# 資安室第一季報告

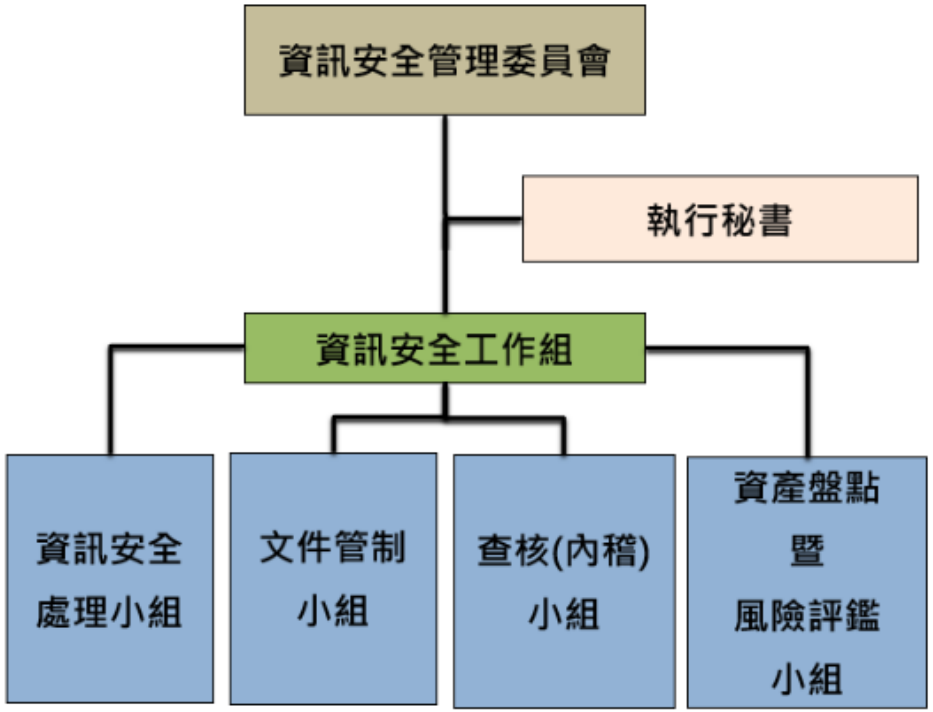
Date: 115/04/01

# 115年第一季 資安報告


## 報告綱要

- 資訊安全管理委員會
- 風險評鑑與因應措施
- 安全管理措施
- 資訊安全管理模式
- 資訊安全投資與改善

# 資訊安全管理委員會




- ✓ 111/09/01 成立資訊安全室，設有專責主管及資訊安全專責人員各一名。
- ✓ 113/12/18 為推動資訊安全管理系統(ISMS)的導入與運行，成立資訊安全管理委員會，總經理擔任召集人並指派副召集人及執行秘書，資訊安全管理代表由各事業單位及功能單位的管理階層擔任，負責協助推動和監督各單位的資訊安全工作。





3

# 風險評鑑與因應措施

- ✓ 114/1/13 董事會通過「資訊安全政策」
- ✓ 114/2/1 公布實施「ISMS資訊安全管理系統」
- ✓ 依據ISMS文件「資訊資產暨風險管理程序書 (ISMS-L2-05) 」規定，依資產清冊執行風險評鑑作業，並產出「風險評鑑報告」。

113年10月 ~ 114年02月執行資產盤點(第一年)
113年10月 ~ 114年02月執行風險評鑑(第一年)
114年11月 ~ 114年12月執行資產盤點(第二年)
114年11月 ~ 114年12月執行風險評鑑(第二年)

