資訊安全風險管理執行情形報告

(業於 112 年 11 月 08 日第 14 屆第 9 次董事會報告)

資訊處報告

資訊安全風險管理報告議程

1. 2023年度/資安已執行項目

1.1 ISMS 、PIMS
1.2 技術面
1.3 管理面及教育訓練

2. 資安計畫持續執行

2.1 ISMS 資安管理系統執行計畫
2.2 PIMS 個資管理系統執行計畫

1. 2023 年度資安已執行項目

2023/01 ~ 2023/10

1.1【管理面】ISMS已執行項目

一階文件 (2022/11)

- 一階文件：2份

二階文件&四階表單 (2022/11~2023/8)

- 二階文件：1份
- 四階表單：1份
- 二階文件：14份
- 四階表單：18份

資安治理 (2023~)

- 資安治理每月月會
- 資安威脅趨勢分享
- 管理制度文件發布

ISMS已完成文件

一階文件

- M-IS-001_資訊安全政策
- M-IS-002_資產與資訊安全管理規範

二階文件

- P-IS-001_資訊安全組織管理辦法
- P-IS-002_資訊安全事件通報管理辦法
- P-IS-003_供應商關係管理辦法
- P-IS-004_資訊資產與風險評鑑管理辦法
- P-IS-005_作業安全管理辦法
- P-IS-006_存取控制管理辦法
- P-IS-007_營運持續管理辦法
- P-IS-008_通訊安全管理辦法
- P-IS-009_資訊安全監督與量測管理辦法
- P-IS-010_資訊安全查核管理辦法
- P-IS-011_資訊安全矯正與持續管理辦法
- P-IS-012_實體與環境安全管理辦法
- P-IS-013_人力資源安全管理辦法
- P-IS-014_系統獲取開發及維護管理辦法
- P-IS-015_資訊安全文件管理辦法

四階表單

- F-IS-001-01_資訊安全組織圖
- F-IS-002-01_資訊安全事件報告單
- F-IS-002-02_資訊安全事件登記簿
- F-IS-003-01_資訊安全切結書
- F-IS-003-02_委外廠商稽核查檢表
- F-IS-004-01_關鍵流程盤點表
- F-IS-004-02_廠務研發_資訊資產清冊
- F-IS-004-03_總公司_資訊資產清冊
- F-IS-004-04_廠務研發_風險評鑑彙整表
- F-IS-004-05_總公司_風險評鑑彙整表
- F-IS-006-01_帳號與權限管理紀錄表
- F-IS-007-01_營運衝擊分析表
- F-IS-007-02_營運持續計畫演練暨處理報告單
- F-IS-009-01_資訊安全管理系統有效性量測表
- F-IS-010-01_資訊安全管理制度內部稽核計畫
- F-IS-010-02_資訊安全管理制度內部稽核表
- F-IS-010-03_資訊安全管理制度內部稽核報告
- F-IS-011-01_矯正處理單
- F-IS-012-01_機房進出日誌

1.1【管理面】PIMS已執行項目

個資盤點訪談
(2023/07~08)

- 數發處
- 行銷處

個資清冊產出
(2023/10)

- 數發處：綜合電商,自有電商
- 行銷處：T&C, 天地合補, 桂格保健, 嬰童, 成奶, 完膳, 廚房, 福樂, 穀物, 飲料, 市調, 活動贈品, 客服, 媒體

PIMS已完成項目

第一階段(7月-8月)

個資盤點訪談

- 顧問說明—個資介紹、個資蒐集法規限制、個資分類與盤點 -7/12
- 數發處及行銷處初步盤點訪談 -8/2, 8/4
- 自有電商&綜合電商流程示意圖產出 -8/3
- 個資盤點表V1 -8/23
- 數發處及行銷處個資複盤 -8/25, 8/30

第二階段(9月)

