附表 B：TPIPAS 規範修正對照表

修正與公告日期：2021 年 12 月 30 日

TPIPAS 與其他規範對照表

臺灣個人資料保護與管理制度（TPIPAS）規範自 2012 年 9 月 4 日制定公告後，嗣於 2016 年 5 月 19 日配合我國個人資料保護法修法（該法係於 2015 年 12 月 30 日修正、2016 年 3 月 15 日正式施行）修正規範並公告沿用至今。嗣於今年考量國內企業或組織內部常已建置相關管理制度，如：ISO 品質管理或資訊安全管理系統，為利各管理系統、制度整合或其他相關需求，爰配合 ISO 國際標準自 2012 年發展出之撰寫管理系統標準（management system standard, MSS）指導綱要，採用 Annex SL（high-level structure）架構，規劃調整 TPIPAS 規範。

TPIPAS :2021	**TPIPAS：2016**	**ISO 9001:2015**	**ISO 27001**	**ISO 27701**	**BS 10012 2017 +A1 2018**
0.簡介	0.前言	簡介	簡介	簡介	0.前言
1.適用範圍	1.適用範圍	1.範圍	1.適用範圍	1.適用範圍	1.範圍
2.版本標示	2.版本標示	2.參考標準	2.引用標準	2.引用標準	2.參考規範
3.用語與定義	3.用語與定義	3.名詞和定義	3.用語及定義	3.用語、定義與縮寫 4.一般要求	3.名詞、定義與縮寫
4.組織環境（新增）	（原無）	4.組織處境	4.組織全景	5.2 組織全景	4.組織全景
5.管理責任（調整）	4.要求事項 ➢ 4.2、4.4.5 5.管理責任 ➢ 5.1、5.2、5.3	5.領導	5.領導作為	5.3 領導作為	5.領導作為
6.制度規劃（新增）	4.要求事項 ➢ 4.1、4.3、4.4.3	6.規劃	6.規劃	5.4 規劃	6.規劃
7.支援（調整）	4.要求事項 ➢ 4.4.4、4.6 7.文件及紀錄之控管	7.支援	7.支援	5.5 支援	7.支援

TPIPAS :2021	TPIPAS：2016	ISO 9001:2015	ISO 27001	ISO 27701	BS 10012 2017 +A1 2018
8.個人資料管理制度之實施（調整）	4.要求事項 ➢ 4.4.1-4.4.3、4.4.6、4.5	8.營運	8.運作	5.6 運作	8.運作
9.績效評估（調整）	6.有效性量測 8.內部評量 9.1 定期檢視	9.績效評估	9.績效評估	5.7 績效評估	9.績效評估
10.改善（調整）	9.改善	10.改善	10.改善	5.8 改善	10.改善
11.個人資料管理制度實施指引	（原無）			6.與 ISO 27002 相關的 PIMS 指引 7.對 PII 控制者於 ISO 27002 附加指引 8.對 PII 處理者於 ISO 27002 附加指引	

個人資料保護法施行細則第 12 條適當安全維護措施與 TPIPAS 規範對照表

個資法施行細則第 12 條	TPIPAS:2021
1.配置管理之人員及相當資源	7.1 資源
2.界定個人資料之範圍	8.2 納入管理之個人資料範圍
3.個人資料之風險評估及管理機制	6.3 因應風險之規劃 8.3 風險管控措施
4.事故之預防、通報及應變機制	8.10 事故之緊急應變
5.個人資料蒐集、處理及利用之內部管理程序	8 管理制度之實施
6.資料安全管理及人員管理	8.7 安全管理措施 8.8 組織人員之監督
7.認知宣導及教育訓練	5 管理責任 7.2 教育訓練
8.設備安全管理	8.7 安全管理措施
9.資料安全稽核機制	8.7 安全管理措施 9.2 內部評量
10.使用紀錄、軌跡資料及證據保存	7.3 文件及紀錄之控管
11.個人資料安全維護之整體持續改善	10.改善

TPIPAS:2021 與 2016 年版規範對照表

TPIPAS:2021	TPIPAS：2016
0 簡介	0 簡介
1 適用範圍	1 適用範圍
2 版本標示	2 版本標示
3 用語與定義	3 用語與定義
4 組織環境 4.1 內外部議題 4.2 利害關係人需求	（本條新增）
5 管理責任 5.1 最高管理階層 5.2 個人資料保護管理政策 5.3 權限與責任分工 5.4 管理代表 5.5 個人資料管理人員	4 要求事項 4.2 個人資料保護管理政策 4.4.5 權限與責任分工 5 管理責任 5.1 最高管理階層 5.2 管理代表 5.3 個資管理人員
6 制度規劃 6.1 總則 6.2 個人資料保護管理手冊 6.3 因應風險之規劃	4 要求事項 4.1 一般要求 4.3 個人資料保護管理手冊 4.4.3 風險管控措施
7 支援 7.1 資源 7.2 教育訓練 7.3 文件及紀錄之控管 7.4 溝通或傳達	4 要求事項 4.4.4 資源管理 4.6 教育訓練與基礎設施 7 文件及紀錄之控管 7.1 文件及紀錄之範圍 7.2 文件管理 7.3 紀錄管理
8 個人資料管理制度之實施 8.1 識別法令及其相關規範 8.2 納入管理之個人資料範圍 8.3 風險管控措施之實施 8.4 個人資料之蒐集、處理與利用 8.5 當事人之相關權利 8.6 維持個人資料之正確性 8.7 安全管理措施 8.8 組織人員之監督	4 要求事項 4.4.1 識別法令及其他相關規範 4.4.2 納入管理之個人資料範圍 4.4.3 風險管控措施 4.4.6 事故之緊急應變 4.5 管理制度之實施

TPIPAS:2021	TPIPAS：2016
8.9 委託蒐集、處理或利用個人資料之監督 8.10 事故之緊急應變	
9 績效評估 9.1 有效性量測 9.2 內部評量 9.3 定期檢視	6 有效性量測 8 內部評量 9.改善 9.1 定期檢視
10 改善 10.1 總則 10.2 矯正措施 10.3 預防措施	9.改善 9.2 矯正及預防措施
11 個人資料管理制度實施指引 11.1 總則 11.2 從設計與預設階段著手隱私保護 11.3 生物特徵個人資料 11.4 風險處置 11.5 當事人同意 11.6 當事人權利 11.7 未成年人之保護 11.8 無障礙 11.9 Cookie 11.10 暫存檔之處理 11.11 自動化決策與剖繪 11.12 國際傳輸 11.13 委託蒐集、處理或利用個人資料之監督	（本條新增）