延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

資訊安全暨隱私資訊管理制度內部稽核表

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日
查核項目 ISMS PIMS	敘　　述			符合性 符合	符合性 不符合	參考文件	補充說明
CH4 5.2	組織全景						
4.1 5.2.1	瞭解組織及全景 組織應決定與其目的有關且影響達成資訊安全系統預期成果能力者之內外部議題			V		YAN-ISMS-02-15 資訊安全全景與關注方規劃程序書	
4.2 5.2.2	瞭解關注方之需要與期望 (a)組織決定資安管理系統關注方 (b)組織應有對應的要求事項				V	YAN-ISMS-02-15 資訊安全全景與關注方規劃程序書	抽查 YAN-ISMS-04-52 組織全景分析表(YAN-ISMS-G-52-11506-01) date115/06/15 本公司同仁對差勤系統之影響說明，已於 113 年完成更換 104 Pro 差勤系統關注者識別及期望與需求分析之內容應就目前使用之差勤系統之反應進行分析
4.3 5.2.3	決定資訊安全管理系統之範圍			V		YAN-ISMS-01-02 適用性聲明書 YAN-ISMS-02-15 資訊安全全景與關注方規劃程序書	
4.4 5.2.4	資訊安全管理系統			V		YAN-ISMS-02-15 資訊安全全景與關注方規劃程序書	
CH5 5.3	領導作為						

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
5.1 5.3.1	領導及承諾 (a)管理階層確保已建立資訊安全政策與資訊安全目標並遵循組織策略方向 (b)確保管理系統要求事項整合過程之紀錄 (c)管理階層提供 ISMS 所需資源支持 (d)管理階層傳達 ISMS 有效性與重要性並確保達成預期效果 (e)管理階層角色適用其責任範圍，參與並支持	V		YAN-ISMS-02-01 資訊安全暨隱私保護組織程序書 YAN-ISMS-01-01 資訊安全政策	
5.2 5.3.2	政策 管理階層應確保建立標準涵蓋之資訊安全政策	V		YAN-ISMS-01-01 資訊安全政策	
5.3 5.3.3	組織角色、責任及權限 組織內部角色相關責任及權限之指派與傳達，並回報落實績效	V		YAN-ISMS-02-01 資訊安全暨隱私保護組織程序書	
CH6 5.4	規劃				
6.1.1 5.4.1.1	一般要求 於規劃資訊安全管理系統時，組織應考量 4.1 所提及之議題及 4.2 所提及之要求事項，並決定需因應之風險及機會。	V		YAN-ISMS-02-04 風險評鑑與管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
6.1.2 5.4.1.2	資訊安全風險評鑑 (a)建立及維持包括下列準則之資訊安全風險準則。 (1)風險接受準則。 (2)履行資訊安全風險評鑑之準則。 (b)確保重複之資訊安全風險評鑑產生一致、有效及適於比較之結果 (c)識別資訊安全風險 (1)應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與漏失資訊之機密性、完整性及可用性相關聯之風險。 (2)識別風險擁有 (d)分析資訊安全風險。 (1)評鑑若 6.1.2(c)(1)中所識別之風險實現時，可能導致之潛在後果。 (2)評鑑 6.1.2(c)(1)中所識別之風險發生的實際可能性。	V		YAN-ISMS-02-04 風險評鑑與管理程序書	
	(3)決定風險等級。 (e)評估資訊安全風險。 (1)以 6.1.2(a)中所建立之風險準則，比較風險分析結果。 (2)訂定已分析風險之風險處理優先序。	V		YAN-ISMS-02-04 風險評鑑與管理程序書	
6.1.3 5.4.1.3	資訊安全風險處理 組織應定義並應用資訊安全風險處理過程	V		YAN-ISMS-02-04 風險評鑑與管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
6.2 5.4.2	資安目標及達成規劃 組織應於各相關部門及層級建立資訊安全目標。資訊安全目標應滿足下列事項。 (a)與資訊安全政策一致。 (b)可量測(若可行時)。 (c)考量適用之資訊安全要求事項，以及風險評鑑及風險處理之結果。 (d)被傳達。 (e)於適當時，更新之。 組織應保存關於資訊安全目標之文件化資訊。 於規劃如何達成資訊安全目標時，組織應決定下列事項。 (f)待辦事項。 (g)所需資源。 (h)負責人員。 (i)完成時間。 (j)結果之評估方式。	V		YAN-ISMS-02-01 資訊安全暨隱私保護組織程序書	
CH7 5.5	支援				
7.1 5.5.1	資源 組織應提供 PDCA 過程所需的資源	V		YAN-ISMS-02-05 人員安全與教育訓練程序	
7.2 5.5.2	能力 人員必要能力的評估、養成、強化皆須保存適切的文件化資訊作為勝任之證據呈現	V		YAN-ISMS-02-05 人員安全與教育訓練程序	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
7.3 5.5.3	認知 人員任職相關遵循守則應提及資安政策、有效貢獻、未遵循 ISMS 要求事項之可能後果，並定期宣導	V		YAN-ISMS-02-05 人員安全與教育訓練程序	
7.4 5.5.4	溝通或傳達 組織應決定內外部溝通傳達之需要與管道，其過程文件化	V		YAN-ISMS-02-05 人員安全與教育訓練程序	
7.5.2 5.5.5.2	制定及更新 制定及更新文件化資訊應確保符合標準要求，包含：識別敘述、格式、合宜性與適切性的審查核准	V		YAN-ISMS-02-02 文件暨紀錄管理程序書	
7.5.3 5.5.5.3	文件化資訊之控制 確保文件之使用、派送、保存、變更等相關作業皆受到適切保護	V		YAN-ISMS-02-02 文件暨紀錄管理程序書	
CH8 5.6	運作				
8.1 5.6.1	運作之規劃及控制 組織應規劃、實作及控制達成資訊安全要求事項所需之過程，並實作 6.1 中所決定之行動。組織亦應實作各項計畫，以達成 6.2 中所決定之資訊安全目標。	V		YAN-ISMS-02-04 風險評鑑與管理程序書	
8.2 5.6.2	資訊安全風險評鑑 組織應依規劃之期間，或當提議或發生重大變更時，考量 6.1.2(a)所建立之準則，執行資訊安全風險評鑑。	V		YAN-ISMS-02-04 風險評鑑與管理程序書	
8.3 5.6.3	資訊安全風險處理 組織應實作資訊安全風險處理計畫。	V		YAN-ISMS-02-04 風險評鑑與管理程序書	
CH9 5.7	績效評估				