產出個資盤點清冊

- 個資清冊生命週期填寫教學 (線上) -9/8
- 數發處及行銷處各單位填寫個資生命週期 -9/11~9/18
- 以行銷處完膳組為首，產出完整個資清冊作為其他單位範例參考 -9/26

第三階段(10月~)

清冊確認及個資風險評鑑

- 數發處及行銷處 盤點清冊確認 -10/18~10/24
- 數發處及行銷處 個資風險評估分析 -10/18~10/24
- 數發處及行銷處 風險評鑑報告產製 -10/25

第四階段(10月~)

PIMS文件待發行

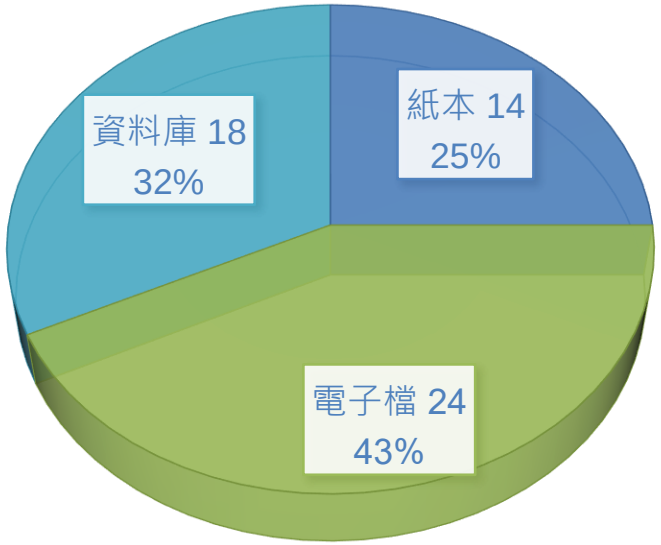
- 二階文件3份
- 三階文件5份
- 四階表單12份

個資風險評鑑(1) — 個資數量統計

- 盤點範圍：數位事業發展處、行銷處、永續發展處
- 個人資料：總計56項

個人資料類型	數量
電子（DA）	24
資料庫（DB）	18
紙本（DC）	14
總計	56

個人資料類型分布圖



風險值計算方式(1)

※風險值 = 敏感度等級 x 資料量等級 x 風險事件等級 x 風險發生可能性等級

➢ 敏感度等級

資料類別	說明	範例	個人資料敏感度等級
高度敏感資料	資料外洩恐造成個人嚴重傷害	1.《個人資料保護法》所定義限制蒐集資料。	3
		2. 個人銀行帳戶及其他財務資訊。	
		3. 與弱勢成人和兒童有關的個人資料。	
		4. 個人特徵的詳細描述。	
		5. 可能對個人造成不利影響的敏感協商。	
中度敏感資料	資料外洩雖造成個人傷害但不致太嚴重	姓名/身分證字號及興趣、宗教、信仰、政治傾向詳細學經歷、婚姻等較難取得之基本資料細節，或者由過多的一般個人基本資料組合而成（超過6種，或姓名+身分證字號/護照號碼組合）的詳細的個人資料。	2
一般個人資料	資料外洩恐造成個人傷害有限	姓名、電話、性別、年齡地址等一般性基本資料且欄位有限（不超過6個，但不包含身分證字號或護照號碼）。	1

➢ 資料量等級

資料筆數	資料量等級
超過50,000（含）筆	4
5,001（含）筆~50,000筆	3
21（含）筆~5,000筆	2
20筆以下	1

風險值計算方式(2)

※風險值 = 敏感度等級 x 資料量等級 x 風險事件等級 x 風險發生可能性等級

➢ 風險事件等級

風險事件衝擊程度	說明	風險事件安全等級
高	違反法令、法規之要求或安全管控措施不當/人為疏失，一旦發生，將 對本公司或民眾權益造成重大損失，恐有刑事或民事責任產生。	3
	組織聲譽與形象嚴重受損（含上新聞媒體）。	
中	無違反法令、法規要求，惟安全管控措施不當或人為疏失，一旦發生， 將對本公司或民眾權益造成損失有限，恐有內部行政處分，無涉及刑事或民事責任。	2
	組織聲譽與形象輕微受損，僅向組織單位申訴或抱怨。	
低	無違反法令、法規要求，惟安全管控措施不當或人為疏失，一旦發生， 對本公司或民眾權益僅造成輕微損害。	1
	無影響組織聲譽與形象。	

