



新法說明及TPIPAS + 修正草案說明

李怡親 專案經理

科技法律研究所 跨域整合中心

財團法人資訊工業策進會

ichinlee@iii.org.tw
www.iii.org.tw



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE

修正條文總覽

修正條文	類型	主要修正重點	法源依據
3.7 查核人員	新增	增訂查核人員定義，確保查核獨立性，不得與管理人員兼任	安維辦法草案§17
7.2.2~7.2.4 教育訓練	修正	強調「定期」辦理，差異化（通識/專業）教育訓練	安維辦法草案§8、§21
7.3.3 使用紀錄與證據管理	修正	明定紀錄範圍三類，相關紀錄保存至少五年	安維辦法草案§25； 個資法§30
7.3.4 系統日誌管理	新增	資通系統日誌記錄範圍、週期及留存政策	安維辦法草案§13
8.2 個人資料管理範圍	修正	每年界定，建立個人資料盤點清冊及流程說明文件	安維辦法草案§18
8.4.3 處理	修正	增列銷毀留存方法、時間、地點及相關證明	安維辦法草案§15
8.4.6 國際傳輸	修正	傳輸前告知當事人，遵循主管機關跨境限制	個資法§21
8.4.7 特種個人資料	修正	加強紙本/電子檔案管理、安全銷毀及加密	安維辦法草案§11
8.7 安全管理措施	修正	用語對齊個資法修正（竊取、竄改、毀損、滅失或洩漏）	個資法 §12文字修正 個資法施行細則 §12 II
8.10 事故之緊急應變	修正	知悉即通報；應變措施記錄；通報主管機關及授證機關	個資法§12、§48II
11.7 未成年人之保護	修正	確認法定代理人有效同意，強化安全措施	Global CBPR
11.14 應對政府存取資料	新增	建立回應司法/政府調閱個資之應對程序及紀錄保存	Global CBPR

安全管理措施修正總覽

修正項目	類型	主要修正重點	法源依據
A8.7.1 存取控制	修正	存取政策核定、特權帳號年度清查、最小權限（識別涉個資人員）、資訊分享紀錄留存	安維辦法草案§23
A8.7.2 事件日誌與可歸責性	修正	原「技術檢視」更名與資安法一致；增完整性監控、日誌至少保存六個月	安維辦法草案§23
A8.7.3 識別鑑別	修正	增訂密碼複雜性規則與定期更換週期	安維辦法草案§12
A8.7.4 媒體安全	修正	刪除「媒體標記」管理措施	—
A8.7.5 實體與環境安全	修正	建立實體安全周界、監視系統、出入紀錄保存期間	安維辦法草案§10
A8.7.6 資訊傳輸	修正	傳輸加密協定之設定截圖、加密證明或傳輸軌跡紀錄	安維辦法草案§11、§22
A8.7.7 系統與資訊完整性	修正	整併A8.7.10；強化惡意程式防護；新增測試環境管理	安維辦法草案§9
A8.7.8 系統發展生命週期	修正	整併A8.7.9；源碼檢測、弱點掃描、滲透測試	安維辦法草案§23
A8.7.9 網路安全防護	新增	網路設備定期維護，防範未授權存取及入侵	安維辦法草案§23
A8.7.10 新興技術風險管理	新增	雲端及AI服務採用之風險評估與規範	商業服務業及零售業個資保護自評表查核項目14
A8.7.11 資料可用性維護	修正	原「營運持續計畫」聚焦個資備份管理、刪除系統備援	安維辦法草案§11、§22
A8.8.2 保密契約	修正	人員異動時交接媒介物，保密義務於離職後延續	安維辦法草案§7

新法預告彙整

訂定中法規命令

1

個人資料保護政策推進會議運作辦法

訂定個資保護政策推進會議之運作方式及相關事項

2

個人資料事故通知通報及應變辦法

訂定個資事故通知、通報內容與時限、應變措施及紀錄保存

3

個人資料檔案安全維護管理辦法

訂定公務機關及非公務機關個資安全維護、管理機制及應採措施

4

個人資料保護長及相關人員職掌職能條件及訓練辦法

訂定個資保護長、專人之職掌、職能條件與訓練事項

5

公務機關個人資料保護管理事項實施情形稽核辦法

訂定稽核頻率、內容、方法、結果交付及改善報告提出等事項

6

檢查非公務機關落實個人資料保護法情形作業辦法

訂定非公務機關個資保護落實情形之檢查規劃、評估方式及考量因素

7

個資法第51條之1第1項非公務機關管轄列表

規範個資保護委員會成立後6年內，非公務機關個資行政監督之管轄權歸屬（報請行政院公告）

8

個人資料保護法施行細則（修正）

配合個資法部分條文修正及相關子法新訂，調整技術性、細節性規範事項

新法預告彙整

重點解析



個人資料保護法

於2025.11.11公告



「個人資料保護法施行細則」草案

於2026.01.22預告



「個人資料檔案安全維護管理辦法」草案

於2026.01.22預告



「個人資料事故通知通報及應變辦法」草案

於2026.01.22預告



「檢查非公務機關落實個人資料保護法情形作業辦法」草案

於2026.02.11預告

- 確立獨立機關權責與「過渡期間」設計
- 增訂行政檢查權
- 強化通報義務
- 強化公部門監督

- 修正去識別之「無從識別特定當事人」之定義

- 資料盤點與範圍界定
- 特種個資：管制規則、加密
- 風險分層：大型非公務機關
- 系統日誌與資料刪除：帳號
- 管資安、管人員、管設備
- 管理、日誌留存、刪除銷毀

