中投有線電視股份有限公司

資通安全維護計畫

第2.0版

生效日期：110 年 11 月 1 日

文件制／修訂紀錄表

文件版本	生效日期	制／修定摘要說明	承辦單位	承辦人
V1.0	109 年 7 月 1 日	初次建立	資安小組	
V2.0	110 年 11 月 1 日	依據修法補充	資安小組	

資通安全維護計畫

目　　錄

壹、 依據及目的.....5
貳、 適用範圍.....5
參、 核心業務及重要性.....5
一、 資通業務及重要性：.....5
二、 非核心業務及說明(選填項目)：.....6
肆、 資通安全政策及目標.....7
一、 資通安全政策.....7
二、 資通安全目標.....7
三、 資通安全政策及目標之核定程序.....8
四、 資通安全政策及目標之宣導.....8
五、 資通安全政策及目標定期檢討程序.....8
伍、 資通安全推動組織.....8
一、 資通安全管理代表.....8
二、 資通安全處理小組.....9
陸、 人力及經費配置.....10
一、 人力及資源之配置.....10
二、 經費之配置.....10
柒、 資通系統及資訊之盤點.....11
一、 資通系統及資訊盤點.....11
二、 機關資通安全責任等級分級.....12
捌、 資通安全風險評估.....12
一、 資通安全風險評鑑.....12
二、 資通安全風險之因應.....13
玖、 資通安全防護及控制措施.....13
一、 資訊及資通系統之管理.....13
二、 存取控制與加密機制管理.....14
三、 作業與通訊安全管理.....15
四、 資通安全防護設備.....18
壹拾、 資通安全事件通報、應變及演練.....18

壹拾壹、 資通安全情資之評估及因應.....18
一、 資通安全情資之分類評估.....18
二、 資通安全情資之因應措施.....19
壹拾貳、 資通系統或服務委外辦理之管理.....20
一、 選任受託者應注意事項.....20
二、 監督受託者資通安全維護情形應注意事項.....20
壹拾參、 資通安全教育訓練.....20
一、 資通安全教育訓練要求.....20
二、 資通安全教育訓練辦理方式.....20
壹拾肆、 公司所屬人員辦理業務涉及資通安全事項之考核機制....21
壹拾伍、 資通安全維護計畫及實施情形之持續精進及績效管理機制
.....21
一、 資通安全維護計畫之實施.....21
二、 資通安全維護計畫之持續精進及績效管理.....21
壹拾陸、 資通安全維護計畫實施情形之提出.....22
壹拾柒、 資通安全偵測與防護之建置及執行方案..... 22
一、資通安全威脅偵測管理機制.....22
二、資通安全防護設備.....23
壹拾捌、 通過資通安全管理驗證之執行方案.....23
一、資通安全管理驗證範圍.....23
二、資通安全管理驗證方案.....23
三、資通安全管理制度稽核機制與缺失改善管理.....24
壹拾玖、 個人資料及用戶隱私安全保護措施.....24
一、 個人資料及用戶隱私之範圍.....24
二、 個人資料及用戶隱私蒐集、處理及利用管理措施.....25
三、 個人資料及用戶隱私資料事故之預防、應變及通報機制.....26
四、 個人資料 及用戶隱私 安全稽核機制.....27
五、 使用記錄、軌跡資料及證據保存.....27
六、 個人資料及用戶隱私安全維護之整體持續改善.....28
七、 業務終止後之個人資料及用戶隱私處理方法.....28
貳拾、 相關附件..... 28

壹、依據及目的

依據資通安全管理法第 10 條及施行細則第 6 條訂定資通安全維護計畫，作為資通安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫(以下簡稱本計畫)。為因應資通安全管理法及機關(構)(以下簡稱機關)資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

貳、適用範圍

本計畫適用範圍涵蓋本公司全部門。

叁、核心業務及重要性

一、 資通業務及重要性：

本機關之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
有線廣播電視業務服務	有線廣播電視業務服務系統	■為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 □為本機關依組織法執掌，足認為重要者	其他： 提供有線廣播電視業務服務	4 小時

