# YAN-ISMS-02-09

# 系統獲取與維護程序書

# _V2.0_20211108

延宇資訊股份有限公司

「資訊安全　　暨隱私資訊　　管理系統」

系統獲取與維護程序書

機密等級: 一般

編號: YAN-ISMS-02-09

版本編號: 2.0

修定日期: 2021/11/08

使用本文件前 ，如對版本有疑問 ，請與修訂者確認最新版次。

文件編號: **YAN-ISMS-02-09**

機密等級: ¢一般 £限閱 £密 £機密

本文件歷次變更紀錄:

| 版次 | 修訂日 | 修訂者 | 說明 | 核准者 |
|---|---|---|---|---|
| 1.0 | 2020/01/31 | 梁維志 | 新增 | 楊文欽 |
| 2.0 | 2021/11/08 | 梁維志 | 因應導入 ISO 27701，修訂相關規範。 | 楊文欽 |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

本程序書由　　資訊安全執行小組（　　個人資料保護推動執行小組　　）負責維護。

本資料為延宇資訊股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複

印，複製或轉變成任何其他形式使用。

目錄:

1 目的

2 適用範圍

3 權責

4 名詞定義

5 作業說明

6 相關文件

# 1 目的

## 1.1

本程序書制訂之目的在於確保延宇資訊股份有限公司（以下簡稱本公司）資訊系統獲取、測試與維護作業之安全管理。

# 2 適用範圍

## 2.1

本公司應用系統程式獲取相關活動，如系統安全需求分析、系統測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

# 3 權責

## 3.1

本公司相關資訊系統獲取、維護人員與委外人員：遵守本程序書之相關規定，以確保本公司相關軟體與資 ?等資訊資產之安全。

# 4 名詞定義

4.1 無。

# 5 作業說明

## 5.1 資訊系統之安全需求

### 5.1.1 各單位如有新資訊系統使用需求時，應填寫「YAN-ISMS-04-47電子作業需求申請單」，經核准後需經專案風險評估，並將評估過程記錄於「YAN-ISMS-04-51專案資訊安全風險評估表」後，始可採購買套裝軟體或由委外開發獲得新資訊系統。

### 5.1.2

新開發或新獲取之資訊系統，或是現有系統功能之強化，應在系統規劃階段，即將安全需求納入系統功能。

### 5.1.3

除由系統自動執行之安控措施之外，亦可考量由人工執行安控措施；在採購套裝軟體時，亦應進行相同之安全需求分析。

### 5.1.4

系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

### 5.1.5 資訊系統安全需求分析應考量事項如下:

#### 5.1.5.1 評估保護資訊機密性、完整性及可用性的需求。

5.1.5.2 □□□□

5.2.2 資料輸入應考量的安控措施如下:

5.2.2.1 是否有超出設定範圍的數值。

5.2.2.2 資料檔案是否有錯誤的文、數字。

5.2.2.3 資料是否有毀損或是不正確。

5.2.2.4 是否有未經授權或是前後不一致之資料。

5.2.2.5 超過資料量的上下限。

5.2.3 應適當建立輸入的資料是否有被竄改情形之安控措施。

5.2.4 應適當建立資料錯誤更正或手動更改資料庫的作業程序。

5.2.5 應依據各系統之重要性，適當建立驗證程序。

5.2.6 為確保應用系統內訊息之鑑別性與安全性，應適當建立安控措施。

5.2.7 應用系統資料輸出應經確認，以確保所儲存資料處理之正確性。

5.3 密碼控制措施

5.3.1

使用加密技術時，如資訊專業人力及經驗不足，可請外界的學者專家提供技術諮詢服務。

5.3.2

應遵守權責主管機關訂定的資料保密規範，及使用權責主管機關檢驗合格或認可的加密模組，以確保加密技術產品的安全功能。

5.3.3

5.4

5.4.1

5.4.2

5.4.3

5.4.4

5.4.5

5.4.6

5.5

5.5.1

5.5.2

5.5.3 在執行變更作業前，應確保系統變更作業能為使用者接受。

5.5.4

系統文件在每次完成變更作業後，應定期更新，舊版的系統文件亦應妥善保管及處理。

5.5.5 應建立系統軟體更新的版本控制機制。

5.5.6

在實際執行變更作業前，變更作業的細項建議，應取得權責主管人員之核准。

5.5.7 所有的系統變更作業請求，皆應建立紀錄。

5.5.8 新系統上線作業前，應執行適當的測試。

5.5.9 新系統納入正式作業前，應注意下列事項:

5.5.9.1 評估系統作業效能及電腦容量是否滿足局及系統使用者的需求。

5.5.9.2

檢查發生錯誤後之回復作業、系統重新啟動的準備作業以及資安事件之緊急應變措施完備與否。

5.5.9.3 進行新系統正式納入例行作業程序之準備及測試。

5.5.9.4

新系統的建置是否影響現有系統的作業，尤其是對系統尖峰作業時段之影響。

5.5.9.5 □□□□

5.6.1 □□□□