- 「雙通」義務：通知與通報之黃金72小時
- 「公開公告」的例外條款
- 大型非公務機關之模擬演練

- 發動門檻：違法或違法之虞；認有必要
- 年度檢查規劃的篩選指標：規模與類型、管理與技術、事故紀錄、受檢情形、與民生密切性

個資法修正重點

個人資料保護法

總統已公布施行，尚未實施

114年個資法修正背景



憲法法庭判決

- 欠缺個人資料保護之獨立監督機制
- 對個人資訊隱私權之保障不足

⚡ 有違憲之虞



獨立監督機制回應

個人資料保護委員會

- ✓ 個資會組織法
立院審議中
- ✓ 配合個資會職權之修正
已於114年11月完成，
正在辦理個資子法制作業
- ✓ 配合數位時代的法規調適
持續研議，籌備處與個資會接力推動

114年個資法修正鳥瞰（修正條文一覽）

第1條之2

政策推進會議

第21條之1
至之5

公務機關個資保護之監督

第12條

事故通報應變及紀錄保存

第22條

非公務機關事前檢查規劃

第18條

個資長、公務機關安維辦法

第51條之1

非公務機關監管過渡機制

第20條之1

非公務機關安維辦法

第53條之1

行政救濟程序

第21條

國際傳輸之限制權限劃一

114年個資法修正重點

三大目標 × 五大關鍵措施



三大優先目標



成立獨立監督機關



強化公務機關管理



確保監理效能穩定



五項關鍵措施

- | | | |
|---|------------|----------|
| 1 | 增訂個資事故處置義務 | §12 |
| 2 | 基礎個資檔案安維辦法 | §18/20-1 |
| 3 | 公務機關置個資保護長 | §18 |
| 4 | 內外部稽核及檢查機制 | §21-1~4 |
| 5 | 六年過渡達成事權集中 | §51-1 |

114年個資法修正重點

關鍵措施1 | 增訂個資事故處置義務 (§12修正)

修正前 Before

- 僅有通知義務 (1項)
- 通報義務僅存在於各部會所定個資檔案安全維護辦法 (非公務機關)
- 通知要件：違法 + 查明後

修正後 After

- ✓ 處置義務：通知、通報、應變、紀錄留存 (4項)
- ✓ 通報要件：子法將規範一定通報範圍，避免無實益通報
- ✓ 通知要件：知悉事故後均須通知

 由個資會統一受理事故通報，另有子法規範圍通報範圍；違反通報等義務者有行政罰

114年個資法修正重點

關鍵措施 2 至 5 | 制度建構與監理效能

2. 基礎個資檔案安維辦法 §18 / §20-1

- ▶ 由個資會訂定共通基礎版本，公私部門均適用
- ▶ 特定業別安維辦法在過渡期繼續有效，管制標準須等於或高於共通版

3. 公務機關置個資保護長 §18

- ▶ 由機關首長指派人員兼任
- ▶ 統籌規劃、督導考核機關個資管理事務
- ▶ 應配給適當人力及資源

4. 內外部稽核及檢查機制 §21-1~4

- ▶ 個資會全面納管，有權稽核及行政檢查
- ▶ 違法未配合改正，個資會得對外公布機關名稱

5. 六年過渡達成事權集中 §51-1

- ▶ 個資會先行納管無明確目的事業主管機關者
- ▶ 每2年檢討，逐步減少目的事業主管機關範圍
- ▶ 個資會成立6年後完成權限移轉

個人資料保護法第五十一條之一第一項所稱由中央目的事業主管機關或直轄市、縣（市）政府管轄之非公務機關列表草案

列表統計總覽

388 類非公務機關 24 個主管機關

118

類

經濟部

最多，佔30%

79

類

衛生福利部

佔20%

37

類

交通部

佔10%

35

類

內政部

佔9%

28

類

農業部

佔7%

*其他 19 個主管機關 合計 91 類 (司法院5、財政部13、金管會12、通傳會11、數位發展部6 ...等)

三大主管機關詳細分類

經濟部 (118類)

- 製造業 (食品、化工、電子半導體、汽車、機械等)
- 零售業、加油站業
- 能源業 (電業、天然氣)
- 自來水事業
- 專利師、商標代理人
- 研究發展服務業
- 電子遊戲場業
- 石油相關業 (煉製、輸入輸出)

衛生福利部 (79類)

- 醫師、牙醫師、護理人員藥師等各類醫事人員
- 醫院、診所、長照機構
- 物理治療、職能治療語言治療、心理師等
- 食品製造業、藥品零售業
- 社會福利機構、托嬰中心
- 志願服務運用機構
- 救護車、人工生殖機構

交通部 (37類)

- 航空業 (航空運輸、航空站地勤、貨運承攬)
- 海運業 (船舶運送、船務代理、貨櫃集散站)
- 陸運業 (汽車、計程車鐵路、大眾捷運)
- 旅遊業 (旅館、旅行業觀光遊樂業)
- 郵政業、外送平台