# 風險評鑑與因應措施

本次風險評鑑的工作配合規劃於115年度辦理的ISO 27001驗證稽核，主要執行範圍為核心系統所在機房及網路重要基礎設施維運管理活動。

一　實體及環境安全
二　電腦與網路安全
三　人員安全
四　系統存取安全
五　資訊安全
六　應用系統安全管理

# 安全管理措施

- 基於風險評鑑產出「資產清冊_風險評鑑暨組態管理表（ISMS-L2-05-F01）」，本次資訊安全管理委員會核定不可接受風險為高風險項目，進行風險處理。

| 資產名稱 | 維護廠商 | 資產管理者 | 負責單位 | 資產位置 | 資產/授權數量 | 組態管理 | 註記 (用途) | 機密性 C | 完整性 I | 可用性 A | 資產總價值x | 資產等級 x | 風險 | 風險擁有者 | 現有管控 | 風險處理前 發生可能性 | 風險處理前 潛在後果 | 風險處理前 風險值 | 風險處理前 風險等級 | 建議風險處理方式 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Windows 11 | 自行維護 | 各資產使用者 | 資訊中心 | 內湖辦公室 | 16 | V | 個人電腦 | 3 | 2 | 2 | 7 | 高 | R405. 軟體或程式作業失效 | 資訊中心最高主管 | 重新安裝作業系統 | 1 | 2 | 14 | 低 | 接受風險 |
| | | | | | | | | | | | | | 感染病毒 | | A.8.7防範惡意軟體 | 1 | 2 | 14 | 低 | 接受風險 |
| | | | | | | | | | | | | | R902. 系統攻擊或入侵 | | A.8.8技術脆弱性管理 | 1 | 2 | 14 | 低 | 接受風險 |
| Windows Office 365 | 自行維護 | 各資產使用者 | 資訊中心 | 內湖辦公室 | 16 | | 個人電腦文書作業 | 3 | 3 | 3 | 9 | 高 | R405. 軟體或程式作業失效 | 資訊中心最高主管 | 重新安裝 | 1 | 2 | 18 | 低 | 接受風險 |
| | | | | | | | | | | | | | R406. 對系統或軟體的未授權變更 | | A.5.18存取權限 | 1 | 2 | 18 | 低 | 接受風險 |
| | | | | | | | | | | | | | R902. 系統攻擊或入侵 | | A.8.8技術脆弱性管理 | 1 | 2 | 18 | 低 | 接受風險 |

# 資訊安全管理模式

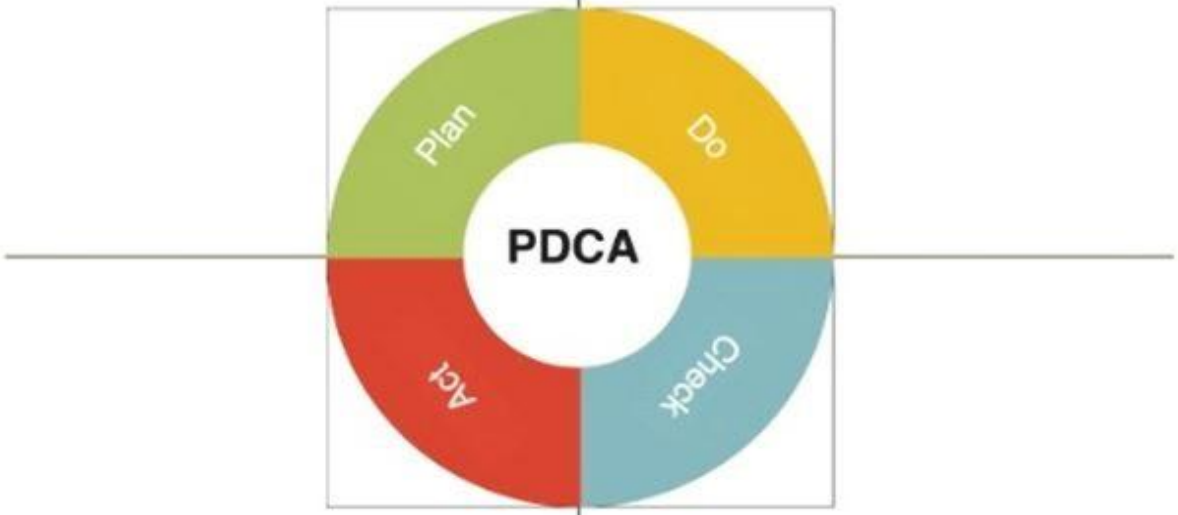
採用PDCA 循環流程管理模式，
確保資訊安全管理目標之達成
並且持續改善。


**資安管理**

- 成立資訊安全管理委員會
- 頒布『資訊安全政策』

**推動執行**

- 資訊安全措施導入
- 資資訊安全宣導與人員教育訓練




**風險改善**

- 改善內部作業程序
- 引進外部解決方案

**風險評估**

- 依資產清冊執行風險評鑑作業，並產出「風險評鑑報告」





7

# 資訊安全管理模式

## 資訊安全管理 (Plan)

- ✓ 111/09/01 成立資訊安全室。
- ✓ 113/12/18 成立資訊安全管理委員會。
- ✓ 114/1/13 董事會通過「資訊安全政策」
- ✓ 114/2/1 公布實施「ISMS資訊安全管理系統」
- ✓ 114/3/6 內部稽核
- ✓ 114/4/10 外部稽核(BSI書面審查)
- ✓ 114/4/24 外部稽核(BSI實地審查)
- ✓ 114/5/14 ISMS ISO/IEC 27001:2022(BSI取證，2025/5/14~2028/5/13)
- ✓ 114/12/30 內部稽核(ISO 27001第二年)
- ✓ 115/2/10 外部稽核(BSI實地審查 ISO 27001第二年)

