延宇資訊股份有限公司

「資訊安全暨隱私資訊管理系統」
PIMS 適用性聲明書

機密等級：一般

編號：YAN-PIMS-01-02

版本編號：1.1

修定日期：2024/01/31

使用本文件前, 如對版本有疑問, 請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說明	核准者
1.0	2023/03/01	梁維志	新增	楊文欽
1.1	2024/01/31	黃韋霖	刪除關於 PII 處理者之控制措施。	梁維志

本程序書由資訊安全執行小組（個人資料保護推動執行小組）負責維護。

本資料為延宇資訊股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

適用性聲明

一、 適用範圍：

本公司個人隱私資料管理系統驗證範圍：

包括在人事、差勤、駐點工程師服務流程之個人資料隱私保護管理作業。

The provision of personal information management including personal information file collection, processing, and using in the within Personnel, attendance, and onsite service management process.

二、 控制措施對應程序文件：

ISO / IEC 27701:2019

章節	敘述	適用性		不適用理由/參考文件
		適用	不適用	
附錄 A	PIMS 特定參考控制目標與控制措施(PII 控制者)			
A.7.2	蒐集與處理的條件 判定並文件化該處理的合法性，具有適用司法管轄區域法律的依據，以及明確定義的合法目的。			
A.7.2.1	識別與文件化特定目的 組織應識別及文件化PII處理的特定目的。	V		PIMS-L2-02 個人資料蒐集管理程序書 YAN-PIMS-02-03 員工個資處理資程序書
A.7.2.2	識別法律基礎 組織應決定、文件化並遵守已識別特定目的而處理PII的相關合法基礎。	V		PIMS-L2-02 個人資料蒐集管理程序書
A.7.2.3	決定同意書取得時機 組織宜確定並文件化一項過程，該過程可以證明由PII當事人取得處理PII的同意方式與時機。	V		PIMS-L2-02 個人資料蒐集管理程序書
A.7.2.4	取得與記錄同意書 組織應根據文件化流程取得並記錄PII當事人的同意。	V		PIMS-L2-02 個人資料蒐集管理程序書
A.7.2.5	隱私衝擊評估 當計劃進行新的PII處理或對PII的現有處理進行變更時，組織應評估需求，並於適當時進行隱私影響評估。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書
A.7.2.6	與PII處理者簽訂合約 組織應與採用之PII處理者簽訂書面協議，並應確保於PII處理者協議中，載明附錄B中適當控制措施的施行。	V		PIMS-L2-03 個人資料處理與利用管理程序書 YAN-ISMS-02-10 資訊委外管理程序書
A.7.2.7	PII共同控制者 組織應確定與任何PII共同控制者一起處理PII時的各自角色和職責(包括PII保護和安全要求)。		V	延宇無任何 PII 聯合控制者處理之行為與作業之需求
A.7.2.8	PII處理紀錄 組織應決定與安全地維護符合義務的PII處理紀錄。	V		PIMS-L2-03 個人資料處理與利用管理程序書
A.7.3	對 PII 當事人的義務 確保提供PII當事人適切資訊，說明有關其PII的處理以及符合適用於相關PII處理的義務。			
A.7.3.1	判定與符合對 PII 當事人的義務 組織應確定並文件化其對PII當事人在處理PII方面的法律，法規和業務義務，並提供履行這些義務的方式。	V		PIMS-L2-04 當事人權利管理程序書