其他主管機關分類

內政部

35類

不動產業、保全業、殯葬業、移民業務、建築師、政黨、宗教團體

農業部

28類

農漁會、農藥販賣業、畜牧場、屠宰業、獸醫師、漁撈養殖業

金融監督 管理委員會

12類

銀行業、保險業、證券業、期貨業、電子支付、會計師

財政部

13類

記帳士、報關業、公益彩券、保稅倉庫、菸酒製造進口業

國家通訊 傳播委員會

11類

電信事業、廣播電視、有線電視、衛星廣播電視事業

教育部

9類

私立各級學校、短期補習班、特殊教育學校、圖書館

運動部

7類

運動彩券業、高爾夫球場、民營運動場館、特定體育團體

數位發展部

6類

網路零售業、軟體出版業、電腦程式設計、第三方支付業

勞動部

6類

人力仲介業、人力供應業、職業訓練機構、工會

環境部

6類

廢棄物清除處理業、病媒防治業、清潔服務業

司法院

5類

民間公證人、全國及地區公證人公會

其他（9個）

14類

法務部、衛生福利部（食品）、文化部、中央銀行、公共工程委員會等

重要規定說明

1

過渡期限制

個資會成立後六年內適用本列表，屆滿後將重新評估，監管權或全數移轉個資會統一管理。

2

列表採中央主管機關列名制

本列表僅列明「中央目的事業主管機關」，未區分地方政府。中央與直轄市、縣（市）政府之管轄分工，仍依各主管機關原監管法令之業務分工決定。

3

列表外機關全數由個資會監管

未納入本列表之非公務機關，一律改由個人資料保護委員會（個資會）籌備處負責行政檢查、裁處等監督管理事項。

4

業務監管範圍維持不變

納入列表之機關，原主管機關對其業務監管之業務分工方式（含行政檢查及裁處）維持不變。

個人資料法施行細則修正重點

個人資料保護法施行細則

預告修正「個人資料保護法施行細則」部分條文

115年預告個資法施行細則修正重點

施行細則修正重點

配合個資法母法修正（114.11.11發布），施行細則進行刪除、配合修正及其他必要調整



配合母法刪除之規定

已由新訂子法取代

§12 安全維護措施框架

個資檔案安全維護管理辦法

§24 公務機關應訂安全維護規定

個資檔案安全維護管理辦法

§22 事故發生後之適當通知方式及內容

個資事故通知通報及應變辦法

§25 專人定義及教育訓練

個資長及相關人員職掌職能條件及訓練辦法

⚖️ §17 無從識別定義修正

修正前

個人資料以代碼、匿名、隱藏部分資料或其他方式，「無從辨識該特定個人者」

⚠️ **解釋疑義：**「匿名」與「匿名化」概念混用；「代碼、隱藏資料」又似指「假名化」，易使外界產生概念混淆。

修正後

「指運用當時存在技術方法，使該個人資料依某呈現方式至少已無從直接識別特定自然人」

✓ **依據：**憲法法庭111年憲判字第13號——學研條款之去識別化，指排除「可直接識別」及「完全匿名且無還原可能性」，而屬可能間接識別之資訊。

預告共通辦法重點

個人資料檔案安全維護管理辦法

預告「個人資料檔案安全維護管理辦法」草案

預告共通辦法重點

法規架構與適用對象

兩層次合規義務一次掌握



全體適用

第 5 ~ 15 條

所有公務機關或非公務機關

- ⑤ 界定個人資料管理範圍
- ⑥ 建立事故通報應變機制
- ⑦ 人員安全管理措施
- ⑧ 個資保護教育訓練
- ⑨ 電子個資設備安全管理
- ⑩ 實體場域安全措施
- ⑪ 特種個資安全管理
- ⑫ 資通系統存取安全
- ⑬ 系統事件日誌記錄保存
- ⑭ 個資定期備份保護
- ⑮ 個資刪除及業務終止處理

+



額外強化要求

第 16 ~ 26 條

公務機關 + 大型非公務機關

- ⑮ 訂定個資安全維護計畫
- ⑯ 指定專責人員及執行小組
- ⑰ 個資盤點清冊 (7大項目)
- ⑱ 每年定期風險評估
- ⑲ 定期辦理事故演練
- ⑳ 差異化教育訓練
- ㉑ 一般個資媒介物管制
- ㉒ 資訊安全強化措施
- ㉓ 內部及委外稽核 (每年 ≥ 1 次)
- ㉔ 個資使用紀錄保存5年
- ㉕ 整體持續改善機制

