# 傳播事業資通安全管理實施計畫範本

國家通訊傳播委員會

中華民國101年9月3日

# <公司全銜>資通安全管理實施計畫

文件編號：　　ISMS-1-001

版　　次：　　1.0

文件日期：　　◯年◯月◯日

機密等級：　　限　　閱

# 壹、背景說明

本公司以「客戶為尊、服務第一、積極創新、持續成長」為具體目標，從「人性」出發，以「客戶」為服務核心，持續強化核心能力，使本公司之服務成為社會大眾的生活好幫手，以及廣大企業的經營好助手。

為確保公司之資通訊資產的機密性、完整性與可用性，必須推動資通安全管理制度、強化全體員工對資通安全之認知，落實資通安全管理於每一個環節，因此，參考主管機關公告之「傳播事業資通安全管理手冊」（以下簡稱資安管理手冊）及相關國家、國際資安標準規範，訂定本「資通安全管理實施計畫」，計畫目標如下：

1、 建立資安管理機制，降低資安風險，保障視聽者權益。

2、 落實資安管理政策，改善資安管理效率，提升公司經營效益。

# 貳、資安管理機制之建立

## 一、法令依據

依主管機關下達之傳播事業資通安全管理作業要點之要求，公司全體同仁應提早因應，以建立企業風險文化，履行法定義務。為執行傳播事業資通安全管理作業，並參考主管機關之資安管理手冊，或依據公司訂定之資安管理政策文件，落實資安管理機制，辦理年度內部稽核。