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
9.1 5.7.1	監督、量測、分析、評估 組織應定期檢視量測與監督事項，並確認過程所需之時間、資源、角色指派等文件化證據呈現	V		YAN-ISMS-02-04 風險評鑑與管理程序書	
9.2 5.7.2	內部稽核 組織應定期進行內部稽核確認要求事項是否有效實作及維持稽核人員條件要求，且應產出稽核計畫及相關報告	V		YAN-ISMS-02-13 資訊安全稽核作業程序	
9.3 5.7.3	管理審查 組織於規劃期間定期進行審查資訊安全管理系統之行動，確保合宜性、適切及有效性 管理審查應包含標準要求之輸入輸出要求項目，以對照是否符合資訊安全目標及計畫	V		YAN-ISMS-02-13 資訊安全稽核作業程序	
CH10 5.8	改善				
10.1 5.8.1	不符合項目與矯正措施 對於不符合項目應採取矯正行動並處理其後果以避免再發事件。 評估及審查矯正措施行動的有效性，必要時採取應對之變更，過程皆須保留文件化資訊	V		YAN-ISMS-02-14 矯正及預防管理程序書	
10.2 5.8.2	持續改善 組織對於事件矯正預防處理應持續改進資訊安全管理系統的合宜性、適切、有效性	V		YAN-ISMS-02-14 矯正及預防管理程序書	
A.5	Organizational controls 組織控制措施				