預告共通辦法重點

全體適用措施（一）

管理基礎 ♦ 人員安全 ♦ 第5-8條



第5條

界定個人資料管理範圍

- 定期清查所保有個資現況
- 界定個資管理範圍



第6條

建立事故通報應變機制

- 建立通報、通知機制
- 訂定事故應變程序



第7條

人員安全管理措施

- 識別涉及個資處理人員
- 建立身分識別與權限管控
- 人員異動交接個資措施



第8條

個資保護教育訓練

- 定期施以認知宣導
- 定期辦理教育訓練

預告共通辦法重點

全體適用措施（二）

設備安全 ◆ 場域保護 ◆ 個資管理 ◆ 第9-15條



電子個資之設備安全

第9條

存取控制、防毒軟體更新、弱點修補



實體場域安全措施

第10條

機房門禁、監控系統、實體障礙



特種個資安全管理

第11條

加密、安全傳輸、安全銷毀



資通系統帳號管理及存取安全

第12條

最小權限原則、帳號清查、密碼複雜性



系統事件日誌記錄

第13條

訂定日誌留存政策、記錄管理者操作紀錄



個資定期備份保護

第14條

定期備份、對備份資料採保護措施



個資刪除及業務終止處理

第15條

刪除、銷毀或移轉紀錄至少留存5年

預告共通辦法重點

公務機關及大型非公務機關

六大額外強化要求



第16-17條 組織治理

安全維護計畫 + 專責人員及執行小組

*特別注意專責人員與查核人員不得互相兼任。



第18-20條 風險管理

個資盤點清冊 → 年度風險評估 → 事故演練



第21條 差異化訓練

通識課 + 專業課，含訓練成效評估



第22條 資料安全

媒介物管制、汰除管理、備份保護

*若為高風險個資，組織得採安全加密、安全傳輸與安全銷毀機制。



第23條 資訊安全

隱碼機制、滲透測試、日誌至少留存六個月



第24-26條 稽核改善

年度稽核、紀錄保存5年、持續改善機制

預告共通辦法重點

組織治理強化

第16條：安全維護計畫 第17條：專責人員與執行小組



個資安全維護計畫

第16條

計畫應包含（共10項）

- ✓ 配置管理人員及相當資源
- ✓ 界定個人資料之範圍
- ✓ 個資風險評估及管理機制
- ✓ 事故預防、通報及應變機制
- ✓ 人員管理、宣導及教育訓練
- ✓ 設備及場域安全管理
- ✓ 資料安全、資訊安全
- ✓ 資料安全稽核機制
- ✓ 使用紀錄、軌跡資料及證據保存
- ✓ 個資安全維護之整體持續改善

△ 計畫修訂須由個資保護長或其指派人員核定



專責人員與執行小組 第17條

大型非公務機關應設置：

個資保護管理專責人員

- 大型非公務機關應指定
- 具備適當專業能力

個資保護管理執行小組

- 辦理個資保護政策研議
- 執行、稽核、改善等事項
- 訂定成員組成及運作規範

查核人員

- 辦理個資安全稽核
- 不得與管理人員兼任（獨立性）
- 具備適當專業能力

預告共通辦法重點

風險管理三步驟

第18條：盤點清冊 第19條：年度風險評估 第20條：事故演練



個資檔案 盤點清冊

第16條

- 1 保有單位
- 2 個資項目、類別、型態、數量
- 3 蒐集之目的、方式、來源
- 4 告知方式或免告知情形
- 5 相關業務或程序
- 6 目的外利用情形
- 7 保存方式、期限及銷毀方式



年度風險評估

第19條

- 1 每年定期識別、分析及評估風險
- 2 個資項目、類別、型態、數量
- 3 處理個資之方法、技術
- 4 內外部之潛在威脅
- 5 依評估結果採適當安全措施
- 6 擬定及實施風險處理計畫



定期事故演練

第20條

- 1 依風險評估結果辦理
- 2 通報機制演練
- 3 通知機制演練
- 4 應變機制演練
- 5 確保機制運行之有效性

預告共通辦法重點

差異化教育訓練與資料安全管理

第21條：教育訓練 第22條：個資檔案安全管理



差異化教育訓練 第21條

依職務規模差異訂定

職務、業務規模、個資保有量、業務性質

通識課 + 專業課

管理人員、查核人員應有對應專業訓練

訓練內容規範

內外部法令遵循、機制程序及措施

訓練成效評估

確保受訓人員具備工作對應責任與能力



個資檔案安全管理 第22條

一般個資（非特種）也需要：

- 訂定紙本及可攜式設備/儲存媒體管制規範
- 媒介物銷毀、報廢或轉作他用之防範措施
- 備份個資應比照原件依辦法規定保護

若風險評估屬優先處理之高風險個資

得另加做： 加密  安全傳輸  安全銷毀
(即第11條第4、5、6款措施)

預告共通辦法修正重點

資訊安全強化措施

第23條 資通系統蒐集、處理或利用個人資料之額外安全要求



帳號管理與身分鑑別

使用者帳號管理、身分鑑別及保護機制



個資顯示隱碼機制

個人資料顯示時應採隱碼處理（如遮蔽部分欄位）



傳輸安全加密

網際網路傳輸採安全加密機制



存取控制與監控

個資檔案與資料庫存取控制及保護監控



防止外部入侵

防止外部網路入侵對策



異常使用監控

非法或異常使用行為之監控及因應機制



日誌留存至少6個月

訂定日誌記錄週期及留存政策，日誌至少留存6個月



定期備份

儲存之個人資料定期備份



系統安全測試

上線前及上線後持續辦理源碼檢測、弱點掃描、滲透測試

115年預告共通辦法重點

內部稽核與紀錄保存

第24條：內部稽核 第25條：個資使用紀錄及證據保存

內部稽核機制

第24條

每年至少辦理1次

稽核安全維護事項與管理機制之情形及成效

稽核機制內容

稽核項目及內容、執行合理頻率、結果紀錄

委外廠商亦應稽核

委託契約明確約定，每年至少1次稽核受託者

結果向最高主管報告

公務機關首長或非公務機關代表人、管理人

落實改善並保存紀錄5年

稽核結果紀錄應保存至少5年

紀錄及證據保存

第25條

應保存下列紀錄（保存期限至少5年）



個資蒐集、處理或利用紀錄

所有個資蒐用行為均需留存紀錄



落實安全維護措施之證據

執行各項安全措施的佐證文件或紀錄



當事人權利行使紀錄

查詢、更正、刪除等請求的處理紀錄

預告共通辦法修正重點

持續改善機制 + 合規行動指南

第26條：整體持續改善 快速自查清單



整體持續改善 第26條



矯正預防措施

安全維護計畫未落實時，應採取矯正及預防措施



定期檢視計畫合宜性

配合法令訂定或修正，參酌業務狀況及技術發展

必要時修正計畫

確保個資安全維護計畫持續與法規及現況吻合



合規行動速查清單

- ☐ 個資盤點清冊是否完整（7大項目）
- ☐ 個資安全維護計畫是否核定
- ☐ 專責人員及執行小組是否到位
- ☐ 年度風險評估是否完成
- ☐ 事故演練是否定期辦理
- ☐ 差異化教育訓練是否執行
- ☐ 系統上線前是否做安全測試
- ☐ 日誌是否留存至少6個月
- ☐ 內部稽核是否每年至少1次
- ☐ 各類紀錄是否保存至少5年

