三階文件 -PIMS

- YAN-PIMS-03-01個資風險評鑑方法論
  - YAN-PIMS-03-01個資風險評鑑方法論_V2.0_20240122

YAN-PIMS-03-01

□□□□□□□□

YAN-PIMS-03-01

個資風險評鑑方法論

_V2.0_20240122

延宇資訊股份有限公司

「資訊安全暨隱私資訊管理系統」

個資風險評鑑方法論

機密等級: 一般

編號: YAN-PIMS-03-01

版本編號: 2.0

修定日期: 2024/01/22

使用本文件前 ，如對版本有疑問 ，請與修訂者確認最新版次。

文件編號: **YAN-PIMS-03-01**

機密等級: ¢一般 £限閱 £密 £機密

本文件歷次變更紀錄:

版次	修訂日	修訂者	說明	核准者
1.0	2021/11/08	梁維志	新增	楊文欽
2.0	2024/01/22	黃韋霖	調整評鑑方法之說明。	梁維志

本程序書由　　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。

目錄:

1 目的

2 適用範圍

3 權責

4 名詞定義

5 作業說明

6 相關文件

1 目的

1.1

判定組織現行個資流程之風險程度，以評估是否須進行風險降低或風險轉移等計畫。利用系統化的方法對個資流程所會遭受之風險進行評估，包括現行存在的弱點情形及個資資產所面臨的威脅種類與衝擊程度。

2 適用範圍

2.1 本公司之個資風險評鑑流程均屬之。

3 權責

3.1 無。

4 名詞定義

4.1 衝擊／影響:

係指威脅利用現況管理之弱點，造成損害或影響時，對公司之衝擊／影響程度。

4.2 發生機率:

根據威脅利用現況管理之弱點，造成損害或影響之發生機率: 高（ H ）、中（ M）、低（ L）。

4.3 敏感個資:

個人資料保護法第 6條第 1 項本文規定，列舉出五項「敏感性個人資訊」，這些個人資料歸類為特種個資，說明如下:

4.3.1 有關醫療之個人資料。

4.3.2 有關基因之個人資料。

4.3.3 有關性生活之個人資料。

4.3.4 有關健康檢查之個人資料，

4.3.5 有關犯罪前科之個人資料。

5 作業說明

5.1 個人資料檔案資訊及風險識別

5.1.1 個人資料檔案 ：為「 YAN-PIMS-04-01個人資料清冊」中，所列之個人資料檔案。

5.1.2 有無特種個資 ：說明個人資料檔案是否有特種個資，請依據「 YAN-PIMS-04-01個人資料清冊」之內容。

5.1.3 檔案數量 ：評估個人資料檔案，每年大約之件數。

5.1.4 個人資料檔案價值 ：依據 ?YAN-PIMS-02-01 個人資料識別與隱私設計管理程序書?，評估個人資料檔案之價值。

5.1.5 作業情境、作業內容及具體風險類型 ：請參照：「 YAN-PIMS-04-08 風險類型暨風險對策參考表 」，識別個人資料檔案之作業情境、作業內容及具體風險類型。

5.1.6 風險處理對策 ：

依據具體風險類型，說明現階段本公司之因應風險之控制措施。

5.2 評估個人資料檔案風險機率及衝擊

5.2.1

評估風險發生機率，及當風險發生時對於本公司所造成之衝擊。評估時，應考量現階段之風險處理措施。

5.2.2 衝擊評估之準則，請參照「表一、衝擊影響等級定義表」。

5.2.3 風險發生之機率，請參照「表二、風險發生機率定義表」。

表一、衝擊影響等級定義表

衝擊 /影響等級	說明
H高風險	1. 商譽受損並可能面臨 100 萬元以上損失 2. 最優先次序執行之風險處置措施
M中風險	1. 商譽受損並可能面臨 10萬元以上 萬元以下之損失 2. 次優先次序執行之風險處置措施
L 低風險	1. 商譽受損並可能面臨 10 萬元以下之損失 2. 最低次序執行之風險處置措施

表二、風險發生機率定義表

機率	說明
高風險機率	每季可能發生超過一次 (每年

中風險機率	每年可能發生超過一次	(每年 2
低風險機率	每年不超過一次	(每年 <=1

5.3 風險值判定

5.3.1

依據風險發生之機率及風險發生後所造成之衝擊，判定個人資料檔案之風險值。

5.3.2 風險值風評估之準則，請參照「表三、風險值評估表」。

表三、風險值評估表

風險值		衝擊／影響等級		
		低（ L)	中（ M)	高（
發生機率	高（ H)	中（ M)	高（ H)	高（
	中（ M)	低（ L)	中（ M)	高（
	低（ L)	低（ L)	低（ L)	高（

5.4 綜合風險值判定

5.4.1

依據個人資料檔案價值及風險值，評估個人資料檔案之綜合風險值。

5.4.2 縱合風險值評估之準則，請參照「表四、縱合風險值評估表」。

表四、縱合風險值評估表

綜合風險值		風險值		
		低（ L)	中（ M)	高（
個資價值	高（ H)	中（ M)	高（ H)	高（
	中（ M)	低（ L)	中（ M)	高（
	低（ L)	低（ L)	低（ L)	中（

5.5 風險改善計畫

5.5.1 如個資資產之 綜合風險值為高（ H) 時，需實施風險改善計畫。

6 相關文件

6.1 YAN-PIMS-02-01個人資料識別與隱私設計管理程序書

6.2 YAN-PIMS-04-08風險類型暨風險對策參考表

6.3 YAN-PIMS-04-01個人資料清冊