➢ 風險發生可能性等級

可能性	說明	可能性等級
發生的可能性高/很有機會發生/很有可能發生	未建立控管程序及相關文件，亦無任何安全控管。	3
發生的可能性中等/也許會發生	尚未建立控管程序及相關文件，但有實施部份安全控管。	2
	或已建立控管程序及相關文件，但部分未落實。	
發生的可能性低	已建立控管程序及相關文件，且已落實。	1

個資風險評鑑(3) — 風險值分布

個資風險分布值域為4~32分，依據業務流程相關之個人資料檔案，並參照「個人資料檔案風險評鑑與管理」程序書之規範執行。

- 顧問建議：本年度可接受之風險值為30（含）。
- 風險值超過30之個人資料檔案共計鑑別出3項。

個資類別 / 風險值	紙本資料(DC)	電子資料(DA)	資料庫（DB）	總計
4	0	2	0	2
8	4	8	2	14
12	0	3	4	7
16	10	8	8	26
24	0	2	2	4
32	0	1	2	3
總計	**14**	**24**	**18**	**56**

個資風險評鑑(4) — 高風險彙整

- 個人資料高風險彙整，共3件

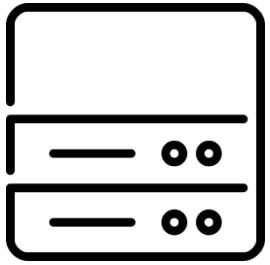
項次	單位	資產編號	資料形式	流程名稱	個資檔案名稱	敏感度等級	風險事件		風險事件等級	風險發生可能性等級	資料量等級	風險值
							類別	事件				
1	A50E00010(自有電商)	A50E00010-03	資料庫	佳格會員	桂格寶寶甜蜜會員(2019整合前(含身分證))	2	資料外洩	文件資料遭竊（外洩）	2	2	4	32
2	A50M10140(永續發展處\客服)	A50M10140-02	資料庫	客服流程	客戶諮詢、退換貨（客服錄音檔）	2	資料外洩	文件資料遭竊（外洩）	2	2	4	32
3	A50M10011(行銷處\保健)	A50M10011-04	電子檔	粉專管理流程	桂格 天地合補IG粉專（T&C）	2	資料外洩	文件資料遭竊（外洩）	2	2	4	32

風險處理建議

➢ 針對本年度高風險項目，風險處理建議如下:

盤點範疇	通用性建議
1. 源頭管理，限縮使用及接觸對象 清查資料庫使用對象，針對相關權限進行限縮，僅開放必要之直接資料使用者使用。	**1.適當個資蒐集以及事前告知** 處理相關業務活動而需蒐集個人資料時，除宜考量蒐集欄位之適當性，以避免過度蒐集個人資料，並應依個資法第8條進行告知事項（含同意書），並留存相關佐證。
2. 留存紀錄，比對稽核軌跡 比照公部門對系統之要求，相關log應至少留存半年（實務上應考量個資保存期限），並不定期清查勾稽，以確保無資料誤（濫）用。	**2. 委外廠商監督** 應對委外廠商執行適當之監督，以避免可能之風險事件產生。（個資法第四條及施行細則第八條）
3. 引進IT技術，進行資料遮蔽或DLP 依據ISO 27001:2022新版規範，採行8.11及8.12之控制措施。	**3. 桌面淨空與螢幕淨空** 將桌面及螢幕機敏信息移除，減少未經授權的訪問，保護個人隱私，降低信息泄露的風險。

1.2【技術面】已執行項目



集團網站主機群遷回 (2023/05~07)