SECTION

組織架構修正

3.7 查核人員

新增條文

法源依據：個人資料檔案安全維護管理辦法草案 §17

查核人員（本條新增）

安維辦法草案§17

TIIPAS：2021+（新版）

指為辦理組織個人資料安全稽核，具有稽核之獨立性及專業性之人員。

組織應要求查核人員與執行個人資料管理之管理人員不得互相兼任，以確保查核獨立性與客觀性。

TIIPAS：2021（舊版）

本條新增，舊版無此條文

修正理由

對應安維管理辦法草案 §17，規定組織應確保管理專責人員及查核人員不得兼任，以確保查核獨立性與客觀性。

【立法目的】防範自查自核的利益衝突問題，確保個資稽核之公正性。

SECTION

教育訓練修正

7.2.2 / 7.2.3 / 7.2.4

強調「定期」辦理

法源依據：安維管理辦法草案 §8、§21

7.2.2~7.2.4

教育訓練相關條文修正（三條並列說明）

🌳 安維辦法草案§8、§21

TIIPAS：2021+（新版）

【7.2.2 基本教育訓練】

組織針對組織人員應「定期」提供必要之個人資料管理教育訓練。

【7.2.3 權責人員教育訓練】

組織應決定個人資料管理制度相關權責人員之必要能力與「定期」教育訓練需求，並規劃與執行。

【7.2.4 成果維持及改善措施】

組織應針對組織人員「定期」教育訓練成果建立紀錄與持續改善機制。

TIIPAS：2021（舊版）

【7.2.2 本教育訓練】

組織針對組織人員應提供必要之個人資料管理教育訓練。
（無「定期」要求）

【7.2.3 權責人員教育訓練】

...與教育訓練需求，並規劃與執行。（無「定期」字樣）

【7.2.4 成果維持及改善措施】

組織應針對組織人員教育訓練成果建立紀錄與持續改善機制。
（無「定期」字樣）

修正理由

對應安維管理辦法草案 §8、§21，明定人員應「定期」接受個資教育訓練。

應定妥適頻率辦理管理制度及差異化（通識及專業課程）之個人資料保護教育訓練，並規劃與執行。

確保訓練成果記錄之完整性與持續性，配合定期辦理要求，強化個資教育訓練之落實。

SECTION

記錄管理修正

7.3.3 使用紀錄與證據管理

7.3.4 系統日誌管理（新增）

🔗 法源依據：安維辦法草案 §25、§13；個資法 §30

7.3.3

使用紀錄與證據管理

🌳 安維辦法草案§25；個資法§30

TIIPAS：2021+（新版）

（更名為「使用紀錄與證據管理」）

其紀錄應包含：

- (1) 個人資料之蒐集、處理或利用紀錄。
- (2) 落實安全維護措施之證據。
- (3) 當事人權利行使之紀錄。
- (4) 保存前三款相關紀錄，應留存至少五年。

TIIPAS：2021（舊版）

（原條名：記錄管理）
組織為落實且證明其已符合本制度所要求之事項，應製作必要之紀錄文件並確立實施相關之管理程序。（無明確紀錄範圍及保存年限）

修正理由

對應安維管理辦法草案§25，明定紀錄範圍三類（蒐集/安全維護/當事人權利行使），對應個資法§30 保存期限規定，相關使用紀錄與證據應保存至少五年，以杜個資法民事請求權上的爭議。

系統日誌管理（本條新增）

安維辦法草案§13

TIIPAS：2021+（新版）

組織維運其資通系統蒐集、處理或利用個人資料，應執行：

- (1) 訂定日誌之記錄時間週期及留存政策，並保存適當時間。
- (2) 確保資通系統具備記錄特定事件之功能，並決定應記錄之特定資通系統事件。
- (3) 記錄資通系統管理者帳號所執行之各項功能。

TIIPAS：2021（舊版）

本條新增，舊版無此條文

修正理由

對應安維管理辦法草案 §13：

1. 確保可歸責性：涉個資之資通系統應採安全控制，利事故追蹤與鑑識。
2. 明確日誌規範：訂定記錄範圍、頻率及留存政策。
3. 強化行為監控：完整記錄重要系統事件（登入、權限變更、個資存取及刪除等），並針對特權帳號操作執行監控與記錄。

SECTION

個人資料管理範圍 與生命週期修正

8.2 / 8.4.3 / 8.4.6 / 8.4.7



納入管理之個人資料範圍

TPIPAS：2021+（新版）

組織應「界定」其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。

TPIPAS：2021（舊版）

組織應「識別」其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。

修正理由

文字微調（「識別」→「界定」）：組織應每年界定個人資料檔案之管理範圍，並建立個人資料盤點清冊及流程說明文件等文件化資訊，使用語更精確且符合實務。

處理 / 國際傳輸

TPIPAS：2021+（新版）

【8.4.3 處理】

- (3) 組織應訂定適當且合法之程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料，並留存相關作業之方法、時間、地點及證明。
- (4) 保存前三款相關紀錄。

TPIPAS：2021（舊版）

【8.4.3 處理】

- (3) 組織應訂定適當且合法程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料。
- (4) 保存前三款相關紀錄。（無留存銷毀方法/時間/地點/證明之要求）