各欄位定義：

1.核心業務名稱：請參考資通安全管理法施行細則第 7 條[1]之規定

列示。

2.作業名稱：該項業務內各項作業程序的名稱。

3.重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4.最大可容忍中斷時間單位以小時計。

二、 非核心業務及說明(選填項目)：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
網管系統	無法即時監控網路系統	4 小時
電子公文系統	影響電子公文行政效率	4 小時
客服作業系統	影響客服作業行政效率	4 小時
防火牆	對外網路中斷或無管制連線	24 小時
網域伺服器	官網無法正確連線提供服務	12 小時

項目符合「ISMS-P-005-01 資通安全目標設定表」(附件 1)規範。

各欄位定義：

1.業務名稱：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)

2.作業名稱：該項業務內各項作業程序的名稱。

3.說明：說明該業務之內容。

4.最大可容忍中斷時間單位以小時計。

肆、資通安全政策及目標

一、 資通安全政策

為了促使本公司 ISMS 能貫徹執行、有效運作、監督管理、持續進行，維護本公司重要資訊系統的機密性、完整性與可用性，特頒佈資通安全管理政策。本政策旨在讓同仁於日常工作時有一明確指導原則，所有同仁皆有義務積極參與推動資通安全管理政策，以確保本公司所有教職員之資料、資訊系統、設備及網路之安全維運，並期許全體同仁均能了解、實施與維持，以達資訊持續營運的目標。

1.落實資通安全，強化服務品質：由全體同仁貫徹執行 ISMS，所有資訊作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資通安全制度的工作，強化服務品質，提升服務水準。

2.加強資安訓練，確保持續營運：督導全體同仁落實資通安全管理工作，每年持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全之重要性，促其遵守資通安全規定，藉此提高資通安全智能及緊急應變能力，降低資通安全風險，達持續營運之目標。

3.做好緊急應變，迅速災害復原：訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資訊系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

二、 資通安全目標

1. 本公司執行 ISMS 需達成之資通安全目標，應依據「ISMS-P-005 資通安全目標管理程序書」之相關規定辦理。
2. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
3. 資通安全教育訓練人員訓練時數，符合「ISMS-P-010 人力資源安全管理程序書」 5.4 人員教育訓練之管理規定。
4. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
5. 提升人員資安防護意識、防止發生中毒或入侵事件。
6. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

三、 資通安全政策及目標之核定程序

資通安全政策簽陳資通安全管理代表核定。

四、 資通安全政策及目標之宣導

1. 本公司之資通安全政策(附件 2)及目標應每年透過教育訓練、內部會議、張貼公告、官網發佈等方式，向所有人員進行宣導，並檢視執行成效。

2. 本公司應每年進行資安政策及目標宣導，並檢視執行成效。

五、 資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於會議中檢討其適切性。

伍、資通安全推動組織

一、 資通安全管理代表

依本法第 11 條之規定，本公司訂定營運經理為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定及督導。

2. 資通安全責任之分配及協調。

3. 資通安全資源分配。

4. 資通安全防護措施之監督。

5. 資通安全事件之檢討及監督。

6. 資通安全相關規章與程序、制度文件核定。

7. 資通安全管理年度工作計畫之核定

8. 資通安全相關工作事項督導及績效管理。

9. 其他資通安全事項之核定。

二、 資通安全處理小組

(一)組織

為推動本公司之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全管理代表召集各業務部門成立資通安全

推動小組，其任務包括：

1.跨部門資通安全事項權責分工之協調。

2.應採用之資通安全技術、方法及程序之協調研議。

3.整體資通安全措施之協調研議。

4.資通安全計畫之協調研議。

5.其他重要資通安全事項之協調研議。

(二)分工及職掌

本公司之資通安全處理小組依下列分工進行責任分組，並依資通安全管理代表指示負責下列事項，本公司資通安全處理小組分組人員名單及職掌應列冊，如「ISMS-P-002-01 資通安全管理委員會人員名冊」(附件 3)，並適時更新之：