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.5.1	資訊安全政策 控制措施：資訊安全政策及主題特定政策應予以定義、由管理階層核 可、發布、傳達予相關人員及相關關注方，且其係知悉，並依規劃期間及發生重大變更時審查。	V		YAN-ISMS-01-01 資訊安全政策	
6.2.1.1	隱私保護政策 無論藉由制定單獨隱私政策，或藉由增強資訊安全政策，組織宜就關於支援及承諾達成對適用之 PII 保護法律及/或法規，以及對組織與其合作夥伴、分包者及適用之第三方(客戶、供應者等)間議定的契約條款(宜明確配置其間之責任)等之遵循性，提出聲明。	V		YAN-PIMS-01-01 隱私保護政策	
6.2.1.2	資訊安全政策之審查 適用CNS27002之5.1.2中所述的控制措施、實作指引及其他資訊。	V		YAN-PIMS-01-01 隱私保護政策	
A.5.2 6.3.1.1	資訊安全之角色及責任 控制措施：應依組織需要，定義並配置資訊安全之角色及責任。	V		YAN-ISMS-02-01 資訊安全暨隱私保護組織程序書	
A.5.3 6.3.1.2	職務區隔 控制措施：衝突之職務及衝突的責任範圍應予以區隔。	V		YAN-ISMS-02-01 資訊安全暨隱私保護組織程序書	
A.5.4 6.4.2.1	管理階層責任 管理階層應要求所有人員，依組織所建立資訊安全政策、主題特定政策及程序，實施資訊安全。	V		YAN-ISMS-02-05 人員安全與教育訓練程序書 YAN-ISMS-02-10 資訊委外管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.5.5 6.3.1.3	與權責機關之連繫 控制措施：組織應建立並維持與相關權責機關之聯繫。	V		YAN-ISMS-02-05 人員安全與教育訓練程序書 YAN-ISMS-02-15 資訊安全全景與關注方規劃程序書	
A.5.6 6.3.1.4	與特殊關注群組之聯繫 控制措施：組織應建立並維持與各特殊關注群組或其他各專家安全論壇及專業協會之聯繫。	V		YAN-ISMS-02-05 人員安全與教育訓練程序書 YAN-ISMS-02-15 資訊安全全景與關注方規劃程序書	
A.5.7	威脅情資 控制措施：應蒐集並分析與資訊安全威脅相關之資訊，以產生威脅情資。	V		YAN-ISMS-03-11 威脅情資管理作業說明書	
A.5.8 6.11.1.1 6.3.1.5	專案管理之資訊安全 控制措施：資訊安全應整合入專案管理中。	V		YAN-ISMS-02-04 風險評鑑與管理程序書 YAN-ISMS-03-10 資訊安全風險評鑑說明書	
A.5.9 6.5.1.1 6.5.1.2	資訊及其他相關聯資產之清冊 控制措施：應識別、書面記錄及實作對處置資訊及其他相關聯資產之可接受使用的規則及程序。	V		YAN-ISMS-02-03 資訊資產管理程序書	
A.5.10 6.5.1.3 6.5.2.3	可接受使用資訊及其他相關聯資產 控制措施：應識別、書面記錄及實作對處置資訊及其他相關聯資產之可接受使用的規則及程序。	V		YAN-ISMS-02-03 資訊資產管理程序書	
A.5.11 6.5.1.4	資產之歸還 控制措施：適切時，人員及其他關注方於其聘用、契約或協議變更或終止時，應歸還其持有之所有組織資產。	V		YAN-ISMS-02-03 資訊資產管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.5.12 6.5.2.1	資訊之分類分級 控制措施：資訊應依組織之資訊安全需要，依機密性、完整性、可用性及相關關注方要求事項分類分級。	V		YAN-ISMS-02-03 資訊資產管理程序書	
A.5.13 6.5.2.2	資訊之標示 控制措施：應依組織所採用之資訊分類分級方案，發展及實作一套適切的資訊標示程序。	V		YAN-ISMS-02-03 資訊資產管理程序書	
A.5.14 6.10.2.1 6.10.2.2 6.10.2.3	資訊傳送 控制措施：應備妥資訊傳送規則、程序或協議，用於組織內及組織與其他各方間之所有型式的傳送設施。	V		YAN-ISMS-02-07 通信與作業管理程序書	
A.5.15 6.6.1.1 6.6.1.2	存取控制 控制措施：應依營運及資訊安全要求事項，建立並實作對資訊及其他相關聯資產之實體及邏輯存取控制的規則。	V		YAN-ISMS-02-07 通信與作業管理程序書 YAN-ISMS-02-08 存取控制程序書	
A.5.16 6.6.2.1	身分管理 應管理身分之整個生命週期。		V	YAN-ISMS-02-08 存取控制程序書 YAN-ISMS-03-04 帳號及通行密碼管理說明書 YAN-ISMS-03-03 電子郵件帳號管理說明書	同仁吳○景於 115/2/28 離職，YAN-ISMS-04-37 系統使用權限管理名冊(日期 115/6/14 未註記停用日期)
A.5.17 6.6.2.4 6.6.3.1 6.6.4.3	鑑別資訊 控制措施：鑑別資訊之配置及管理應由管理過程控制，包括告知人員關於鑑別資訊的適切處理。	V		YAN-ISMS-03-04 帳號及通行密碼管理說明書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.5.18 6.6.2.2 6.6.2.5 6.6.2.6	存取權限 控制措施：應依組織之存取控制的主題特定政策及規則，提供、審查、修改及刪除對資訊及其他相關聯資產之存取權限。	V		YAN-ISMS-02-08 存取控制程序書 YAN-ISMS-03-04 帳號及通行密碼管理說明書	
A.5.19 6.12.1.1	供應者關係中之資訊安全 控制措施：應定義並實作過程及程序，管理與供應者產品或服務之使用相關聯的資訊安全風險。	V		YAN-ISMS-02-10 資訊委外管理程序書	
A.5.20 6.12.1.2	於供應者協議中闡明資訊安全 控制措施：應依供應者關係之型式，建立相關的資訊安全要求事項，並與各供應者議定。	V		YAN-ISMS-02-10 資訊委外管理程序書	
A.5.21 6.12.1.3	管理 ICT 供應鏈中之資訊安全 控制措施：應定義並實作過程及程序，管理與 ICT 產品及服務供應鏈相關聯之資訊安全風險。	V		YAN-ISMS-02-10 資訊委外管理程序書	
A.5.22 6.12.2.1 6.12.2.2	供應者服務之監視、審查 及變更管理 控制措施：組織應定期監視、審查、評估及管理供應者資訊安全實務作法及服務交付之變更。	V		YAN-ISMS-02-10 資訊委外管理程序書	
A.5.23	使用雲服務之資訊安全 控制措施：應依組織之資訊安全要求事項，建立獲取、使用、管理及退出雲端服務的過程。	V		YAN-ISMS-02-10 資訊委外管理程序書	
A.5.24 6.13.1.1	資訊安全事故管理規劃及準備 控制措施：組織應藉由定義、建立並溝通或傳達資訊安全事故管理過程、角色及責任，規劃並準備管理資訊安全事故。	V		YAN-ISMS-02-11 安全事件管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.5.25 6.13.1.4	資訊之評鑑及決策 控制措施：組織應評鑑資訊安全事件，並判定是否將其歸類為資訊安全事故。	V		YAN-ISMS-02-11 安全事件管理程序書	
A.5.26 6.13.1.5	對資訊安全事故之回應 控制措施：應依書面記錄程序，回應資訊安全事故。	V		YAN-ISMS-02-11 安全事件管理程序書	
A.5.27 6.13.1.16	由資訊安全事故中學習 控制措施：應使用由資訊安全事故中所獲得之知識，強化及改善資訊安全控制措施。	V		YAN-ISMS-02-11 安全事件管理程序書	
A.5.28 6.13.1.7	證據之收集 控制措施：組織應建立並實作程序，用以識別、蒐集、獲取及保存與資訊安全事件相關之證據。	V		YAN-ISMS-02-11 安全事件管理程序書	
A.5.29 6.14.1.1 6.14.1.2 6.14.1.3	中斷期間之資訊安全 控制措施：組組織應規劃，如何於中斷期間維持資訊安全於適切等級。	V		YAN-ISMS-02-12 營運持續運作管理程序書	
A.5.30	營運持續之ICT備妥性 控制措施：應依營運持續目標及 ICT 持續之要求事項，規劃、實作、維護及測試 ICT 備妥性。	V		YAN-ISMS-02-12 營運持續運作管理程序書	
A.5.31 6.15.1.1 6.15.1.5	法律、法令、法規及契約要求事項 控制措施：應識別、書面記錄及保持更新資訊安全相關法律、法令、法規及契約之要求事項，以及組織為符合此等要求事項的作法。	V		YAN-ISMS-02-02 文件暨紀錄管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.5.32 6.15.1.2	智慧財產權 控制措施：組織應實作適切程序，以保護智慧財產權。	V		YAN-ISMS-03-01 資訊資產管理說明書 YAN-ISMS-02-13 資訊安全稽核作業程序書	
A.5.33 6.15.1.3	紀錄之保護 控制措施：應保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。	V		YAN-ISMS-02-02 文件暨紀錄管理程序書	
A.5.34 6.15.1.4	隱私及 PII 保護 控制措施：組織應依適用之法律、法規及契約的要求事項，識別並符合關於隱私保護及 PII 保護之要求事項。	V		YAN-ISMS-02-05 人員安全與教育訓練程序書 YAN-ISMS-02-13 資訊安全稽核作業程序書	
A.5.35 6.15.2.1	資訊安全之獨立審查 控制措施：應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全的作法及其實作(包括人員、過程及技術)。	V		YAN-ISMS-02-13 資訊安全稽核作業程序書	
A.5.36 6.15.2.2 6.15.2.3	資訊安全政策、規則及標準之遵循性 控制措施：應定期審查組織資訊安全政策、主題特定政策、規則及標準之遵循性。	V		YAN-ISMS-02-13 資訊安全稽核作業程序書	
A.5.37 6.9.1.1	書面記錄之運作程序 控制措施：應書面記錄資訊處理設施之運作程序，並使所有需要的人員均可取得。	V		YAN-ISMS-02-02 文件暨紀錄管理程序書	
A.6	People Controls 人員控制措施				