修正理由

為落實個人資料生命週期管理，確保組織於資料銷毀或業務終止時之安全性與可追溯性，增列留存包含銷毀方法、時間、地點及銷毀證明之完整紀錄要求。

【8.4.6 國際傳輸】

組織於國際傳輸個人資料時，應確實檢視並遵循主管機關對國際傳輸之限制；於傳輸前應明確告知當事人擬傳輸之國家或區域，並保存相關紀錄。

【8.4.6 國際傳輸】

組織於國際傳輸個人資料時，其程序應合乎法律要求，並保存相關紀錄。（無明確告知當事人目的地之要求）

為強化個人資料於國際傳輸過程之保護，明定：

1. 傳輸前確實檢視主管機關跨境傳輸限制；
2. 傳輸前告知當事人擬傳輸之國家或區域，提升處理之透明性。

特種個人資料之蒐集、處理及利用

安維辦法草案§11

TPIPAS：2021+（新版）

- (2) 例外得蒐集、處理或利用特種個人資料時，「符合法律規定之特定情形」。
- (3) 針對載有特種個人資料之紙本或電子檔案，應採取適當之資料安全管理措施。
- (4) 保存前「三」款相關紀錄。

TPIPAS：2021（舊版）

- (2) 例外得蒐集、處理或利用特種個人資料時，係屬合乎法律要求。（無第3款）
- (3) 保存前二款相關紀錄。

修正理由

- 對應安維管理辦法草案 §11，鑑於特種個人資料高度敏感性，強化管理：
1. 訂定紙本及可攜式設備管制規範。
 2. 媒介物銷毀/報廢時應採適當防範措施。
 3. 備份個人資料應比照原件保護。
 4. 建置加密及安全傳輸措施。
 5. 落實安全銷毀，確保資料不可回復，並留存相關紀錄。

SECTION

安全管理措施 與事故緊急應變

8.7 / 8.10

法源依據：個資法§12、§48II

安全管理措施

🌳 個資法 §12文字修正

TPIPAS：2021+（新版）

組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止「個人資料被竊取、竄改、毀損、滅失或洩漏」之必要且適當之安全管理措施。

TPIPAS：2021（舊版）

...採取防止個人資料「外洩、滅失、毀損、竄改及其他侵害」之必要且適當之安全管理措施。

修正理由

個資法§12修法說明指出，為使所列事故類型及用語與新修正之個資法條文一致，修正為「竊取、竄改、毀損、滅失或洩漏」，刪除「其他侵害」一語（易生誤解），確保制度用語與法條完全對應。

事故之緊急應變

林 個資法§12、§48II

TIIPAS：2021+（新版）

- (1) 「知悉事故時」於適當時機及方式通知當事人。
- (2) 採取即時有效應變措施，防止事故擴大，並記載相關事實、影響、已採取之因應措施，保存相關紀錄。
- (3) 將事故即時通報「主管機關及其他依法令應通報之政府機關」。
- (4) 將事故即時通報授證機關。另：組織應將通知之內容、方式、時限與通報範圍、應變措施及紀錄保存，以供備查。

TIIPAS：2021（舊版）

- (1) 「查明後」於適當時機及方式通知當事人。
- (2) 防止組織所受損害擴大之方法。
- (3) 避免類似事件再次發生之方法。
- (4) 將事故即時通報「授證機關」。（無主動通報主管機關義務）

修正理由

因應個資法§12修訂：

1. 知悉時」即負通知義務，不以確認違法為前提（避免「查明時點爭議」）。
2. 應採即時應變措施，詳實記載，留存相關紀錄。
3. 配合個資法§48II，明定組織知悉個資事故且符合法定通報範圍時，負有主動通報主管機關之義務。
4. 確保事故可追溯性，作為釐清爭議與合規證明依據。

SECTION

特殊主體與政府存取 11.7 / 11.14 (新增)

法源依據：Global CBPR 計畫要求

未成年人之保護

Global CBPR

TIIPAS : 2021+ (新版)

組織於蒐集、處理或利用未成年人個人資料時，宜有較高之注意義務與安全管理措施，並應確認已採取措施足辨識：

- 未成年之法定代理人已有效代為同意，或
- 足辨識具其他符合法律規定之特定情形。

TIIPAS : 2021 (舊版)

組織於蒐集、處理或利用未成年人個人資料時，宜有較高之注意義務與安全管理措施。

修正理由

配合 Global CBPR 計畫要求更新：

- ① 強化安全管理機制：針對未成年人個資採取更嚴謹之安全控管措施。
- ② 確認同意有效性：採取有效措施確認取得法定代理人之同意，或確認符合其他法定特定情形，保障未成年人隱私權益。

應對政府存取資料（本條新增）

 Global CBPR

TIIPAS：2021+（新版）

組織應建立應對程序，回應要求揭露組織所持有之個人資料之國內、外司法或其他政府傳票、搜索令或其他命令，其內容應包括：

- (1) 確認要求與回應方式符合法律規定之特定情形。
- (2) 保存相關紀錄。

TIIPAS：2021（舊版）

本條新增，舊版無此條文

修正理由

配合 Global CBPR 計畫要求：明定組織應建立應對程序，以規範回應國內外司法或政府機關調閱個人資料之請求。確保調閱要求與回應方式均符合法律規定，並保存相關紀錄，確保透明性與可追溯性。

SECTION

附表A 安全管理措施修正

A8.7.1 ~ A8.8.2

法源依據：各條詳見安維管理辦法草案相關條文

存取控制

TIIPAS：2021+（新版）

1. 存取控制政策（明定應經權責人員核定，納入去識別化為帳號管理機制之一）
2. 帳號管理（增：至少每年定期清查帳號；特權帳號評估較高頻率清查；閒置超時自動登出）
4. 最小權限（增：識別業務涉及個資之人員，限縮授權範圍；大型非公務機關應採隱碼機制）
7. 資訊分享（增：保存分享方式與對象之紀錄）