資安管理實施內容應符合保障資通安全及維護全體同仁權益之原則，並應包含下列各款事項：

（一）資通安全管理標準。

（二）資通安全等級評估。

（三）資通安全管理機制。

（四）資通安全教育訓練。

（五）資通安全應變通報。

（六）資通安全實施評鑑。

## 二、PDCA 流程

本公司依據整體營運活動與所面臨的風險，建立、實作、運作、監視、審查、維持與改進資通安全，資通安全管理機制採用之 PDCA（Plan, Do,

Check, Act）過程模型，詳見圖 1 所示，並依據主管機關頒布之「傳播事業資通安全管理作業手冊」之規定，建立本公司之資通安全管理機制。

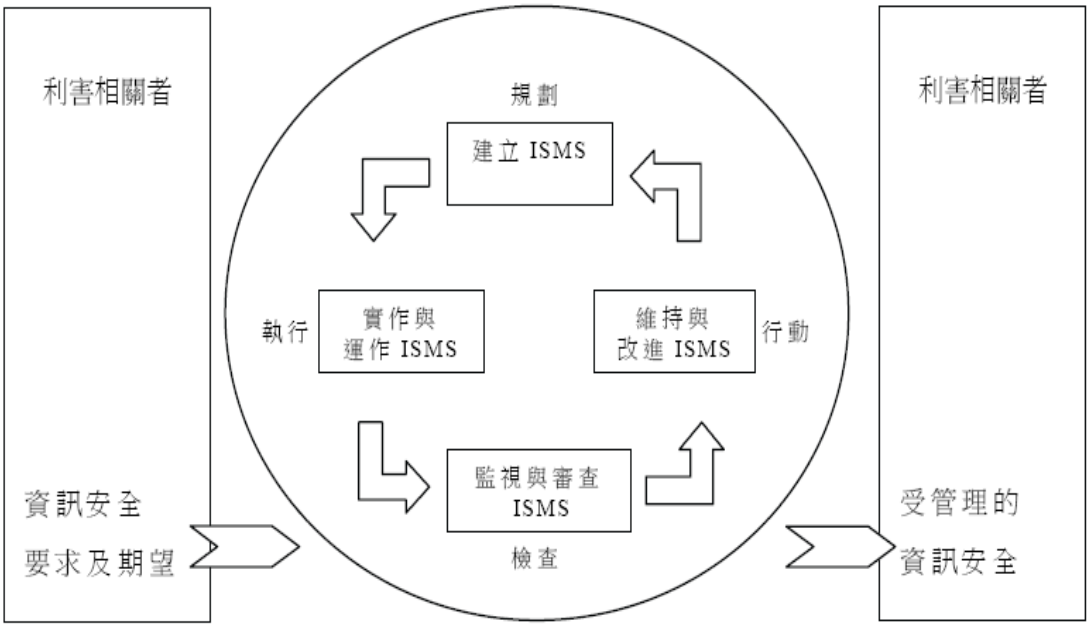



圖 1 資通安全管理機制採用之 PDCA 過程模型

## 三、推動目標

（一）由本公司決策高層主管支持與參與資通安全管理政策，各單位主管亦應督導部屬，協助達成本公司資通安全目標。

（二）全體同仁應充分了解資通安全管理制度的重要性，建立使命感，積極推動，提升公司之形象。

（三）確保資通訊資產的機密性、完整性及可用性，防止敏感性資料與客戶個人資料不當揭露。

（四）各項資通安全防護及管理規定，應符合主管機關之法規及相關資通安全政策之要求。
（五）提供資安相關教育訓練，建立資通安全認知，培養資通安全管理知能。
（六）依據本公司執照核發之營業項目範圍，得區分為不同之事業體或是部門調查營運所需之資產群組，並依據主管機關資通安全等級評估方法，進行衝擊分析與風險評鑑，以選定適當之導入範圍。
（七）導入範圍內之資通訊資產應予以適當保護，採行合宜之資安控制措施，並定期演練前項備援回復作業。
（八）所有資安事故或可疑之安全弱點，應即時依程序通報反映，並予以適當調查及處理。
（九）發現資安議題應即時研商對策，謀求改善機制，健全資通安全管理制度。
（十）透過稽核程序，找出資安問題，提出改善建議，降低資安風險。
（十一）有違反本計畫所定之政策與資安相關規範者，依法令或本公司懲戒規定辦理。
（十二）提供委外廠商及第三方團體必要之資通安全技術協助。
（十三）須考量時間與資源，列出優先順序，逐步推展最終及於全公司，並申請通過外部驗證，驗證範圍應符合資安管理系統 CNS/ISO/IEC 27001 標準。
（十四）本計畫所定之政策應每年定期評估檢討，以反映政府法令、技術發展及業務需求等，以落實資通安全作業。
（十五）本計畫所定之政策須經資通安全管理推動小組審議通過，奉董事長核定後實施，修正時亦同。