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員		張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日
查核項目 ISMS PIMS	敘　　述			符合性		參考文件		補充說明
				符合	不符合			
A.6.1 6.4.1.1	篩選 控制措施：對所有成為員工之候選者，應於其加入組織前，進行背景查證調查，且持續進行，同時將適用的法律、法規及倫理納入考量，並宜相稱於營運要求事項，其將存取之資訊的分類分級及所察覺之風險。			V		YAN-ISMS-02-05 人員安全與教育訓練程序書		
A.6.2 6.4.1.2	聘用條款及條件 控制措施：聘用契約協議應敘明人員及組織對資訊安全之責任。			V		YAN-ISMS-02-05 人員安全與教育訓練程序書		
A.6.3 6.4.2.2	資訊安全認知及教育訓練 控制措施：組織及相關關注方之人員，均應接受與其工作職能相關的組織資訊安全政策、主題特定政策及程序之適切資訊安全認知及教育訓練，並定期更新。			V		YAN-ISMS-02-05 人員安全與教育訓練程序書		
A.6.4 6.4.2.3	懲處過程 控制措施：應明確訂定並傳達獎懲過程，以對違反資訊安全政策之人員及其他相關關注方採取行動。			V		YAN-ISMS-02-05 人員安全與教育訓練程序書 YAN-ISMS-02-10 資訊委外管理程序書		
A.6.5 6.4.3.1	聘用終止或變更後之責任 控制措施：應對相關人員及其他關注方定義、施行並傳達於聘用終止或變更後，仍保持有效之資訊安全責任及義務。			V		YAN-ISMS-02-05 人員安全與教育訓練程序書		
A.6.6 6.10.2.4	機密性或保密協議 控制措施：反映組織對資訊保護之需要的機密性或保密協議，應由人員及其他相關關注方，識別、書面記錄、定期審查及簽署。			V		YAN-ISMS-02-05 人員安全與教育訓練程序書 YAN-ISMS-02-10 資訊委外管理程序書		