1.工作職掌(風險管理)

1.1 制定資通安全風險管理制度，每年定期或不定期執行風險評估作業。

1.2 持續不斷的評估與檢討風險管理之具體成效。

1.3 每年定期或不定期審查風險評估的結果與風險改善處理計畫。

1.4 負責每年定期或不定期資訊資產之盤點、彙總、造冊與管理作業。

1.5 負責每年定期或不定期執行資通安全管理制度(ISMS)驗證範圍內資訊資產之風險評估作業。

1.6 負責執行資通安全風險管理作業（包括風險改善計畫、風險改善計畫之後續追蹤與管控）等事宜。

1.7 負責適用性聲明之擬定與傳達。

1.8 參與執行外部評鑑與應對或改善措施。

2.工作職掌(事件管理)

2.1 負責建立資通安全事件之預防、應變及復原處理作業。

2.2 受理資通安全事件回報與事件處理。

2.3 監控、記錄與調查資通安全事件。

2.4 建立、演練與維護核心資訊系統之業務持續計畫(BCP)，如「ISMS-P-006-01 關鍵營運流程分級表」(附件 4)。

2.5 製作及維護核心資訊系統業務持續計畫(BCP)之演練成果報告，如「ISMS-P-006-02 業務持續計畫＼災害復原演練暨處理報告單」(附件 5)。

資通安全推動組織相關辦法，均符合「ISMS-P-002 資通安全組織與權責管理程序書」管理規定。

陸、人力及經費配置

一、 人力及資源之配置

1. 本公司依資通安全責任等級分級辦法之規定，屬資通安全責任等級 C 級，最低應設置資通安全人員 1 人，其分工如下，本公司現有資通安全人員名單及職掌，依規定列冊並適時更新，依「ISMS-P-010-04 人員工作執掌表」(附件 6)辦理。

2. 本公司之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本公司之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

3. 本公司之資通安全長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

4. 人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、 經費之配置

1. 資通安全處理小組於規劃配置相關經費及資源時，應考量本公司之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

2. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全處理小組提出，由資通安全處理小組視整體資通安全資源進行分配，並經資通安全管理代表核定後，進行相關之建置。

3. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安

全維護計畫持續改善機制之管理審查。

4. 資安人力與經費相關辦法，均符合「ISMS-P-010 人力資源安全管理程序書」管理規定。

柒、資通系統及資訊之盤點

一、 資通系統及資訊盤點

1. 本公司每年辦理資訊系統及資訊資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為人員類、資訊類、硬體類、軟體類、環境保護類等，資訊及資通系統盤點相關辦法，均符合「ISMS-P-003 資訊資產管理程序書」管理規定。

2. 資訊及資通系統資產項目如下：

(1) 人員類（People / PE）：正式編制人員、臨時人員、工讀生、專案人員、委外廠商……等。

(2) 資訊類（Information / IF）：資料庫與資料檔案、備份資料、原始程式碼、網路架構圖、系統文件、操作或支援程序、使用手冊、教育訓練教材、管理制度文件、緊急應變&復原計畫、營運持續計劃（BCP）、稽核日誌、契約與協議、報表、表單記錄……等。

(3) 硬體類（Hardware / HW）：

一般硬體：包含電腦設備（伺服器、筆記型電腦、個人電腦、工作站）、CD/DVD 燒錄器、CD/DVD 光碟機、磁帶機、軟碟機、投影機、PDA、印表機……等。

通訊設備：集線器、橋接器、網路交換器、路由器、數據機、電話自動交換機（PBX）、網路纜線、防火牆、入侵偵測系統、視訊會議設備、傳真機、手機。

儲存媒體：CD/DVD（空白）、硬碟（無資料）、磁片（空白）、磁帶（空白）、移動式硬碟（空白）、錄音/影帶（無資料）……等。。

(4) 軟體類（Software / SW）：應用系統軟體、作業系統軟體、開發工具、套裝軟體、公用程式、防火牆軟體、防毒軟體、驗證軟體、資料庫管理系統（DBMS）、加密軟體、文件管理系統、內部開發程式、內部發展系統……等。