- 新主機群環境
- 資料庫重建
- 結構性差異校正

網站滲透測試 (2023/06~08)

- 針對外部網頁滲透測試並修補漏洞
- 測試範圍新增ChatBot相關網站

伺服器弱點掃描 (2023/09~)

- 針對系統做弱點掃描並修補漏洞
- 掃描範圍新增ChatBot運作機群

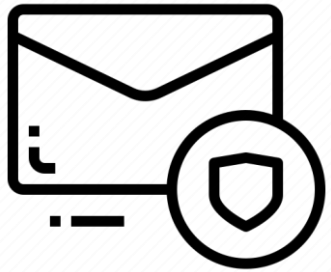
1.2【技術面】已執行項目

資安投資抵減 (2023/05)

- 2022~2023年驗收&請購資安項目
- 提出申請 (IT/總務/財務/顧問)

集團核心防火牆汰換 (2023/06~08)

- 大園&IDC機房核心防火牆汰換
- 因伺服器需求的增加做結構性強化



郵件安全防護 (2023/07)

- 郵件雲端流程防護
- 惡意傳遞事件追蹤

1.3【管理面及教育訓練】已執行項目

網站維護商作業管理 (2023/05~08)

- 作業流程及帳號管理
- 權限及維護範圍控管

PIMS基礎訓練 (2023/07)

- 個資介紹、個資分類與盤點
- 個資蒐集法規限制

個資清冊填報 (2023/09)

- 個資清冊生命週期
- 重點單位輔導參考

2. 資安計畫持續執行

2023/11 ~ 2024

2.1 ISMS 資安管理

專案導入範圍

專案目標

- 依據ISO 27001 認證要求，協助建立、調整及優化現行資訊安全管理制，並通過第三方驗證取得國際標準證書。

專案範圍

- BPM系統、維運及管理，與機房管理、網路管理、辦公室安全等支援性管理。(IDC 機房、大園機房)

專案時程

- 2023 年10 月~2024 年9 月

管理制度導入流程

一、現況診斷與差異分析

現行 貴單位資訊安全制度
現行組織業務運作特性分析
現行文件表單驗及證範圍分析等...