TIIPAS：2021（舊版）

1. 存取控制實施（存取控制政策與存取實施機制）。
2. 帳號管理（含申請、開通、停用及刪除之程序；刪除/禁用逾期帳號、閒置帳號；閒置超時自動登出）
4. 最小權限（組織應落實最小權限的概念）
7. 資訊分享（確保存取授權符合政策規定）

修正理由

- ① 落實存取政策核定：納入去識別化；特權帳號至少每年清查，防止閒置帳號遭非法提權。
- ② 深化最小權限：識別業務涉及個資人員，限縮授權；配合安維辦法草案§23，大型非公務機關資通系統應採顯示隱碼機制。
- ③ 資訊分享紀錄留存：記載分享對象與方式，達成軌跡留存目標。

事件日誌與可歸責性（原：技術檢視）

安維辦法草案§23

TIIPAS：2021+（新版）

1. 記錄事件（增：監控影響「完整性」之事件，即未授權存取或修改）
2. 日誌紀錄之檢視、分析、通報（強化：調查結果報告權責主管）
3. 日誌紀錄之保存與維護（新增款）：訂定記錄時間週期及留存政策；日誌至少保存六個月；採存取控制防止日誌遭毀損或竄改，僅限授權人員存取。

TIIPAS：2021（舊版）

1. 稽核事件（監控影響個人資料機密性的事件）
2. 稽核紀錄的檢視、分析（定期檢視，通報給權責主管）（無日誌保存時間規定）

修正理由

- ① 更名：原「技術檢視」→「事件日誌與可歸責性」，對齊資通安全責任等級分級辦法及表十之資通系統防護基準。
- ② 強化完整性控管：未授權存取或惡意竄改均應納入稽核項目與監控機制。
- ③ 明定日誌留存：配合安維辦法草案§23，至少保存六個月，採存取控制防竄改，確保事故調查可追溯性。

識別鑑別 / 媒體安全

安維辦法草案§12

TIIPAS：2021+（新版）

【A8.7.3 識別鑑別】

2. 身分驗證管理：使用預設密碼登入系統時，應於登入後立即變更。身分驗證相關資訊不以明文傳輸。「應依需要制定並落實密碼規則與更新週期，落實密碼管理原則。」

【A8.7.4 媒體安全】

1. 媒體存取
- ~~2. 媒體標記（本款刪除）~~
2. 媒體儲存
3. 媒體傳輸
4. 媒體汰除

TIIPAS：2021（舊版）

【A8.7.3 識別鑑別】

2. 身分驗證管理：使用預設密碼登入系統時，應於登入後立即變更。身分驗證相關資訊不以明文傳輸。（無密碼複雜性/更新週期要求）

【A8.7.4 媒體安全】

1. 媒體存取
2. 媒體標記（組織應建立媒體標記之方法且進行適當標記）
3. 媒體儲存
4. 媒體傳輸
5. 媒體汰除

修正理由

因應安維管理辦法草案§12規定，增訂使用者設置符合一定複雜性要求之密碼，並定期更換，強化帳號安全性。（雖然新版NIST密碼認證指引，明確表示不再建議使用符號與數字的複雜組合設定，惟安維辦法仍有密碼複雜性規定）

鑑於數位化環境下，實體或邏輯標記已不足以防範未授權存取，現行實務已轉向以身分驗證與權限控管為核心之防禦機制，爰刪除「媒體標記」管理措施。

實體與環境安全 / 資訊傳輸

安維辦法草案§10

TIIPAS：2021+（新版）

【A8.7.5 實體與環境安全】
管理目標增列：...導致個人資料之洩漏「或毀損」。

1. 實體存取控制（增：明定資訊機房及檔案庫房，管控「進入」場所之「權限」）
2. 實體存取監視（增：建立人員及個人資料進出監視；制定合理保存期間，保存出入紀錄）

【A8.7.6 資訊傳輸】

2. 傳輸機密性：組織應採取適當措施確保個人資料傳輸的機密性，「並提供傳輸加密協定之設定截圖、加密證明文件或傳輸軌跡紀錄」。

TIIPAS：2021（舊版）

【A8.7.5 實體與環境安全】
管理目標：...導致個人資料之洩漏。（無「或毀損」）

1. 識別安全周界，管控進出
2. 定期檢視，建立監視與環境控管安全機制

【A8.7.6 資訊傳輸】

2. 傳輸機密性：組織應採取適當措施確保個人資料傳輸的機密性。（無加密證明要求）

修正理由

- ① 配合安維辦法草案§10：建立資訊機房、檔案庫房等敏感區域之實體安全周界。
- ② 落實進出管控：設置監視系統，控管進入人員權限。
- ③ 出入紀錄保存：確保發生爭議時具備充足資訊。

確保網路資料交換均具備安全加密（如TLS/SSL或其他具同等安全強度之加密機制），並要求組織提供實際加密行為軌跡或證明，強化稽核可追溯性。

系統與資訊完整性（整併A8.7.10）

安維辦法草案§9

TIIPAS：2021+（新版）

1. 安全性檢測
2. 稽核事件（已移至A8.7.2統一管理）
2. 惡意程式防護（強化）：資通系統出入端點部署有效防護機制；防毒軟體自動更新至最新病毒碼；啟用即時防護功能；定期完整系統掃描；依程序對偵測到之惡意程式進行隔離、刪除或適當處置。
3. 資通系統監看
4. 測試環境管理（新增）：區隔正式與測試環境；避免使用真實個人資料；如需使用需透過申請程序許可。