(5) 環境保護類(Environment / EV)：

建築類：電腦機房、會議室、辦公室、監控室、接待區、交貨區/裝載區……等。

環境保護設施：不斷電系統、第二電力供應迴路、穩壓器、機櫃、避雷裝置、警報系統、備用發電系統、環境控制系統（火偵測、熱偵測、水偵測、溫濕度偵測、自動消防滅火系統)……等。

3.本公司每年度應依資訊及資通系統盤點結果，製作資訊及資通系統資產清冊，欄位與相關規範依「ISMS-P-003-01 資訊資產清冊」(附件 7)管理規定。

4.各項資訊資產之清查，由權責單位依據業務流程導向將所有資訊資產進行清查，以利後續進行資產鑑別、分類分級與維護管理。

5.各單位管理之資訊或資通系統如有異動，應即時通知資通安全處理小組更新資產清冊。

二、 機關資通安全責任等級分級

本公司因主管機關指定為關鍵基礎設施-網際網路接取服務提供者，維運自行或委外開發之資通系統，為資通安全等級分類 C 級機關。

捌、資通安全風險評估

一、 資通安全風險評鑑

為提升及維持本公司資通安全管理制度之運作，每年定期（每年至少執行一次）由資通安全處理小組進行資通安全風險評鑑作業，包含資通系統及資訊等，相關作業流程與評鑑規範，依據「ISMS-P-003 資訊資產管理程序書」、「ISMS-P-004 資通安全風險管理程序書」管理規定。

二、 資通安全風險之因應

依據風險評鑑結果採取對策或控制措施，擬訂風險處理計畫，依據「ISMS-P-004-02 風險評鑑報告」(附件 8)改善，以期將風險降至可接受之程度，降低資訊資產遭受損害的風險。

玖、資通安全防護及控制措施

本公司依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及資通系統之防護基準，採行相關之防護及控制措施如下:

〇、 資訊及資通系統之管理

(一)資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。

2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。

3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

(二)資訊及資通系統之使用

1. 本公司同仁使用資訊及資通系統前應經其管理人授權。

2. 本公司同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。

3. 本公司同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

4. 非本公司同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。

5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

(三)資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。

2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。

3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、 存取控制與加密機制管理

(一)網路安全控管

網路安全控管，依據「ISMS-P-012 網路安全管理程序書」管理規範。

1. 網路區域劃分如下：

(1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

(2) 內部區域網路 (Local Area Network, LAN) ：機關內部單位人員及內部伺服器使用之網路區段。

2. 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。

4. 內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

5. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

6. 網域名稱系統(DNS)防護

(1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

(2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

7. 無線網路防護

(1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二)資通系統權限管理

1. 資通系統應設置通行碼管理，需符合「ISMS-P-013 帳號密碼及存取控制管理程序書」要求，通行碼需滿足：

(1) 使用者及管理者密碼長度設定至少 8 碼，且應符合密碼設置原則。

(2) 密碼內容之設定，應參雜數字、英文字母大小寫及特殊符號，至少符合下列要求中之 2 項。

(3) 使用者每 6 個月應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

(三)特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通系統之特權帳號不得共用。

3. 資通系統之管理者每季應清查系統特權帳號。

(四)加密管理

1. 機密資訊於儲存或傳輸時應進行加密。

2. 加密保護措施應遵守下列規定：

(1) 應落實使用者更新加密裝置並備份金鑰。

(2) 一旦加密資訊具遭破解跡象，應立即更改之。

三、 作業與通訊安全管理

(一)防範惡意軟體之控制措施

1. 主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

3.使用者不得私自使用已知或有嫌疑惡意之網站。

(二)遠距工作之安全措施

(1) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

(2) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三)確保實體與環境安全措施

實體與環境安全措施，依據「ISMS-P-011 實體與環境安全管理程序書」管理規範。

1.電腦機房之門禁管理

(1) 電腦機房應進行實體隔離。

(2) 工程人員或來訪人員應申請及授權後方可進入電腦機房，管理者並應定期檢視授權人員之名單，如「ISMS-P-011-01 機房門禁卡使用登記表」(附件 9)。

(3) 人員及設備進出應留存記錄，如「ISMS-P-011-02 機房進出管制登記表」(附件 10)。

2.電腦機房之環境控制

(1) 電腦機房之空調、電力應建立備援措施。

(2) 電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全之危險。

3.辦公室區域之實體與環境安全措施

(1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(2) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(四)資料備份

1.重要資料及資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2.敏感或機密性資訊之備份應加密保護。

3.資料備份依據「ISMS-P-015 資訊備份管理程序書」管理規範。

(五)媒體防護措施

1.使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

2.對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶,應保存於上鎖之櫃子,且需由專人管理鑰匙。

(六)電腦使用之安全管理

1.電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

2.連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

3.筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

4.下班時應關閉電腦及螢幕電源。

5.如發現資安問題，應主動循機關之通報程序通報。

(七)行動設備之安全管理

1.機密資料不得由未經許可之行動設備存取、處理或傳送。

2.機敏會議或場所不得攜帶未經許可之行動設備進入

(八)即時通訊軟體之安全管理

1.使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

2.使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：

(1) 用戶端應有身分識別及認證機制。

(2) 訊息於傳輸過程應有安全加密機制。

(3) 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。

(4) 伺服器端之主機設備及通訊紀錄應置於我國境內。

(5) 伺服器通訊紀錄（log）應至少保存六個月。

四、 資通安全防護設備

資通安全防護，依據「ISMS-P-012 網路安全管理程序書」管理規範。

1. 應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練

為即時掌控資通安全事件，並有效降低其所造成之損害，本公司應符合資通安全事件通報及應變辦法規定，訂定資通安全事件通報、應變及演練，依本公司「ISMS-P-009 資通安全事件管理程序書」規範之資通安全事件通報應變程序辦理，通報依「ISMS-P-009-01 資通安全事件報告單」(附件 11)完成資通安全事件之通報及應變程序，並經承辦之權責人員、資通安全長簽核，留存完整之紀錄。

壹拾壹、資通安全情資之評估及因應

本公司接獲資通安全情資，應依據「ISMS-P-009 資通安全事件管理程序書」規範，評估該情資之內容，並視其對本公司之影響、可接受之風險及本公司之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、 資通安全情資之分類評估

本公司接受資通安全情資後，應指定資通安全人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一)資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二)入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據

明確等內容，屬入侵攻擊情資。

(三)機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

二、 資通安全情資之因應措施

本公司於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一)資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二)入侵攻擊情資

由資通安全人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三)機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

壹拾貳、資通系統或服務委外辦理之管理

本公司委外辦理資通系統之建置、維運或資通服務之提供時，依據「ISMS-P-018 委外作業管理程序書」辦理，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、 選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

二、 監督受託者資通安全維護情形應注意事項

1. 受託者執行受託業務，需簽屬保密協定，如「ISMS-P-018-01 委外切結書」(附件 12)，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

2. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

3. 本公司應定期或於知悉受託者發生可能影響受託業務之資通安全事件，依「ISMS-P-018-03 委外廠商資通安全要求查核表」(附件 13)辦理。

壹拾叁、資通安全教育訓練

資通安全教育訓練，依據「ISMS-P-010 人力資源安全管理程序書」管理規範。

一、 資通安全教育訓練要求

本公司依資通安全責任等級分級屬 C 級，每年至少 1 名資通安全及資訓人員各 12 小時以上資通安全專業課程訓練或資通安全職能訓練，一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