二、風險評鑑與管理

整合於作業中，識別價值及風險因子資料庫，判別適當的威脅及可能性，進而產出風險評鑑

三、建立管理制度文件

建立 貴公司之四階文件包含資安政策、管理程序書、工作指導書、文件表單及記錄

六、外部稽核並取得證書

透過第三方驗證 審查貴公司導入範圍之驗證結果及核准頒布

五、內部稽核

內部稽核 驗證組織專案範圍在這段時間導入之驗收成果

四、制度落實

營運持續管理計畫(BCP)
教育訓練、相關活動之執行紀錄

ISMS 資安管理系統之【階段性】執行計畫

1. 現況診斷與差異分析

2023/10~2023/12

- ☐ 現況分析訪談
- ☐ 資安組織架構討論

2. 風險評鑑與管理

2023/12~2024/02

- ☐ 資訊資產盤點
- ☐ 定義資訊資產價值
- ☐ 風險評鑑作業
- ☐ 風險管理

3. 建立管理系統文件

2023/12~2024/05

- ☐ 建立管理制度程序文件
- ☐ 建立資訊安全目標
- ☐ 建立適用性聲明書

4. 制度落實與內部稽核

2024/04~2024/08

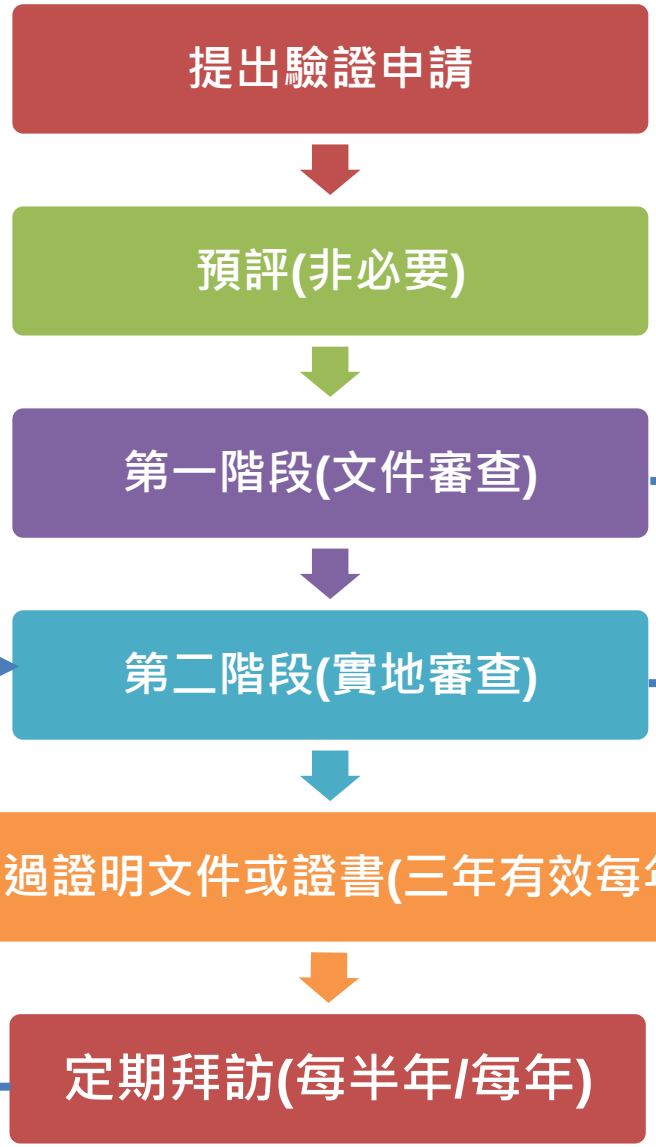
- ☐ 落實管理制要求作業
- ☐ 落實營運持續演練作業
- ☐ 執行內部稽核作業
- ☐ 改善稽核發現事項
- ☐ 執行管理審查會議