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.6.7 6.3.2.2	遠距工作 控制措施：應實作安全措施，當人員於遠端工作時，保護於組織場所外存取、處理或儲存之資訊。		V	YAN-ISMS-02-08 存取控制程序書	Forti 防火牆授權於 2020/09/05 到期，VPN 帳號僅開放 1 組資安長使用，帳號使用中。 組織應審慎評估授權失效之重要設備持續使用 SSLVPN 可能會產生憑證與帳號外洩之風險考量。
A.6.8 6.13.1.2 6.13.1.3	資訊安全事件通報 控制措施：組織應提供機制，供人員透過適切之管道，及時通報所觀察到或可疑的資訊安全事件。	V		YAN-ISMS-02-11 安全事件管理程序書	
A.7	Physical controls 實體控制措施				
A.7.1 6.8.1.1	實體安全周界 控制措施：應定義及使用安全周界，以保護收容資訊及其他相關聯資產之區域。	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.2 6.8.1.2 6.8.1.6	實體進入 控制措施：保全區域應藉由適切之進入控制措施及進出點加以保護。	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.3 6.8.1.3	保全辦公室、房間及設施 控制措施：應設計辦公室、房間及設施之實體安全並實作。	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.4	實體安全監控 控制措施：應持續監視場所，防止未經授權之實體進出。	V		YAN-ISMS-02-06 實體安全管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.7.5 6.8.1.4	防範實體及環境威脅 控制措施：應設計並實作防範實體及環境威脅(諸如天然災害及其他對基礎設施之蓄意或非蓄意的實體威脅)之措施。	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.6 6.8.1.5	於安全區域內工作 控制措施：應設計並實作於安全區域內工作之安全措施。	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.7 6.8.2.9	桌面淨空及螢幕淨空 控制措施：應定義對紙本及可移除式儲存媒體之桌面淨空規則，以及對資訊處理設施的螢幕淨空規則，並適切實施之。	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.8 6.8.2.1	設備安置及保護 控制措施：設備應安全安置並受保護	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.9 6.8.2.6	場所外資產之安全 控制措施：應保護場域外資產	V		YAN-ISMS-02-03 資訊資產管理程序書 YAN-ISMS-03-01 資訊資產管理說明書	
A.7.10 6.5.3.1 6.5.3.2 6.5.3.3 6.8.2.5	儲存媒體 控制措施：儲存媒體應依組織之分類分級方案及處置要求事項，於其獲取、使用、運送及汰除的整個生命週期內進行管理。	V		YAN-ISMS-02-03 資訊資產管理程序書	
A.7.11 6.8.2.2	支援之公用服務事業 控制措施：應保護資訊處理設施免於電源失效，以及因支援之公用服務事業失效，所導致的其他中斷。	V		YAN-ISMS-02-06 實體安全管理程序書 YAN-ISMS-03-01 資訊資產管理說明書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.7.12 6.8.2.3	佈纜安全 控制措施：應保護傳送電源、資料或支援資訊服務之纜線，以防範竊聽、干擾或破壞。	V		YAN-ISMS-02-06 實體安全管理程序書	
A.7.13 6.8.2.4	設備維護 控制措施：應正確維護設備，以確保資訊之可用性、完整性及機密性。	V		YAN-ISMS-02-06 實體安全管理程序書 YAN-ISMS-03-01 資訊資產管理說明書	
A.7.14 6.8.2.7	設備汰除或重新使用之保全 控制措施：應查證包含儲存媒體之設備項目，以確保於汰除或重新使用前，所有敏感性資料及具使用授權的軟體已移除或安全覆寫。	V		YAN-ISMS-02-06 實體安全管理程序書 YAN-ISMS-03-01 資訊資產管理說明書	
A.8	Technological controls 技術控制措施				
A.8.1 6.3.2.1 6.8.2.8	使用者端點裝置 控制措施：應保護儲存於使用者端點裝置、由使用者端點裝置處理或經由使用者端點裝置可存取之資訊。	V		YAN-ISMS-02-08 存取控制程序書	
A.8.2 6.6.2.3	特殊存取權限 控制措施：應限制並管理特殊存取權限之配置及使用。	V		YAN-ISMS-03-04 帳號及通行密碼管理說明書	
A.8.3 6.6.4.1	資訊存取限制 控制措施：應依已建立之關於存取控制的主題特定政策，限制對資訊及其他相關聯資產之存取。	V		YAN-ISMS-02-08 存取控制程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.8.5 6.6.4.2	安全鑑別 控制措施：安全鑑別技術及程序應依資訊存取限制及關於存取控制之主題特定政策實作。	V		YAN-ISMS-02-08 存取控制程序書	
A.8.6 6.9.1.3	容量管理 控制措施：資源之使用應受監視及調整，以符合目前容量要求及預期容量要求。	V		YAN-ISMS-02-07 通信與作業管理程序書 YAN-ISMS-02-09 系統獲取與維護程序書 YAN-ISMS-02-10 資訊委外管理程序書 YAN-ISMS-04-21 系統與網路檢查記錄表	
A.8.7 6.9.2.1	防範惡意軟體 控制措施：應實作防範惡意軟體之措施，並由適切的使用者認知支援之。	V		YAN-ISMS-03-07 惡意軟體防護管理說明書	Microsoft Defender，防毒軟體病毒碼更新日115/06/29。
A.8.8 6.9.6.1 6.15.2.3	技術脆弱性管理 控制措施：應取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適切措施。	V		YAN-ISMS-02-07 通信與作業管理程序書	弱點掃描 115/06/25 初掃，115/06/29 複掃。
A.8.9	組態管理 控制措施：應建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)。		V	YAN-ISMS-03-12 組態管理作業說明書	組態項目資料(環境類)YAN-ISMS-G-57-11506-12，組態編號不應沿用前任設備之編號。

