the privacy of user and customer data, improve security measures, and improve system availability.

- 導入適當的 IT 備援機制與雲端備份解決方案, 加上定期的災害演練, 讓公司的營運中斷損害, 控制於設定目標範圍內。
  Have appropriate IT backup mechanisms and cloud backup solutions, plus regular disaster drills to contain the damages that caused company's business interruption and loss within the expected target range.

- 重要營運系統與營運活動取得第三方資安認證與外部定期檢視, 特別是生產與組裝廠區, 以及重要電子商務平台網站等。
  Obtained third-party information security certification and regular external inspections for important systems and operations, especially production and assembly plants, as well as important e-commerce platform websites, etc.
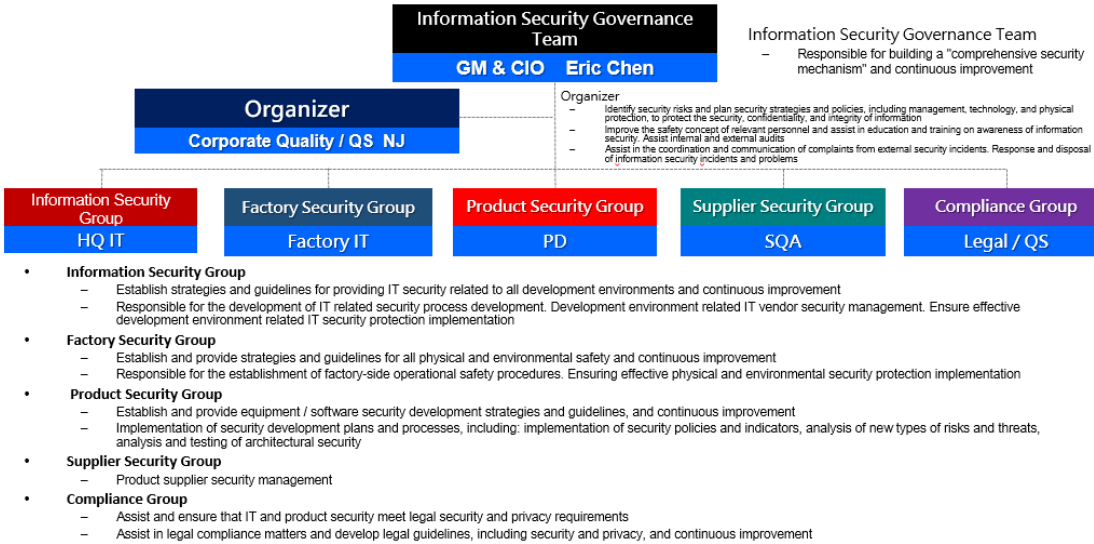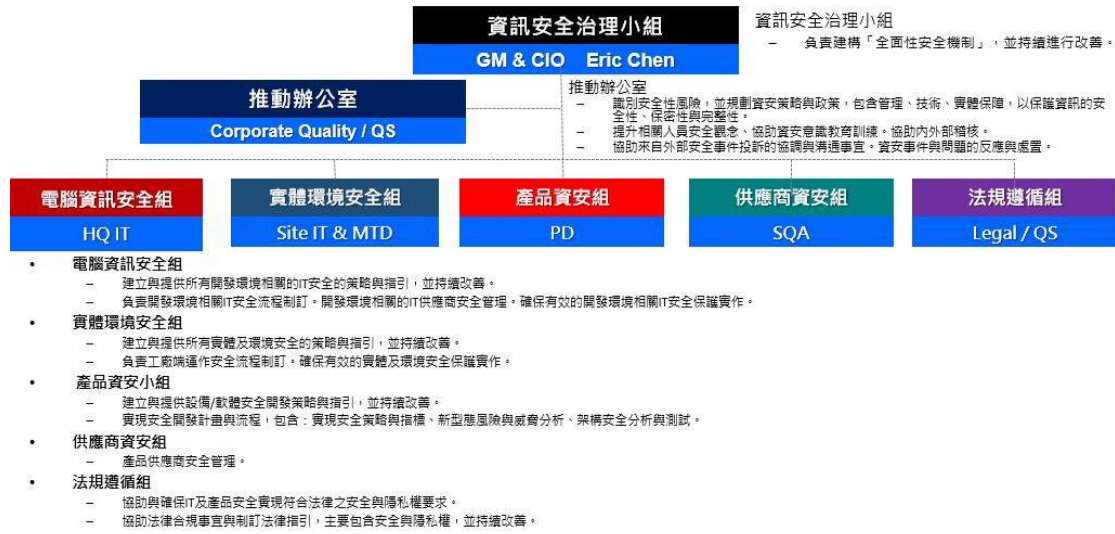
二. 資訊安全目標
Objectives