5. 稽核作業與驗證

2024/08

- ☐ 管理制度驗證前準備
- ☐ 管理制度驗證作業文件審查
- ☐ 管理制度驗證作業實地審查
- ☐ 取得證書或通過證明文件

驗證流程



⚠ 重大議題：無法執行第二階段

主要缺失：
90天內限期改善並擇日特別拜訪
次要缺失：
須於5 天內提出改善計畫，
於下次追蹤拜訪確認改善成果
改善建議：
提供組織持續優化精進之方案

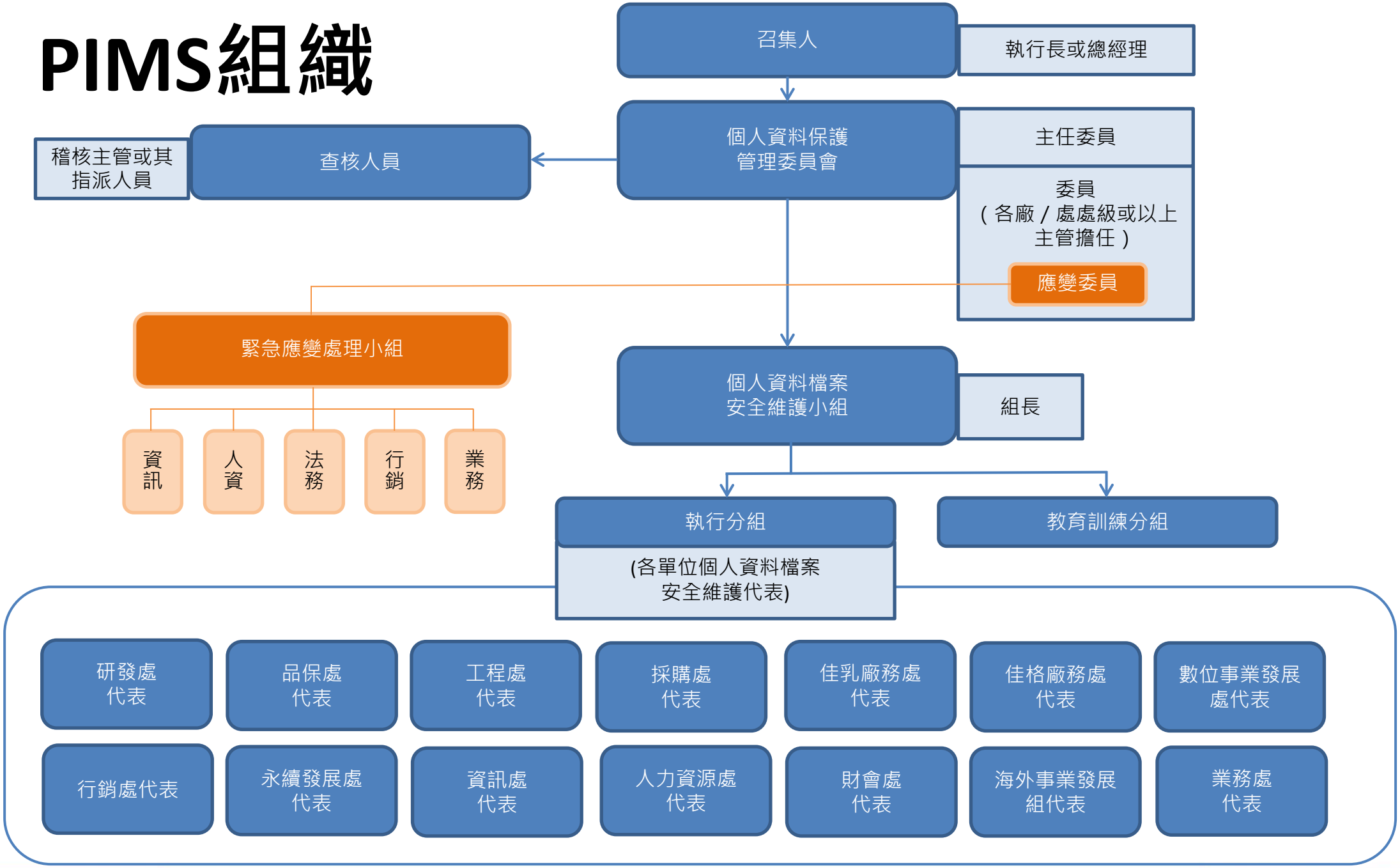
可延伸驗證
可調整範圍
可轉換版本

預期效益

建立以風險為導向，持續運作改善管理制度	1. 建立符合標準及主管機關之風險評估方法。 2. 建立可持續運作改善之管理框架，得以面對法令法規持續變動之要求。 3. 識別出有助於及決定組織整體風險之因素。 4. 強化的風險管理實務和控制，及為達成組織所要準備情形，其可採取之措施。
落實資安治理，確保業務發展與資安治理一致性	1. 組織之安全準備情形，確保組織資訊安全管理的一致性。 2. 提升競爭力及形象、確保業務資訊。 3. 鑑別資訊安全管制點，建立資訊硬體設施及軟體之管理機制。
提昇組織風險評估與風險處理專業能力	1. 鑑別資訊安全管制點，建立資訊硬體設施及軟體之管理機制。 2. 預防電腦或資訊被違規使用。 3. 制定並實施相關復原活動與維護復原計畫。 4. 發展策略因應遭受的破壞與可能的損失。 5. 事件發生能夠及時偵測，消除與日俱增之資訊安全威脅。