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘述	符合性		參考文件	補充說明
		符合	不符合		
A.8.10	資訊刪除 控制措施：當於資訊系統、裝置或所有其他儲存媒體中之資訊不再屬必要時，應刪除之。	V		YAN-ISMS-03-13 資訊保護作業說明書	
A.8.11	資料遮罩 控制措施：應使用資料遮蔽，依組織關於存取控制之主題特定政策及其他相關的主題特定政策，以及營運要求事項，並將適用法令納入考量。	V		YAN-ISMS-03-13 資訊保護作業說明書	
A.8.12	資料洩露預防 控制措施：應將資料洩露預防措施，套用至處理、儲存或傳輸敏感性資訊之系統、網路及所有其他裝置。	V		YAN-ISMS-03-13 資訊保護作業說明書	
A.8.13 6.9.3.1	資訊備份 控制措施：應依議定之關於備份的主題特定政策，維護資訊、軟體及系統之備份複本，並定期測試之。	V		YAN-ISMS-03-05 資訊備份管理說明書	
A.8.14 6.14.2.1	資訊處理設施之多備 控制措施：資訊處理設施之實作應具充分多備(redundancy)，以符合可用性之要求事項。	V		YAN-ISMS-02-12 營運持續運作管理程序書	
A.8.15 6.9.4.1 6.9.4.2 6.9.4.3	存錄 控制措施：記錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。	V		YAN-ISMS-02-08 存取控制程序書	
A.8.16	監視活動 控制措施：應監視網路、系統及應用之異常行為，並採取適切措施，以評估潛在資訊安全事故。	V		YAN-ISMS-03-02 網路及系統安全管理說明書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.8.17 6.9.4.4	鐘訊同步 控制措施：組織所使用資訊處理系統之鐘訊，應與經認可的時間源同步。	V		YAN-ISMS-02-07 通信與作業管理程序書	
A.8.18 6.6.4.4	具特殊權限公用程式之使用 控制措施：應限制並嚴密控制可能篡越系統及應用程式之控制措施的公用程式之使用。	V		YAN-ISMS-03-04 帳號及通行密碼管理說明書	
A.8.19 6.9.5.1 6.9.6.2	運作中系統之軟體安裝 控制措施：應實作各項程序及措施，以安全管理對運作中系統安裝軟體。	V		YAN-ISMS-02-09 系統獲取與維護程序書 YAN-ISMS-03-07 惡意軟體防護管理說明書	弱點掃描 115/06/25 初掃，115/06/29 複掃。
A.8.20 6.10.1.1	網路安全 控制措施：應受保全、管理及控制網路與網路裝置，以保護系統及應用程式中之資訊。		V	YAN-ISMS-03-02 網路及系統安全管理說明書	稽核了解 Forti 防火牆授權 2020/09/05 已到期 PA-440 防火牆因營運之業務需求，短暫下架。
A.8.21 6.10.1.2	網路服務之安全 控制措施：應識別、實作及監視網路服務之安全機制、服務等級及服務要求事項。		V	YAN-ISMS-03-02 網路及系統安全管理說明書	Forti 防火牆授權已到期，相關網路安全服務無法應對現行已知漏洞，應考量使用授權有效之設備或其他替代方案進行安全管控。
A.8.22 6.10.1.3	網路區隔 控制措施：應區隔組織網路中各群組之資訊服務、使用者及資訊系統。	V		YAN-ISMS-03-02 網路及系統安全管理說明書	Forti 防火牆授權已到期，然網路區隔仍執行中。