	Target
專責小組	
建立資安專責小組, 強化資訊安全及資安法規遵循, 如歐洲 GDPR..	100%
外部認證	
生產廠區通過國際資安認證 ISO 27001 規範; 交易網站全數採用超文本傳輸安全協定 (https)	100%
高可用性	
提供高可用度之 ERP, CRM, PLM, MES, e-mail 資訊平台, 降低可能之營運中斷損失	99.5%

|	Target
Task Force	
Establish a task force on information security to strengthen information security and compliance with information security regulations, such as European GDPR ..	100%
External certification	
The production plant passed the ISO 27001 standard for international information security certification; all transaction sites use encrypted transmission security protocols (https)	100%
High availability	
Provide high-availability ERP, CRM, PLM, MES, e-mail information platform to reduce possible loss of operation interruption	99.5%

三. 資安治理組織
Organization

資訊安全治理小組
GM & CIO　Eric Chen

資訊安全治理小組
- 負責建構「全面性安全機制」，並持續進行改善。

推動辦公室
Corporate Quality / QS

推動辦公室
- 識別安全性風險，並規劃資安策略與政策，包含管理、技術、實體保障，以保護資訊的安全性、保密性與完整性。
- 提升相關人員安全觀念、協助資安意識教育訓練。協助內外部稽核。
- 協助來自外部安全事件投訴的協調與溝通事宜。資安事件與問題的反應與處置。

電腦資訊安全組	實體環境安全組	產品資安組	供應商資安組	法規遵循組
HQ IT	Site IT & MTD	PD	SQA	Legal / QS

- **電腦資訊安全組**
  - 建立與提供所有開發環境相關的IT安全的策略與指引，並持續改善。
  - 負責開發環境相關IT安全流程制訂。開發環境相關的IT供應商安全管理。確保有效的開發環境相關IT安全保護實作。
- **實體環境安全組**
  - 建立與提供所有實體及環境安全的策略與指引，並持續改善。
  - 負責工廠端運作安全流程制訂。確保有效的實體及環境安全保護實作。
- **產品資安小組**
  - 建立與提供設備/軟體安全開發策略與指引，並持續改善。
  - 實現安全開發計畫與流程，包含：實現安全策略與指標、新型態風險與威脅分析、架構安全分析與測試。
- **供應商資安組**
  - 產品供應商安全管理。
- **法規遵循組**
  - 協助與確保IT及產品安全實現符合法律之安全與隱私權要求。
  - 協助法律合規事宜與制訂法律指引，主要包含安全與隱私權，並持續改善。

Information Security Governance Team
GM & CIO　Eric Chen

Information Security Governance Team
- Responsible for building a "comprehensive security mechanism" and continuous improvement

Organizer
Corporate Quality / QS　NJ

Organizer
- Identify security risks and plan security strategies and policies, including management, technology, and physical protection, to protect the security, confidentiality, and integrity of information
- Improve the safety concept of relevant personnel and assist in education and training on awareness of information security. Assist internal and external audits
- Assist in the coordination and communication of complaints from external security incidents. Response and disposal of information security incidents and problems