2.2 PIMS 個資管理

PIMS組織


召集人
執行長或總經理
稽核主管或其指派人員
查核人員
個人資料保護管理委員會
主任委員
委員
(各廠 / 處處級或以上主管擔任)
應變委員
緊急應變處理小組
資訊
人資
法務
行銷
業務
個人資料檔案安全維護小組
組長
執行分組
(各單位個人資料檔案安全維護代表)
教育訓練分組
研發處代表
品保處代表
工程處代表
採購處代表
佳乳廠務處代表
佳格廠務處代表
數位事業發展處代表
行銷處代表
永續發展處代表
資訊處代表
人力資源處代表
財會處代表
海外事業發展組代表
業務處代表

從個資保護生命週期建置PIMS

PIMS專案導入範圍

專案目標

- 個資法及其施行細則(細則第12條11項安全維護措施)
- BS 10012(ISO 27701)

專案範圍

- 全公司
- 2023年以**數位事業發展處**及**行銷處**作為重點部門

專案時程

- 2023 年06 月~2024

PIMS 個資管理之【階段性】執行計畫

1. 建立個資保護架構

2023/10~2023/12

- 訂定個資保護管理政策
- 成立個資保護管理組織
- 製作建置PIMS作業時程表及建置範圍
- 公告個資保護管理政策

2. 個資盤點與風險評估流程

2023/7~2023/10

- 盤點法規及上級機關訂定之規範
- 流程分析及盤點個人資料
- 執行個資風險評鑑及隱私權衝擊分析
- 建置PIMS內部規範

3. 管理制度運作

2023/10~2024

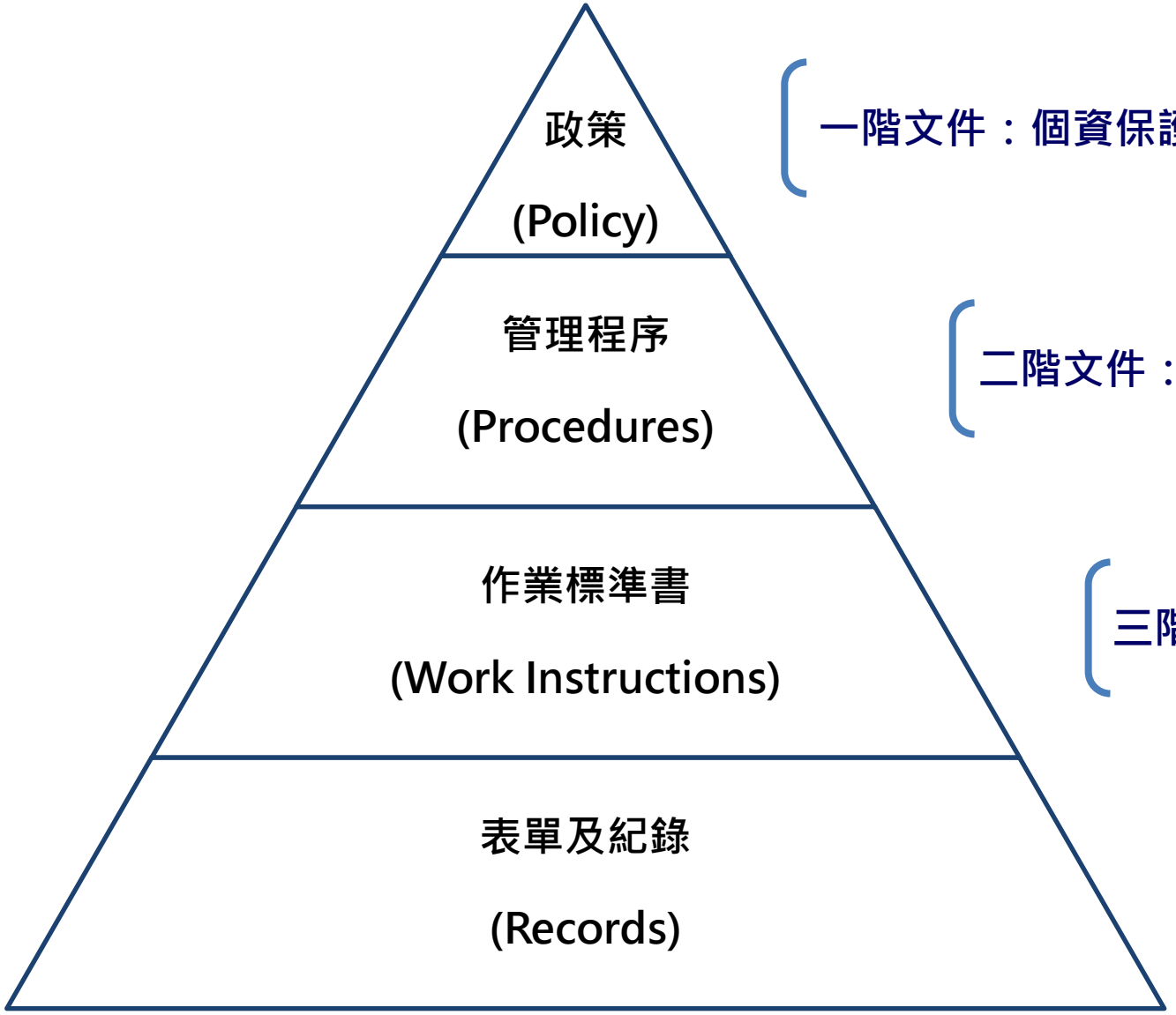
- 制訂績效衡量指標
- 運作PIMS管理制度
- 執行PIMS內部稽核
- 修正PIMS並實施改善措施