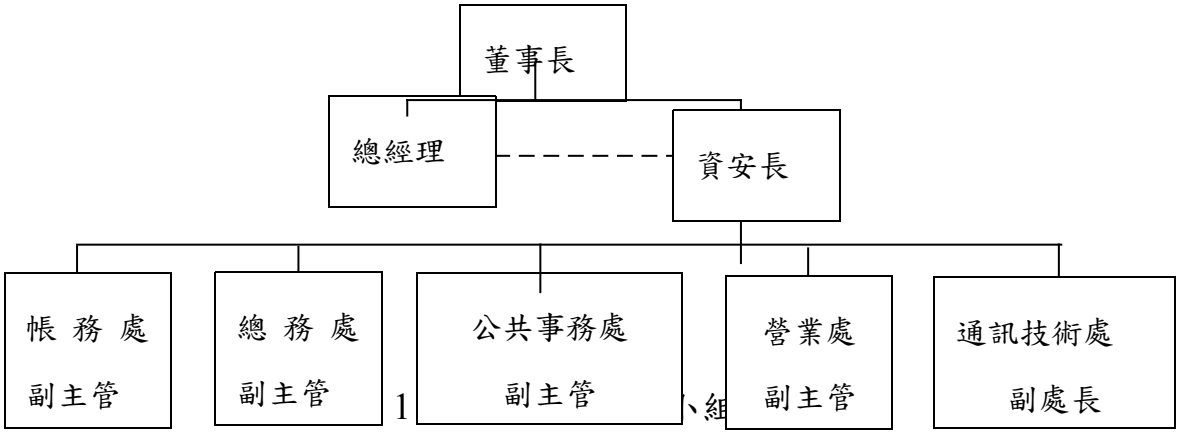
## 貳、資安管理機制之推動

### 一、成立資安管理小組

本公司應成立資通安全管理推動小組，並指派高層主管擔任資安長，由各部門之副主管擔任小組成員，組織架構詳見圖 2 所示，負責推動以下工作：

1、資安政策研訂事項。
2、資安組織權責分工協調事項。
3、資訊資產安全管理研議事項。
4、人員管理及資安教育訓練研議事項。
5、實體與環境安全管理研議事項。
6、通信與作業管理研議事項。
7、存取控制管理研議事項。
8、系統獲取、開發及維護安全管理研議事項。
9、資安事故管理研議事項。

10、營運持續管理計畫研議事項。
11、法規遵循之研議事項。
12、其他資安管理事項研議事項。
13、執行資安管理機制相關事務。




## 二、資通訊資產盤點

本公司應依據資安管理手冊之三大類業務項目區分建議，盤點關鍵業務類、支援業務類、行政業務類資產如下，並分別進行資產群組之調查。

**（一）關鍵業務類資產（表格內為參考，依公司實際狀況填寫）**

| |
|---|
| 傳播執照核定範圍之發射設備、傳輸鏈路、主控臺、信號源接收設備、頭端機房、分配線網路、鎖碼系統、傳送系統等，包含以下業務：<br>☒ 廣播電視<br>☒ 有線廣播電視<br>☒ 衛星廣播電視 |

**（二）支援業務類資產（表格內為參考，依公司實際狀況填寫）**

| |
|---|
| 廣播電視節目供應業務及支援傳播事業營運所需之資訊處理設施，包含：客戶管理系統、帳務管理系統，及所有相關客戶個人資料蒐集、處理及利用之系統。 |

**（三）行政業務類資產（表格內為參考，依公司實際狀況填寫）**

| |
|---|
| 內部輔助單位之業務項目，例如：人事、行政、總務等之業務資產。 |

本公司應依據每一資產群組失效後之「衝擊影響程度」，評估資通安全等級，決定資通安全管理機制改善之優先順序，並每年定期檢討更新。評估後須填寫「資通系統安全等級自我評估彙整表」（詳見資安管理手冊附表一）及「資通安全等級自我評估說明表」（詳見資安管理手冊附件二）。

## 三、資通安全等級評估

（一）需將支援營運所需之「關鍵業務」、「支援業務」及「行政業務」等資產群組全部納入，區分優先順序，逐步建立資通安全管理機制。

（二）針對每個資產群組依「影響業務運作」、「資料保護受到損害」、及「法律規章之遵循」等之影響構面，分別評定各影響構面之資產安全等級，區分為A、B、C三級。

（三）資產群組失效之衝擊影響程度，依據各影響構面，採用最高原則方式處理，當有任一影響構面之衝擊影響程度為A級者，則該資產群組之資產安全等級應評估為A級；如全部影響構面之衝擊影響程度均為C級者，該資產群組之資產安全等級則評估為C級。

（四）最後將所有經評定資產群組之資產安全等級彙整，取其最高者，作為評定本公司之資通安全等級之依據，如最高之資產群組資通安全等級為A者，其之資通安全等級為A級；如最高之資產群組資通安全等級為B者，公司之資通安全等級為B級；如最高之資產群組資通安全等級為C者，公司之資通安全等級為C級。

## 四、風險評鑑作法

若本公司前項資產群組之安全等級經初步評定為A級者，得視需要參考CNS/ISO/IEC 27005標準，進一步實施詳細風險評鑑（Detailed Risk Assessment），以決定風險處理策略（可參考資安管理手冊附件三範例或是自行定義其風險管理作法）。