Information Security Group	Factory Security Group	Product Security Group	Supplier Security Group	Compliance Group
HQ IT	Factory IT	PD	SQA	Legal / QS

- **Information Security Group**
  - Establish strategies and guidelines for providing IT security related to all development environments and continuous improvement
  - Responsible for the development of IT related security process development. Development environment related IT vendor security management. Ensure effective development environment related IT security protection implementation
- **Factory Security Group**
  - Establish and provide strategies and guidelines for all physical and environmental safety and continuous improvement
  - Responsible for the establishment of factory-side operational safety procedures. Ensuring effective physical and environmental security protection implementation
- **Product Security Group**
  - Establish and provide equipment / software security development strategies and guidelines, and continuous improvement
  - Implementation of security development plans and processes, including: implementation of security policies and indicators, analysis of new types of risks and threats, analysis and testing of architectural security
- **Supplier Security Group**
  - Product supplier security management
- **Compliance Group**
  - Assist and ensure that IT and product security meet legal security and privacy requirements
  - Assist in legal compliance matters and develop legal guidelines, including security and privacy, and continuous improvement

四. 資安治理運作模式

Operation mode

本公司依據 ISO/IEC 27001:2013 標準的要求，建立、實施、保持和持續改進資訊安全管理體系。本公司全體員工將有效地貫徹執行並持續改進以確保其有效性。 資訊安全管理制度 ISMS（Information Security Management System）所涉及的過程基於以下 PDCA 模式。詳見下圖。

The company establishes, implements, maintains and continuously improves the information security management system in accordance with the requirements

of the ISO / IEC 27001: 2013 standard. All employees of the company will effectively implement and continuously improve to ensure its effectiveness. The processes involved in the Information Security Management System (ISMS) are based on the following PDCA model. See details below
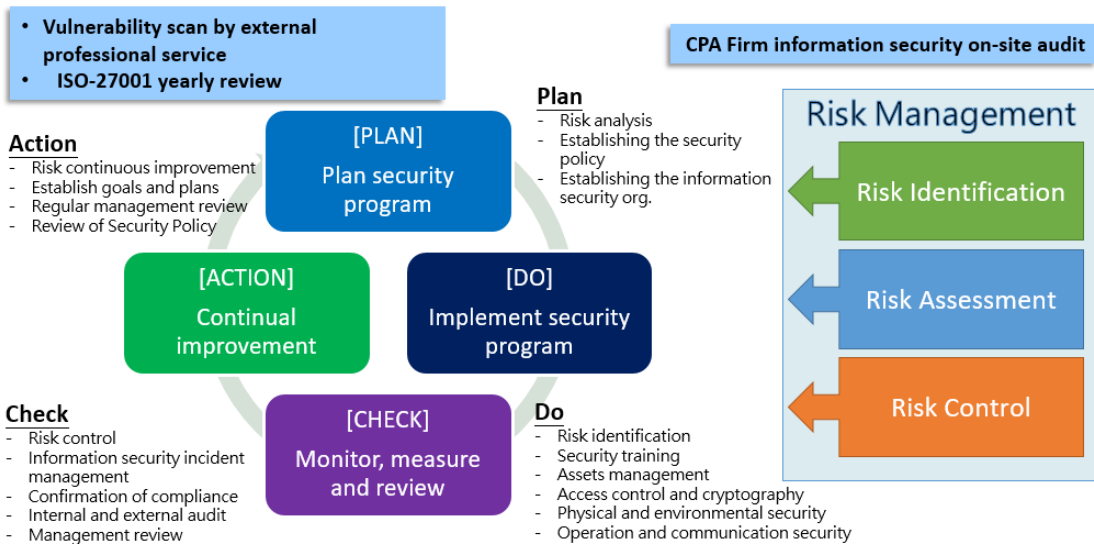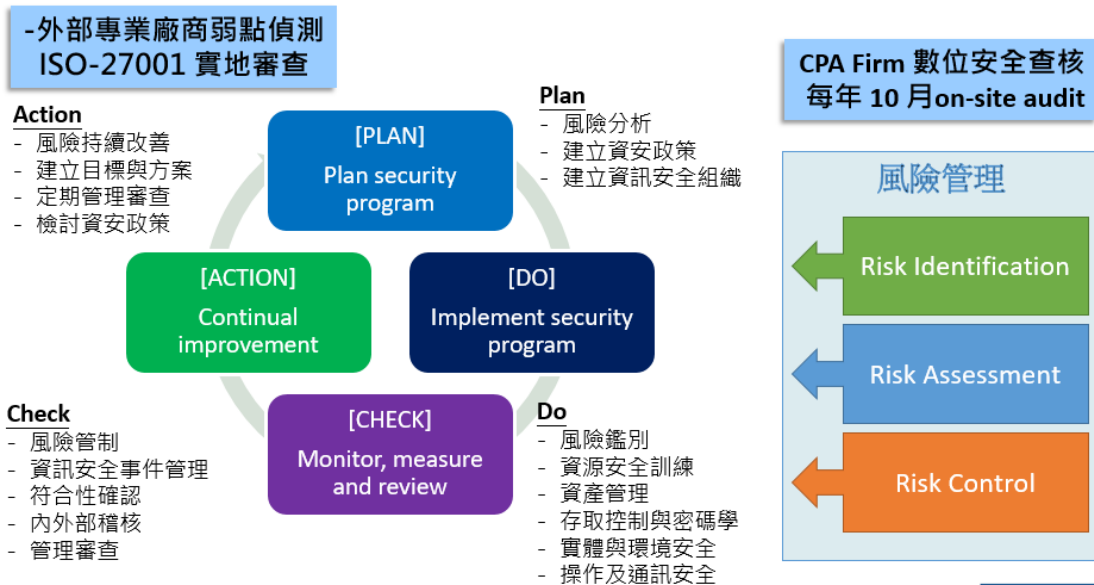
五. **資安防護重點工作**