# 資訊安全管理模式

## 推動執行 (Do)

- 資訊安全措施導入

| | |
|---|---|
| 114/1~114/2 | 新世代防火牆上線 |
| 114/1/21 | 主機弱掃/網頁弱掃 |
| 114/2/4,114/6/18 | BCP(Business Continuity Planning) 營運持續演練 |
| 114/2/11 | Hinet WAF 應用程式防火牆上線 |
| 114/6 | SOC導入(中華資安) |
| 114/6 | 微軟AD導入 |
| 114/7/15 | 主機弱掃/網頁弱掃(複測) |
| 114/9/10,114/9/12 | BCP(Business Continuity Planning) 營運持續演練-紙本 |
| 114/12 | 投保資安險(114/12/1 12時 ~ 115/12/1 12時 /保額500萬 USD) |

# 資訊安全管理模式

## 推動執行 (Do)

- **資訊安全宣導與人員教育訓練**

資安宣導: MIS/ICSO每月定期進行「MIS資安宣導 資訊安全與軟體使用」及「資安情報」不定期宣導。(115 年度至第一季 Total 宣導次數: 9 次)。

資安教育:

新人訓練 115年度至第一季 24 人次。

資安教育訓練/一般人員

114/11/21 資安威脅趨勢與因應

(總完成人數396/總完成時數396/人員占比85%/及格率100%)

資安教育訓練/資訊人員

115 Q1 AI 對資訊安全的影響及因應 E-Course

(總完成人數2/總完成時數4/人員占比100%)

資安會議: 115年至第一季召開資安相關會議 4 次

# 資訊安全管理模式

## 風險評估 (Check)

●依資產清冊執行風險評鑑作業，並產出「風險評鑑報告」

資訊系統帳號盤點。
系統組態管理確認。
防火牆規則盤點及控管。
每年進行伺服器弱點掃描。
每年進行開發程式源碼掃描。
以中華電信HiNet SOC 做為資安情資收集， MIS/ICSO會依據所提供的資訊加強防護。

## 風險改善 (Action)

● 改善內部作業程序

內部稽核 ： 藉由內部稽核進行檢討改進
外部稽核 ： 取得證書

● 引進外部解決方案

【台灣 CERT/CSIRT 聯盟】110/9成為其會員
【台灣資安主管聯盟】 113/11/29成為其「上市櫃會員」
中華電信輔導ISO27001:2022，分別於114年5月 、115年2月取得BSI認證。

# 資訊安全投資與改善

- 資安事件與因應：
  駭客病毒入侵： 115年至第一季無重大駭客或病毒入侵事件。
  電腦網路故障： 115年至第一季無重大網路中斷事件。
  環境設施故障： 115年至第一季無重大環境設施(泛指機房冷氣,供電等設施)故障。
  重大資安事件： 115年至第一季無因發生重大資通安全事件所遭受之損失或影響營運、商譽等之情事。
  115年至第一季無經證實侵犯客戶隱私或遺失客戶資料投訴之情事。

- 114年外稽：ISMS ISO/IEC 27001:2022(BSI取證， 2025/5/14~2028/5/13)
  115年外稽：第二年驗證通過

# 資訊安全投資與改善

- 115年至第一季 資安人員相關教育課程與活動：

| 主辦單位 | 課程/活動名稱 | 日期 | 時數(小時) | 參加人員 | 證(明)書 |
|---|---|---|---|---|---|
| 財團法人台灣金融研訓院 | AI 對資訊安全的影響及因應 E-Course | 115/1/19 | 2 | 資安室主管 | IS1001600012046 |
| 財團法人台灣金融研訓院 | AI 對資訊安全的影響及因應 E-Course | 115/3/9 | 2 | 資安室人員 | IS1001600012211 |

## ➢ 資訊安全投資：

| 項目 | 功能 |
| --- | --- |
| 新世代防火牆 | 外部威脅管理 |
| 防火牆防禦七合一 | 外部威脅管理 |
| 萬用憑證 | 外部威脅管理 |
| 源碼檢測&主機/網站弱點掃描 | 弱點與漏洞辨識 |
| 應用程式防火牆 | 異常偵測 |
| HINET SOC 監控 | 異常偵測 |
| WithSecure EDR&EPP | 防毒防駭 |
| 資訊機房(監視器/溫濕度報警) | 資訊設備防護 |
| AD（Active Directory） | 身分及存取管理和端點安全管理 |
| 投保資安險-保額500萬 USD<br>(114/12/1 12時 ~ 115/12/1 12時) | 財務損失風險轉移 |