二、 資通安全教育訓練辦理方式

1. 本公司應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，規劃如「ISMS-P-010-02 教育訓練計畫表」(附件 14)，以建立人員資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

2. 本公司資通安全認知宣導及教育訓練之內容得包含：

(1) 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、

要求事項及人員責任、資通安全事件通報程序等)。

(2) 資通安全法令規定。

(3) 資通安全作業內容。

(4) 資通安全技術訓練。

3. 員工報到時，於新進員工教育訓練時加強資通安全宣導，應使其充分瞭解本公司資通安全相關作業規範及其重要性。

壹拾肆、公司所屬人員辦理業務涉及資通安全事項之考核機制

本公司所屬人員根據「ISMS-P-010-01 員工保密切結書」(附件15)之要求，持續負有資訊保密之責任，平時考核或聘用，依據人事管理規章，及本公司各相關規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

一、 資通安全維護計畫之實施

為落實本安全維護計畫，使本公司之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本公司之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、 資通安全維護計畫之持續精進及績效管理

1. 本公司之資通安全處理小組應依據「ISMS-P-007 資通安全稽核管理程序書」規範，每年召開資通安全管理審查會議，依「ISMS-P-007-01 資通安全內部稽核計畫表」(附件 16)，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

2. 管理審查議題應包含下列討論事項：

(1) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

(2) 資通安全維護計畫內容之適切性。

(3) 資通安全績效之回饋，包括：

A. 資通安全政策及目標之實施情形。

B.人力及資源之配置之實施情形。

C.資通安全防護及控制措施之實施情形。

D.不符合項目及矯正措施。

(4) 風險評鑑結果及風險處理計畫執行進度。

(5) 資通安全事件之處理及改善情形。

(6) 利害關係人之回饋。

(7) 持續改善之機會。

3.持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，如「ISMS-P-007-03 資通安全內部稽核總結報告」(附件17)，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本公司依據資通安全管理法第16條之規定，應於每年向中央目的事業主管機關，提出資通安全維護計畫實施情形，使其得瞭解本公司之年度資通安全計畫實施情形。

壹拾柒、資通安全偵測與防護之建置及執行方案

一、資通安全威脅偵測管理機制

本公司業於109年6月完成 資通安全責任等級C級核定，並依「資通安全責任等級分級辦法」附表六之規定，本公司為非建置資通安全威脅偵測管理機制之單位，但為評估關鍵基礎設施安全現況，以有效掌握關鍵基礎設施資訊安全之運行，並且協助通傳會強化領域資安監控作業之運作管理，本公司實施資通安全防護機制及依據「資通安全情資分享辦法」要求具備資通安全防護項目之資安偵蒐機制，以配合通傳會進行情資分享。

二、資通安全防護設備

本公司業於109年6月完成資通安全責任等級C級核定，並依「資通安全責任等級分級辦法」附表六之「資通安全防護」辦理項目規定，本公司依現有業務運作狀況，完成以下資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級：

防毒軟體。

網路防火牆。

郵件伺服器具備電子郵件過濾機制。

壹拾捌、通過資通安全管理驗證之執行方案

一、資通安全管理驗證範圍

本機構已實施組織全景之識別 ，並植基於核心業務項目、通信網路基礎設施、電信業務營運系統、與外部其他電信網路之介接、軟硬體資源之上下游供應鏈管理等因素綜合考量，將資通安全管理驗證範圍定義如下:

1.「有線廣播電視系統」、2.「市內國內長途陸纜電路出租業務」之資訊安全管理維運作業。

二、資通安全管理驗證方案

依「資通安全責任等級分級辦法」附表六之規定，本公司業於 109 年 6 月完成資通安全責任等級 C 級核定，並將於 109 年 11 月內完成全部核心資通系統導入 ISO/IEC 27001 :2013 標準，並完成公正第三方驗證，以及持續維持其驗證有效性；本公司強化管理做法將優於僅導入之規定。