Major changes & enhancements

Zero Trust

◆ *以往防外，現在也要防內*

同仁的公司電腦, 同仁在外以VPN遠端進入公司
網路, 跨building/ 海外分處/ 工廠/RD測試環境的網路行為都有可能會是駭客入侵的跳板,
應該予以適當的管制與區隔, 依照實際的需求予以放行, 讓合理的人連結使用合理的
server跟service, 內部網路不可以做無管制的開放連結

◆ 採取網路分隔的方式來保護重要的資產，不再只是仰賴持續的警覺
再予以反應 (使用防火牆設定policy, 僅允許開哪些必要port 跟 IP 連結)
執行人(IP/MAC/帳號), 事(port), 物(IP/帳號) 的確認來制定網路連結 policy (白名單)

◆ 採取最低權限的授與策略，嚴格實施存取控制, 檢測與記錄所有的流量

資安防護重點工作

Item	Description
防火牆管制內部網路連線	依照實際的需求予以放行, 讓合理的人連結使用合理的 server跟 service, 內部網路不可以做無管制的開放連結
更安全的網路傳輸	LADP 改為 LDAPs; HTTP改為 HTTPS; 禁止POP3郵件傳送
MFA 多因子認證	重要主機的管理員登入; 從公司外部以 VPN 方式進入內網均需做 二次身份驗證
資料備份的加強	Server/工廠/RD 資料備份需儘可能做到防駭及縮短資料回復時間 及所產生的可能資料時間差異
可視度提升	採用雲端平台監控各電腦在內部的網路異常行為, 當有事件產生 時能在最短時間內做出處置與應對

六. 重大資安事件與處理

Major security incidents and handling

➤ 將 AQIRT@advantech.com 宣告於研華官網, 做為資安事件舉報信箱
https://www.advantech.tw/csr/company_commitment/quality_assurance
https://advcloudfiles.advantech.com/csr/Quality-Assurance/品質與資訊安全事件舉報處理準則_20.pdf