章節	敘述	適用性		不適用理由/參考文件
		適用	不適用	
A.7.3.2	決定PII當事人資訊 組織應確定並文件化要提供給PII當事人資訊，有關其PII的處理以及此類資訊的提供時機。	V		PIMS-L2-04 當事人權利管理程序書
A.7.3.3	提供資訊予PII當事人 組織應提供PII當事人清晰且易於存取資訊，以識別PII控制者並描述其PII的處理。	V		PIMS-L2-04 當事人權利管理程序書
A.7.3.4	提供修訂或撤銷同意書之機制 組織應為PII當事人提供修訂或撤回其同意的機制。	V		PIMS-L2-04 當事人權利管理程序書
A.7.3.5	提供拒絕個資處理之機制 組織應提供機制，讓 PII 當事人得以拒絕其 PII 的處理。	V		PIMS-L2-04 當事人權利管理程序書
A.7.3.6	存取、更正與/或刪除 組織應實作政策，程序和/或機制，來履行其對PII當事人存取，更正與/或刪除其PII的義務。	V		PIMS-L2-04 當事人權利管理程序書
A.7.3.7	控制者通知第三方的義務 組織應將已分享的PII相關的修訂，撤銷或拒絕通知共享的第三方，並實作適當的政策，程序和/或機制來處置。	V		PIMS-L2-03 個人資料處理與利用管理程序書
A.7.3.8	提供處理之PII的複本 組織應可依PII當事人請求，提供PII複本。	V		PIMS-L2-02 個人資料蒐集管理程序書
A.7.3.9	處理請求 組織應界定並文件化政策和程序，以處理和回應PII當事人的合法請求。	V		PIMS-L2-02 個人資料蒐集管理程序書
A.7.3.10	自動決策 組織應識別並說明僅依 PII 的自動處理而產生有關 PII 當事人決策的相關義務，包括法律義務。		V	延宇無 PII 有關之自動化處理之相關操作
A.7.4	隱私設計與預設 為確保流程和系統的設計，使蒐集和處理(包括利用、揭露、保留、傳輸和汰除)僅限於已識別目的所需。			
A.7.4.1	蒐集限制 組織應限制PII的蒐集，為與已識別目的相關，成比例且必要的極小化。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-02 個人資料蒐集管理程序書
A.7.4.2	處理限制 組織應限制其PII的處理對於已識別目的來說，為適當、相關且必要。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-03 個人資料處理與利用管理程序書
A.7.4.3	正確與品質 組織應確保並文件化在PII的整個生命週期中，PII的正確性，完整性和最新為其處理目的所必須。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-02 個人資料蒐集管理程序書

章節	敘述	適用性		不適用理由/參考文件
		適用	不適用	
A.7.4.4	PII極小目標 組織應界定並文件化其資料最小化目標，以及用於符合目標的機制(如去識別化)。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-02 個人資料蒐集管理程序書
A.7.4.5	PII處理後之去識別化與刪除 組織應於已識別目的不再需要原始PII時，刪除PII或以無法再識別或重新識別PII當事人的形式提供。一旦出於確定的目的不再需要原始的PII。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-03 個人資料處理與利用管理程序書
A.7.4.6	暫存檔 組織應確保因處理PII而產生的暫存檔，依據文件化程序所指定的期限汰除(例如抹除或銷毀)。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-03 個人資料處理與利用管理程序書 ISMS-2-07 通信與作業管理程序書 YAN-ISMS-02-02 文件暨紀錄管理程序書
A.7.4.7	保存 組織保存PII的時間不應超過其處理目的所需的時間。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-03 個人資料處理與利用管理程序書 ISMS-2-07 通信與作業管理程序書 YAN-ISMS-02-02 文件暨紀錄管理程序書 YAN-ISMS-03-05 資訊備份管理說明書
A.7.4.8	汰除 組織應具有PII汰除的文件化政策、程序和/或機制。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-03 個人資料處理與利用管理程序書
A.7.4.9	傳輸控制措施 組織應對透過資料傳輸網路進行傳輸(例如發送到另一個組織)的PII設計適當的控制措施，以確保資料到達預期的目的地。	V		PIMS-L2-01 個人資料識別與隱私設計管理程序書 PIMS-L2-03 個人資料處理與利用管理程序書 YAN-ISMS-02-02 文件暨紀錄管理程序書 YAN-ISMS-03-02 網路及系統安全管理說明書
A.7.5	PII 分享、轉移與揭露 根據適用的義務確定是否分享PII，並文件化何時將其分享、轉移給其他司法管轄區域或第三方，和/或揭露PII。			
A.7.5.1	識別司法管轄區域間 PII 轉移基礎 組織應識別並文件化司法管轄區域間PII轉移的相關基礎。		V	本公司無司法管轄區域間 PII 轉移。
A.7.5.2	PII可轉移的國家與國家組織 組織應指出並文件化可能將PII轉移到的國家與國家組織。		V	延宇無 PII 轉移至其他國家或國際組織之需求。
A.7.5.3	PII轉移紀錄 組織應記錄與第三方間的PII轉移，並確保與第三方的合作以支援未來與PII當事人義務有關的請求。	V		PIMS-L2-03 個人資料處理與利用管理程序書 YAN-ISMS-02-02 文件暨紀錄管理程序書 YAN-ISMS-03-02 網路及系統安全管理說明書

章節	敘述	適用性		不適用理由/參考文件
		適用	不適用	
A.7.5.4	PII揭露第三方之紀錄 組織應記錄對第三方的PII揭露，包括已揭露的PII，對象與時間。	V		PIMS-L2-03 個人資料處理與利用管理程序書 YAN-ISMS-02-02 文件暨紀錄管理程序書 YAN-ISMS-03-02 網路及系統安全管理說明書