## 五、訂定資安管理政策文件：

本公司資通安全文件，係為管制資安各項管理性及支援性作業而建立之必要程序，文件架構，詳見圖3所示，各階文件應加以文件化，並注意適時更新，讓有需要的使用者均可隨時取得。

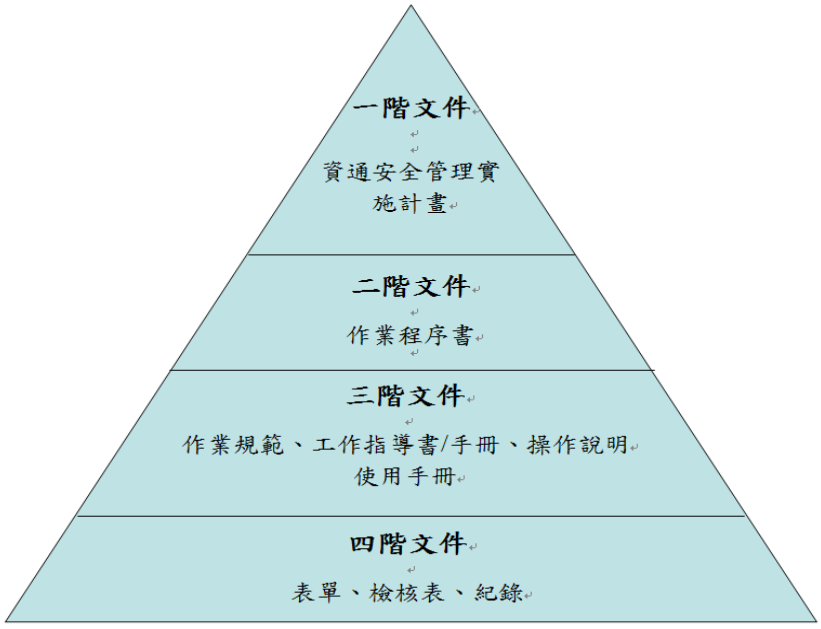


圖 3　資通安全管理文件位階

**1. 一階文件**

本公司資通安全管理實施計畫，提供本公司資通安全管理機制一個整體性的描述，說明本公司資通安全實施之範圍、資通安全政策、相關程序、並描述本公司各項流程間之交互關係。所有與資通安全相關之人員，均應熟悉本政策文件之政策及執行目標，並將其運用為各種程序、方法及工作規範之指導原則。

**2. 二階文件**

應依據內部稽核表之內容，規劃及發展資安相關之各項活動與服務所需之組織運作流程。

**3. 三階文件**

為確保本公司各項資安規劃、維運及支援作業（Operation Support）工作於必要時能有適當之指引，針對流程中之關鍵技術或作業另訂說明文件，如作業指導書（或手冊）、作業規範、操作說明（或使用手冊）等，以作為相關作業執行時之指導。

**4. 四階文件**

為利於落實本公司各項作業，並達到制度化與一致化之目的，對於資通安全之各項要求，於流程執行過程中提供細部之表單、大綱、及查核表等，以利相關人員依照規定之表單及資料執行各項作業，並記錄作業執行結果。此類表單，可以採用電子媒體方式處理，但仍必須保留該表單必要之資料。