專案時程

- 2023年：行銷處及數位事業發展處
- 2024年：財會處、人資處、採購處、資訊處、新事業發展組、業務處、佳格中壢廠、佳格新竹廠、大園廠務處、工程處、研發處、品保處

各項執行工作 時程規劃	112年 10月	112年 11月	112年 12月	113年 01月	113年 02月	113年 03月	113年 04月	113年 05月	113年 06月	113年 07月	113年 08月	113年 09月	113年 10月	113年 11月	113年 12月
專案工作計畫書															
專案啟動															
個資政策、組織、文件管理程序															
個資盤點(總部各處室)					(2月上旬)										
個資盤點(外廠)							(4月上旬)								
個資風險評鑑(行銷及數發)		(10月下旬)													
個資風險評鑑(總部各處室)								(5月上旬)							
個資風險評鑑(外廠)										(6月下旬)					
個資風險處理與再評鑑(行銷及數發)		(10月下旬)													
個資風險處理與再評鑑(ALL)													(9月下旬)		
PIMS文件發行(含優化微調)			(12月上旬)												
PIMS落實															
內部稽核與改善				(1月上旬，行銷處&數發處)										(11月上旬)	
管理審查					(行銷處&數發處)										(12月上旬)
教育訓練															

產出PIMS 四階管理文件



一階文件：個資保護最高指導原則

二階文件：各項作業之管理原則與程序

三階文件：各項作業之標準作業程序

四階文件：表單及執行紀錄

PIMS預計發行文件

二階文件 (共3份)

- 個人資料保護生命週期管理程序書
- 個人資料保護當事人之權利聲明管理程序書
- 個人資料檔案風險評鑑與管理程序書

三階文件 (共5份)

- 個人資料委外監督控管作業說明書
- 個人資料保護緊急應變處理作業辦法
- 個人資料檔案安全控管作業說明書
- 個人資料檔案安全維護計畫
- 業務終止後個人資料處理方法

四階文件 (共12份)

- 委外專案資料刪除、銷毀及載體返還切結書
- 委外廠商自我評估表
- 委託書
- 個人資料申訴事件記錄單
- 個人資料委外廠商查核表
- 個人資料保護契約條款
- 個人資料檔案風險改善計畫表
- 個人資料檔案清冊
- 個資事故通報及受理流程
- 個資事故通報單
- 個資風險評估表
- 當事人權利行使申請書