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.8.23	網頁過濾 控制措施：應管理對外部網站之存取，以降低暴露於惡意內容。	V		YAN-ISMS-03-02 網路及系統安全管理說明書	
A.8.24 6.7.1.1 6.7.1.2	密碼技術之使用 控制措施：應定義並實作有效使用密碼技術之規則(包括密碼金鑰管理)。		V	YAN-ISMS-02-09 系統獲取與維護程序書 YAN-ISMS-03-06 系統獲取與維護作業說明書	網站憑證 4 個憑證自動更新(入口網、報修網站憑證到期日 2026/09/06，書架系統憑證到期日 2026/09/12，MAIL 憑證到期日 2026/09/13)。 M365 Admin Center 授權管理工具故障，未及時通報與開立「YAN-ISMS-04-22 資訊-個資安全事件通報單」。

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.8.32 6.9.1.2 6.11.2.2 6.11.2.3 6.11.2.4	變更管理 控制措施：資訊處理設施及資訊系統之變更，應遵循變更管理程序。	V		YAN-ISMS-02-03 資訊資產管理程序書 YAN-ISMS-02-07 通信與作業管理程序書 YAN-ISMS-02-09 系統獲取與維護程序書 YAN-ISMS-03-02 網路及系統安全管理說明書 YAN-ISMS-03-14 變更管理作業說明書	
ISO27701 附錄之控制措施					
附錄 A(PII 控制者)					
A.7.2	蒐集及處理條件 判定並登載處理係合法，具適用管轄區之法律依據，並具明確定義且合法的目的。				
A.7.2.1	識別並登載目的 組織應識別並登載將處理 PII 之特定目的。	V		YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.2.2	敘明法律依據 組織應判定、登載並遵循針對所識別目的而處理 PII 之相關法律依據。	V		YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.2.3	判定何時及如何取得同意 組織應決定並登載過程，藉由該過程可證明是否、何時及如何向 PII 當事人取得 PII 處理之同意。	V		YAN-PIMS-02-02 個人資料蒐集管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.7.2.4	取得並記錄同意 組織應依書面過程取得並記錄 PII 當事人之同意。	V		YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.2.5	隱私衝擊評鑑 每當規劃進行 PII 之新處理或對 PII 的既有處理進行變更時，組織應評鑑對隱私衝擊評鑑之需要，並於適當時實作。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書	
A.7.2.6	與PII處理者之契約 組織應與其所使用之所有 PII 處理者簽定書面契約，並應確保其與 PII 處理者的契約闡明附錄 B 中適當控制措施之實作。	V		YAN-PIMS-02-03 個人資料處理與利用管理程序書	
A.7.2.8	與處理PII有關之紀錄 組織應判定並安全維護必要之紀錄，以支援其處理 PII 的義務。	V		YAN-PIMS-02-03 個人資料處理與利用管理程序書	
A.7.3	PII 當事人之義務 確保向 PII 當事人提供有關處理其 PII 之適當資訊，並履行 PII 當事人有關處理其 PII 的所有其他適用義務。				
A.7.3.1	判定並達成PII當事人之義務 組織應判定並登載 PII 當事人有關處理其 PII 之法令及營運義務，並提供履行此等義務的方法。	V		YAN-PIMS-02-04 當事人權利管理程序書	
A.7.3.2	判定提供予PII當事人之資訊 組織應判定並登載將提供予 PII 當事人之有關處理其 PII 及此種提供時序的資訊。	V		YAN-PIMS-02-04 當事人權利管理程序書	
A.7.3.3	提供資訊予PII當事人 組織應向 PII 當事人提供清晰且易於存取之資訊，以識別 PII 控制者並描述其 PII 之處理。	V		YAN-PIMS-02-04 當事人權利管理程序書	
A.7.3.4	提供修改或撤回同意之機制 組織應提供機制，以供 PII 當事人用以修改或撤回其同意。	V		YAN-PIMS-02-04 當事人權利管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.7.3.5	提供反對PII處理之機制 組織應提供機制供 PII 當事人用以反對其 PII 之處理。	V		YAN-PIMS-02-04 當事人權利管理程序書	
A.7.3.6	存取、更正及/或抹除 組織應實作政策、程序及/或機制，以履行供 PII 當事人存取、更正及/或抹除其 PII 之義務。	V		YAN-PIMS-02-04 當事人權利管理程序書	
A.7.3.7	PII控制者告知第三方之義務 組織應將共享 PII 有關之任何修改、撤回或異議，告知共享 PII 的第三方，並實作如此做之適當政策、程序及/或機制。		V	YAN-PIMS-02-03 個人資料處理與利用管理程序書	PIMS 該四階表單內未說明同意提供 PII 給第三方組織。
A.7.3.8	提供所處理PII之複本 組織應能於 PII 當事人請求時，提供所處理 PII 之複本。	V		YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.3.9	處置請求 組織應定義並登載政策及程序，供用以處置及回應 PII 當事人之合法請求。	V		YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.4	於設計即保護隱私及預設保護隱私 確保設計過程及系統時，將蒐集及處理(包括利用、揭露、留存、傳輸及棄置)限制於敘明目的之必要範圍。				