**5. 資通安全文件之核定**

(1) 資通安全一階文件由資通安全管理推動小組研擬，經董事長/總經理核定後實施，修正時亦同。

(2) 資通安全第二、三、四階文件，由資通安全管理推動小組授權各分組研提，並由分組召集人審查核定後實施。

## 六、推動方式

資通安全等級經本公司核定後，依據 A（B、C）級，選擇適用之安全基準，建立資通安全管理機制。（以下擇一）

（一）資通安全等級評定為 C 級者，應實施「資通安全管理內部稽核表」（詳見資安管理手冊附件五）之最小限度安全需求項目。

（二）資通安全等級評定為 B 級者，應實施「資通安全管理內部稽核表」之全部控制措施。

（三）資通安全等級評定為 A 級者，除實施前述「資通安全管理內部稽核表」之全部控制措施外，並以通過資安管理第三方驗證為目標，逐年改善最終及於全公司。

## 七、稽核方式

（一）每年至少執行一次內部稽核。

（二）已通過資安管理驗證之資產群組，應定期維持更新，免另辦理內部稽核作業。

## 八、資通安全認知訓練

為建立電信事業員工正確資通安全認知、提升安全防護水準，應推動內部資通安全教育訓練，規劃每年應辦理之資通安全教育訓練及宣導時數如下：

主管、資通訊人員、業務人員及一般人員，每年至少須分別達到3、12、6、3小時之資通安全認知訓練。

## 九、資通安全應變通報

應建立資通安全事故應變作業機制，當發生資通安全事故時，應立即填具「國家通訊傳播委員會資通安全事故通報單」（詳見資安管理手冊附件六）向主管機關通報，並採取應變措施。

## 十、資通安全實施評鑑

（一）內部稽核

本公司每年應於12月底前至少執行一次內部稽核，並將稽核結果依規定填寫以下記錄：

資安管理手冊之附件五、六執行內部稽核時，須填具附件如下：

1. 檢查項目勾選「符合」者，須備妥相關佐證資料以供查核。
2. 檢查項目勾選「不符合」者，須填具「資通安全管理矯正／預防措施一覽表」（資安管理手冊附件七）及「資通安全管理矯正／預防措施單」（資安管理手冊附件八）。
3. 檢查項目勾選「不適用」者，須填具「內部稽核表檢查項目勾選不適用之說明」（資安管理手冊附件九）。

（二）行政檢查

本公司萬一發生資通安全事故影響等級為3級或4級者，須於三天內備妥下列相關資料，以供主管機關行政檢查之用。

1. 重大資安事故應變措施之處理說明。
2. 資通安全管理實施計畫及執行成果
3. 資安管理手冊附件五至附件九、各檢查項目之佐證資料、或經主管機關認可之資通安全管理機制驗證機構產出之稽核報告。

## 十一、年度提報資料要求

（一）本公司應於每年3月底前，依核定之資通安全等級，提報下列資料至主管機關：

1、資安管理手冊之附件一、附件二、附件五。

2、依資安管理手冊之要項說明三（六）執行內部稽核，檢查項目勾選「不符合」者，須提報資安管理手冊之附件七及附件八。

3、依資安管理手冊之要項說明三（六）執行內部稽核，檢查項目勾選「不適用」者，須提報資安管理手冊之附件九。

（二）若本公司取得主管機關認可之資安管理機制驗證機構之 CNS/ISO/IEC 27001 證明者，僅須提報資安管理手冊之附件一及附件二，得免提報資安管理手冊之附件五、附件七至附件九，惟須檢附該驗證證書及驗證報告等相關資料影本。

## 十二、配合工作事項

前項資產群組其安全等級經本公司核定後，依據核定之資通安全等級，完成以下工作事項，詳見表 1 所示：

表 1 資通安全管理實施計畫執行工作事項表

| 作業等級 | 資通訊設施防護縱深 | 實施目標 |
|---|---|---|
| A | 宜建置至少包括防毒閘道設備、網路型防火牆、入侵偵測防禦系統、網路型垃圾郵件過濾設備等取得本會資通設備安全審驗證明之基礎型設備。 | 以通過資安管理第三方驗證為目標 |
| B | 宜建置至少包括防火牆、入侵偵測防禦系統、防毒軟體、垃圾郵件過濾設備等設備。 | 自行規劃並成立資安管理推動小組 |
| C | 宜建置至少包括防火牆、入侵偵測防禦系統、防毒軟體、垃圾郵件過濾設備等設備。 | 加強資安宣導 |

## 柒、附註

請參閱資安管理手冊之附件。