➤ Announce AQIRT@advantech.com on Advantech's official website as a mailbox for reporting on security incidents
https://www.advantech.com/csr/company_commitment/quality_assurance
https://advcloudfiles.advantech.com/csr/Quality-Assurance/品質與資訊安全事件舉報處理準則_20.pdf
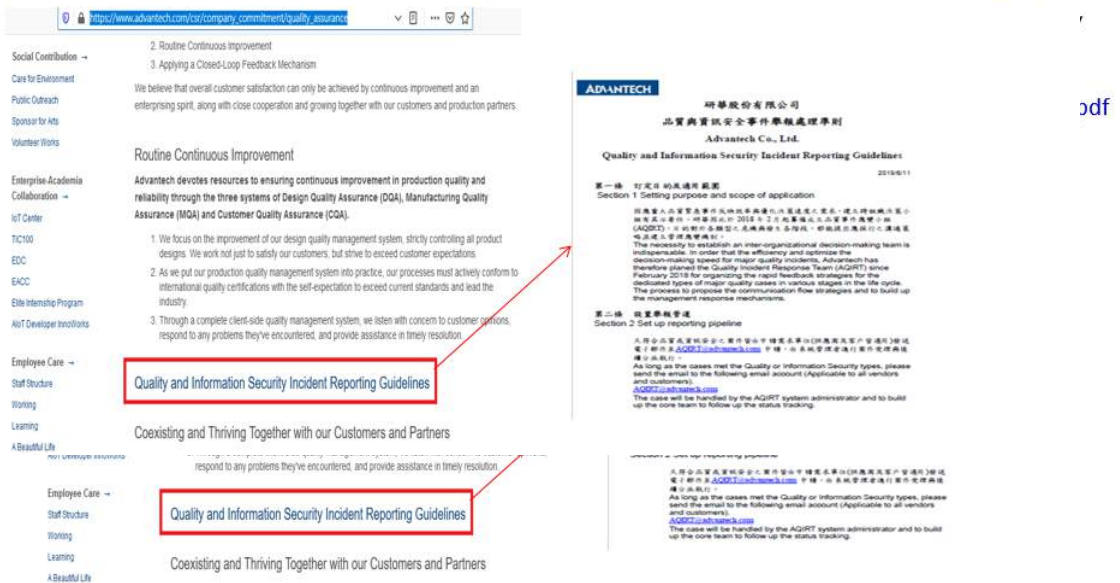
七. 資訊安全作業程序與要點

Information security procedures and policies

參考文件: 資訊安全政策管理

References: Information Security Policy Management

八. 資訊安全認證

Information Security Certification

Item	台灣 Taiwan	中國大陸 China
認證範圍 Certification scope	林口與東湖廠區 Linkou and Donghu Plant	全廠區 Kunshan Plant
認證內容 Certification content	ISO 27001	ISO 27001
取得認證時 Certification date	2019/07	2018/04
認證公司 Certification from	SGS	CQC

昆山廠:
China

ADVANTECH *Enabling an Intelligent Planet*

台灣廠:

Taiwan

台灣廠:

Certificate TW19/00241, continued

Advantech Co., Ltd.

ISO/IEC 27001:2013

Issue 1

Detailed scope

The information security management system that covers the
following product manufacturing processes at Linkou and Donghu
plants supported by Manufacturing Technology Department which is
in accordance with the Statement of Applicability, version A0.

- Embedded PC Series Product.
- Industrial Panel PC Series Product
- Industrial PC Series Product
- Wire/Wireless Communication Product
- Medical Computing Platform Product
- Industrial Automation Series Product

Additional facilities

B1 and 4F~7F, No. 1, Lane 169, Kangning Street, Xizhi District,
New Taipei City 221, Taiwan (R.O.C.)

UKAS
MANAGEMENT
SYSTEMS

0005