TIIPAS：2021（舊版）

1. 安全性檢測
2. 稽核事件：規劃資通系統有稽核特定事件之功能
3. 惡意程式防護：針對出入端點、工作站、伺服器、可攜式媒體等設備
4. 資通系統監看

修正理由

- ① 收攏稽核規範：原「稽核事件」移至A8.7.2統一管理（維持制度邏輯一致性）。
- ② 強化惡意程式防護：配合安維辦法草案§9，於出入端點部署有效防護，自動更新、即時防護、定期完整掃描。
- ③ 落實開發測試安全：測試環境隔離及避免使用真實個資（如需使用，須申請核准）。（原A8.7.10整併入本條）

系統發展生命週期階段（整併A8.7.9）

安維辦法草案§23

TIIPAS：2021+（新版）

管理目標：確保組織系統發展之安全需求（含機密性、完整性、可用性、遵循性）。

1. 運用SSDLC概念，合理滿足系統之安全需求
2. 資通系統發展及維運各階段導入適當安全措施（含帳號管理、身分鑑別、存取控制、隱碼及加密、日誌紀錄與監控、入侵防護及備份等）
3. 委外開發：安全需求納入委外契約
4. 對外服務系統：上線前辦理源碼檢測、弱點掃描及滲透測試，完成漏洞修補；系統上線後應持續辦理
5. 定期評估各項安全措施有效性，持續改善

TIIPAS：2021（舊版）

管理措施（原A8.7.8）：運用SSDLC概念之安全設計概念。
（原A8.7.9單獨一條）：組織資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求納入委外契約。

修正理由

1. 強化開發安全週期：導入SSDLC概念，系統自需求、設計至維運均符合機密性與完整性要求；委外開發應納入契約規範。
2. 落實預防性檢測：配合安維辦法草案§23，系統上線前執行源碼檢測、弱點掃描及滲透測試，完成修補。
3. 持續維護：系統上線後，仍應定期辦理安全性檢測與修補。

網路安全防護 & 新興技術風險管理（新增）

商業服務業及零售業個資
保護自評表查核項目14

TPIPAS：2021+（新版）

【A8.7.9 網路安全防護】

管理目標：確保組織網路系統有效應對威脅與風險。

管理措施：組織應制定有效網路安全防護政策，如定期維護網路設備軟硬體、韌體及元件，避免系統遭未經授權存取、入侵，損害資料之機密性、完整性與可用性，並保存相關更新之紀錄。

TPIPAS：2021（舊版）

（原A8.7.9「系統發展生命週期委外階段」已整併至A8.7.8，本條號由新條文接替）

修正理由

配合安維管理辦法草案§23，確保組織網路系統有效應對威脅與風險，增列本條管理規範。組織應制定網路安全防護政策，包含定期維護網路設備之軟硬體、韌體及相關元件，以避免遭未經授權之存取或入侵。

【A8.7.10 新興技術風險】

管理目標：確保組織於採納及運用新興技術時，能適當識別、評估並管理其所衍生之相關風險。

1. 雲端服務：就取得、環境設定及維運訂定規範（存取控制、加密、備份），並定期檢視與更新。
2. 人工智慧（AI）系統或服務：就取得、環境設定及使用管理訂定相關規範。

（原A8.7.10「獲得程序與系統文件」已整併至A8.7.7，本條號由新條文接替）

鑑於雲端運算及AI等新興技術廣泛應用，為確保組織有效識別並管理衍生之個資安全風險：

1. 雲端採用：訂定政策、確保個資安全（存取控制、加密、備份），記錄更新。
2. AI倫理與安全：開發、部署或採購AI時，建立規範、落實風險評估與控管。

資料可用性維護 / 保密契約

安維辦法草案§11、§22 / §7

TIIPAS：2021+（新版）

【A8.7.11 資料可用性維護】

管理目標：確保組織所留存之個人資料具實現蒐集目的所必要之可用性，減少因個人資料滅失或無法存取致當事人受侵害之風險。

管理措施：訂定資料備份之政策，決定備份之合理頻率，並定期測試備份，以驗證備份媒體之可靠性及資訊之完整性。備份資料應比照原件予以保護。

~~2.系統備援（刪除）~~

【A8.8.2 保密契約】

管理措施：...並確保於人員離職或職務變動時，異動人員有義務配合個人資料媒介物之交接、返還或資料刪除措施；同時，異動人員於合理期間內仍須負有保密義務。

TIIPAS：2021（舊版）

【A8.7.11 營運持續計畫】

管理目標：確保組織業務運作正常，訂定最大可容忍中斷時間（MTPD）與最低可接受服務水準。

- 1.系統備份（含碼與資料，並定期測試）
- 2.系統備援（可容忍中斷時間，由備援設備提供最低服務水準）

【A8.8.2 保密契約】

管理措施：...並確保於人員離職或職務變動後適當期間內仍負有保密義務。（無交接/返還/刪除義務）

修正理由

配合安維辦法草案§11、§22，將重點調整為針對個資之「備份」管理：目標改為確保個資可用性；刪除「系統備援」相關規範，聚焦個人資料備份政策；備份資料應比照原件保護。

配合安維辦法草案§7：針對職務上具取得個資可能性之人員，約定保密義務。明定人員異動（含離職、調職）時，應履行個資媒介物之交接、返還或資料刪除義務，防止個資保護真空期。



Thank you