三、資通安全管理制度稽核機制與缺失改善管理

1. 為評估本公司之資通安全管理驗證範圍之資訊安全管理制度有效落實，並促使資訊安全管理制度達到持續改善之目的，實施內部資通安全稽核作業遵照「ISMS-P-007 資訊安全稽核管理程序書」配合實施辦理。

2. 第三方外部驗證與內部資通安全稽核之不符合事項或改善缺失皆須採取矯正措施，並且遵照「ISMS-P-008 矯正及預防管理程序書」稽核改善配合實施辦理，並將缺失登錄於「ISMS-P-008-01 矯正及預防處理單」(附件 18)進行各項矯正預防措施的追蹤及查核，以確保各項矯正預防措施確實被執行。

壹拾玖、個人資料及用戶隱私安全保護措施

本公司依據「個人資料保護法」 、「國家通訊傳播委員會所管特定非公務機關資通安全管理作業辦法」 與「國家通訊傳播委員會指定非公務機構個人資料檔案安全維護辦法」之規定，確實維護與管理所保有個人資料及用戶隱私檔案安全，以個人資料及用戶隱私之蒐集、處理及利用管理並避免人格權受侵害。

本公司已依業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，並且導入與執行 BS 10012 PIMS 個人資訊管理系統，與業務終止後個人及用戶隱私資料處理方法。

一、 個人資料及用戶隱私之範圍

(一)範圍

本政策及個人資料管理制度適用於本公司於個人資料蒐集、處理、利用等作業之相關單位及人員為範圍，依據「PIMS-01-01_個人資料管理政策」相關政策辦理。

(二)特定目的及類別

1. 特定目的

依據法務部所訂定之「個人資料保護法之特定目的及個人資料之類別」文件中挑選符合本公司蒐集、處理及利用個人資料之特定目的。

2. 個人資料範圍及類別

依據法務部所訂定之「個人資料保護法之特定目的及個人資料之類別」文件，對應本公司蒐集、處理及利用個人資料欄位及內容。

3. 相關作業流程，依據「PIMS-03-01_特定目的及類別管理作業要點」規定辦理。

(三)用戶隱私範圍

用戶隱私資料包含客戶使用本公司網站服務時蒐集到的個人識別資料，相關蒐集與保護依據「台數光隱私權聲明內容」(附件 19)辦理。

二、 個人資料及用戶隱私蒐集、處理及利用管理措施

1. 直接向當事人蒐集個人資料或用戶隱私資料時，應明確告知以下事項：

(1) 公司名稱。

(2) 蒐集目的。

(3) 個人資料之類別。

(4) 個人資料及用戶隱私資料利用之期間、地區、對象及方式。

(5) 當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料 及用戶隱私 資料 。

(6) 當事人得自由選擇提供個人資料 或用戶隱私資料 時，不提供將對其權益之影響。

2. 所蒐集非由當事人提供之個人資料 或用戶隱私資料 ，應於處理或利用前向當事人告知個人資料 或用戶隱私資料 來源及前項應告知之事項。

3. 得為辦理特定目的進行個人資料或用戶隱私資料之蒐集、處理、利用，於委託期限屆滿時應主動刪除或銷毀。但因法令規定執行業務所必須或經書面同意者，不在此限。

4. 利用個人資料或用戶隱私資料 為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料 或用戶隱私資料行銷。

5. 當事人表示拒絕行銷或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料或用戶隱私資料時，應提供聯絡窗口資訊。並將聯絡窗口及電話等資料，揭示於本 機構 營業處所或公司網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

6. 負責保管及處理個人資料檔案 或 用戶隱私資料 之員工，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

7. 由指定之管理員工定期清查所保有之個人資料 或 用戶隱私資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

8. 本公司如有委託他人或他機構蒐集、處理或利用個人資料用戶隱私資料 時，當對受託者為 適當之監督並與其明確約定相關監督事項。

9. 所蒐集之個人資料或用戶隱私資料 如需作特定目的外利用，必須先行檢視是否符合規定。

10. 本公司因故終止業務時，原保有之個人資料 及用戶隱私資料 ，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