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.7.4.1	限制蒐集 組織應將 PII 蒐集限制於與所識別目的相關、成比例及必要之最小量。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.4.2	限制處理 組織應將 PII 處理限制於對所識別目的係合宜、相關且必要。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-03 個人資料處理與利用管理程序書	
A.7.4.3	準確性及品質 組織應確保並登載，於 PII 整個生命週期中，PII 之準確性、完備性及最新性係基於其處理目的之需要。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.4.4	PII最小化目標 組織應定義並登載資料最小化目標，以及用以達成該等目標之機制(諸如去識別化)。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-02 個人資料蒐集管理程序書	
A.7.4.5	處理結束時之PII去識別化及刪除 一旦就所敘明目的不再需要原始PII時，組織應刪除PII或以不允許識別或再識別PII當事人之形式提供之。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-03 個人資料處理與利用管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.7.4.6	暫時檔案 組織應確保於書面所規定之期限內，依書面程序棄置(例:抹除或銷毀)因PII處理而建立之暫時檔案。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-03 個人資料處理與利用管理程序書 YAN-ISMS-02-07 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	留存 組織留存PII之時間不得超過PII處理所必要的時間。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-03 個人資料處理與利用管理程序書 YAN-ISMS-02-07 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	棄置 組織應具棄置PII之書面政策、程序及/或機制。	V		YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-03 個人資料處理與利用管理程序書	

延宇資訊股份有限公司

機密等級：■一般□限閱□密□機密	文件編號：YAN-ISMS-04-27	保存年限：2 年
日期：115 年 6 月 29 日	紀錄編號：YAN-ISMS-G-27-11506-01	版本：2.2

稽核版次	ISO 27001:2022 ISO 27701:2019	受稽單位	全公司	稽核員	張弘志、黃韋霖、廖嘉文、廖志昇	稽核日期	115 年 6 月 29 日

查核項目 ISMS PIMS	敘　　述	符合性		參考文件	補充說明
		符合	不符合		
A.7.4.9	PII傳輸控制措施 組織應對透過資料傳輸網路傳輸(例:發送至另一組織)之PII，設計適當的控制措施，以確保資料抵達其預期之目的地。		V	YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書 YAN-PIMS-02-03 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	PIMS 該四階表單內未說明因服務之業務需求，移轉與揭露對象。
A.7.5	PII 共享、轉移及揭露 判定是否並登載何時，依適用義務，PII 被共享、轉移至其他管轄區或第三方及/或揭露。				
A.7.5.3	PII轉移紀錄 組織應記錄與第三方之間的PII轉移，並確保與該等第三方合作，以支援與PII當事人義務有關之未來請求。	V		YAN-PIMS-02-03 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.7.5.4	向第三方揭露PII之紀錄 組織應記錄向第三方揭露之PII，包括已揭露的PII為何、向誰及何時揭露。	V		YAN-PIMS-02-03 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	