三、 個人資料及用戶隱私資料事故之預防、應變及通報機制

（一）事故預防

1. 本公司員工如因其工作執掌相關而須輸出、輸入個人資料或用戶隱私資料 時，均須通過身份驗證機制以識別員工身份，同時在使用範圍及使用權限內為之，其中通行碼應保密，不得洩漏或與他人共用。

2. 本公司對內或對外從事個人資料傳輸或用戶隱私資料時，加強管控避免外洩。

3. 加強員工認知宣導及教育訓練，本公司每年員工參與個人資料保護法教育訓練，促使員工知悉應遵守之規定且留存紀錄以供備查，並嚴加管制。

（二）事故應變及通報

1. 發現個人資料或用戶隱私資料遭竊取、竄改、毀損、滅失或洩漏，危及本公司正常營運或大量當事人權益之重大個人資料或用戶隱私事故即向國家通訊傳播委員會通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

2. 對於個人資料對於個人資料或用戶隱私資料或用戶隱私資料遭竊取之對象，應以適當方式通知遭竊取之對象，應以適當方式通知使其知悉及本使其知悉及本機構機構個人資料個人資料或用戶隱私資料或用戶隱私資料外洩事實、已採取之外洩事實、已採取之處理措施、客服電話窗口等資處理措施、客服電話窗口等資訊。

3. 針對個人資料針對個人資料或用戶隱私或用戶隱私事故發生原因研議改進措施。事故發生原因研議改進措施。

4. 相關應變與通報程序，依據「PIMS-02-12_個人資料事故管理程序」辦理。

四、 個人資料 及用戶隱私 安全稽核機制

本公司依據「PIMS-02-14_個人資料稽核管理程序」辦理，定期每年1次，辦理個人資料及用戶隱私檔案安全維護稽核， 稽查本機構是否落實規範事項，針對稽查 結果不符合事項及潛在不符合之風險，應規劃改善措施 並確保相關措施之執行。執行改善與預防措施時，應確認不符合事項之內容及發生原因、 提出改善及預防措施方案，以及紀錄查察情形及結果。

五、 使用記錄、軌跡資料及證據保存

本公司為防止個人資料被竊取、竄改、毀損、遺失或洩漏後，未有相關紀錄可供追蹤，故訂定「PIMS-03-03_ 紀錄及證據管理作業要點」規範使用紀錄及實體、電子軌跡證據之保存方式；個人資料蒐集相關告知及同意證據之紙本及電子資料，如無其他法令限制，應至少保存5年；電子形式軌跡資料(含應用系統及資料庫之軌跡資料、網路設備之異常軌跡資料等)，如無其他法令限制，應至少保存5年，以確保相關證據於司法訴訟時，於時效內均能完整提出。

六、 個人資料及用戶隱私安全維護之整體持續改善

本公司將依據「PIMS-02-16_持續維護及改善管理程序」相關程序，隨時檢視個人資料或用戶隱私資料安全維護執行狀況，注意相關技術發展及法令修正等事項，檢討個人資料及用戶隱私安全維護是否合宜，並予必要之修正。針對個人資料及用戶隱私安全稽核結果不符合法令之虞者，規劃改善與預防措施。

七、 業務終止後之個人資料及用戶隱私處理方法

本公司因業務終止、交易完成、特定目的消失、契約或法令規定期限屆滿等，將依據「PIMS-03-06_業務終止管理程序」相關程序，對所保有之紙本個人資料或用戶隱私資料應以碎紙、委外焚化等方式銷毀紙本，個人資料或用戶隱私資料儲存於磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物者，應以消磁、剪斷、敲擊等破壞措施銷毀。本公司進行前項個人資料或用戶隱私資料銷毀處

理時，應記載處理之時間、地點，並以照相或錄影方式留存紀錄。

貳拾、相關附件

附件表單。