個人資料事件應變演練

輔導顧問師 林信成 （Albert Lin）

ISO27001 /BS10012 /ISO29100 /ISO9001主導稽核員

Mobile: 0933-510515

E-mail: bingo1982012@gmail.com

SafeLink 博創資訊科技股份有限公司

課程大綱

- 第一章 個人資料事件風險之認知與介紹
- 第二章 營運持續管理簡介
- 第三章 營運衝擊分析與營運持續管理策略
- 第四章個人資料事件應變演練計畫擬定與實施
- 第五章個人資料事件應變演練計畫測試、維護及再評估

第一章 個人資料事件風險之認知與介紹

- ◆1-1 風險概觀
- ◆1-2 造成風險之因素
- ◆1-3 風險管理

1-1 風險概觀

美國Risk Management Plan (RMP)內容

風險管理制度
(Risk Management Program)

危害評估
(Hazard Assessment)

- 最嚴重意外排放事件
- 可能意外排放事件
- 廠外影響分析
- 五年意外排放事故紀錄

預防計畫
(Prevention Program)

- 管理系統
- 製程危害分析
- 標準操作步驟
- 員工訓練
- 預防保養
- 開車前檢查
- 變更管理
- 安全稽核
- 事故調查
- 製程安全資訊

應變計畫
(Emergency Response Program)

- 緊急應變計畫
- 應變步驟及防護具使用
- 逃生與保護措施
- 應變訓練
- 應變及消減技術
- 通報及應變程序
- 使用、檢查、測試、保養紀錄

進行風險管理的重要性

- 資訊具有價值，必須受到適當的保護
  - 保護資訊免受多種威脅的攻擊。
  - 保證業務持續運作，將損失降至最低。
- 100% 安全是一種過高的期望
  - 依據風險等級，分配有限之資源加以控管。
  - 必須透過控制措施，降低資訊風險到達可接受程度。
- 系統化管理資訊風險
  - 建立PIMS 必須管理個人資料事件風險。
  - 有效保障個人資料事件之投資。

風險管理流程


風險管理
1. 準則與方法
2. 風險評鑑
識別資產與重要性
威脅分析
弱點分析
計算風險
不可接受風險
3. 風險處理
評估對策
選定控制措施
執行處理方案
評估成效

1-2 造成風險之因素

認識資訊資產

◆資訊資產受到破壞會影響業務進行，甚至造成中斷或癱瘓。

◆資產是組織的資源或產出，可以是有形或無形，包含IT 與非IT。

- 有形資產：例如：資訊設備、儲存媒體、人員、基礎設施、資料（含個人資料）等。
- 無形資產：例如：應用系統、業務流程、知識等。

認識弱點

- 存在於資訊系統或其他組成元件的弱點，如果被威脅利用，會造成危害。
  - 例如軟體測試不足、硬體設計缺失、內部控制程序不足。
- 弱點存在於資訊資產本身，為資產之特性，例如：
  - 所在之地理位置。
  - 適用材質。
  - 使用、設計或管理方式。
- 優點也可能成為弱點
  - 例如：攜帶方便之隨身碟或筆記型電腦
- 通常以被威脅利用難易程度進行評估。

認識威脅

◆足以造成資訊資產危害之狀況或事件。

– 例如：破壞、洩漏、篡改資料或阻斷服務而危害。

◆威脅通常可以分為：

– 不可抗力因素，例如：地震、颱風。

– 人為錯誤，例如：資料輸入錯誤、設備操作錯誤。

– 惡意行動，例如：駭客入侵、竊取資料、販賣牟利。

◆通常以發生可能性或機率進行評估。

1-3 風險管理

本校個資事件等級判斷

等級	影響程度	事件性質描述
0	小	當事人權利行使處理不當或對於本校個人資料管理所引起之抱怨或申訴
		個人資料外洩筆數在20筆以內(團體訴訟不成立)
		外洩之個人資料僅含有一般性之識別資料
1	中	違反本校個人資料管理規範。當事人向高層主管提出抱怨或申訴
		一般個人資料外洩筆數在21~10,000筆之間 特種個人資料外洩筆數在21~1,000筆之間
		外洩之個人資料含有個人活動相關資料
2	大	上級單位、政府機構糾正、要求改善
		一般個人資料外洩筆數在10,001~20,000筆之間 特種個人資料外洩筆數在1,001~5,000筆之間
		外洩之個人資料含有金融財務相關資料
3	嚴重	違反法律要求、司法訴訟事件或公眾媒體報導影響本校聲譽。當事人向本校以外政府單位或相關機構檢舉或抱怨及申訴。
		一般個人資料外洩筆數在20,001筆以上 特種個人資料外洩筆數在5,001筆以上
		外洩之個人資料含有個資法第六條所定義之特種個人資料

本校個資事件通報管理

事件 （影響程度）	通報對象	通報 方式	處理期限 （目標值）	結案 通報方式
0(小)	個資保護專責人員	電話 （郵件）	接獲通報後24小時以內	電話(郵件) 個人資料事件紀錄通報單
1(中)	個資保護專責人員 單位主管		接獲通報後8小時以內	
2(大)	個資保護專責人員 單位主管 執行秘書		接獲通報後2小時以內	
3(嚴重)	個資保護專責人員 單位主管 執行秘書 召集人		接獲通報後1小時以內	

個資事件損害賠償及團體訴訟

個資法第34條第一款：

建立對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。

個資事件通知

個資法第12條：

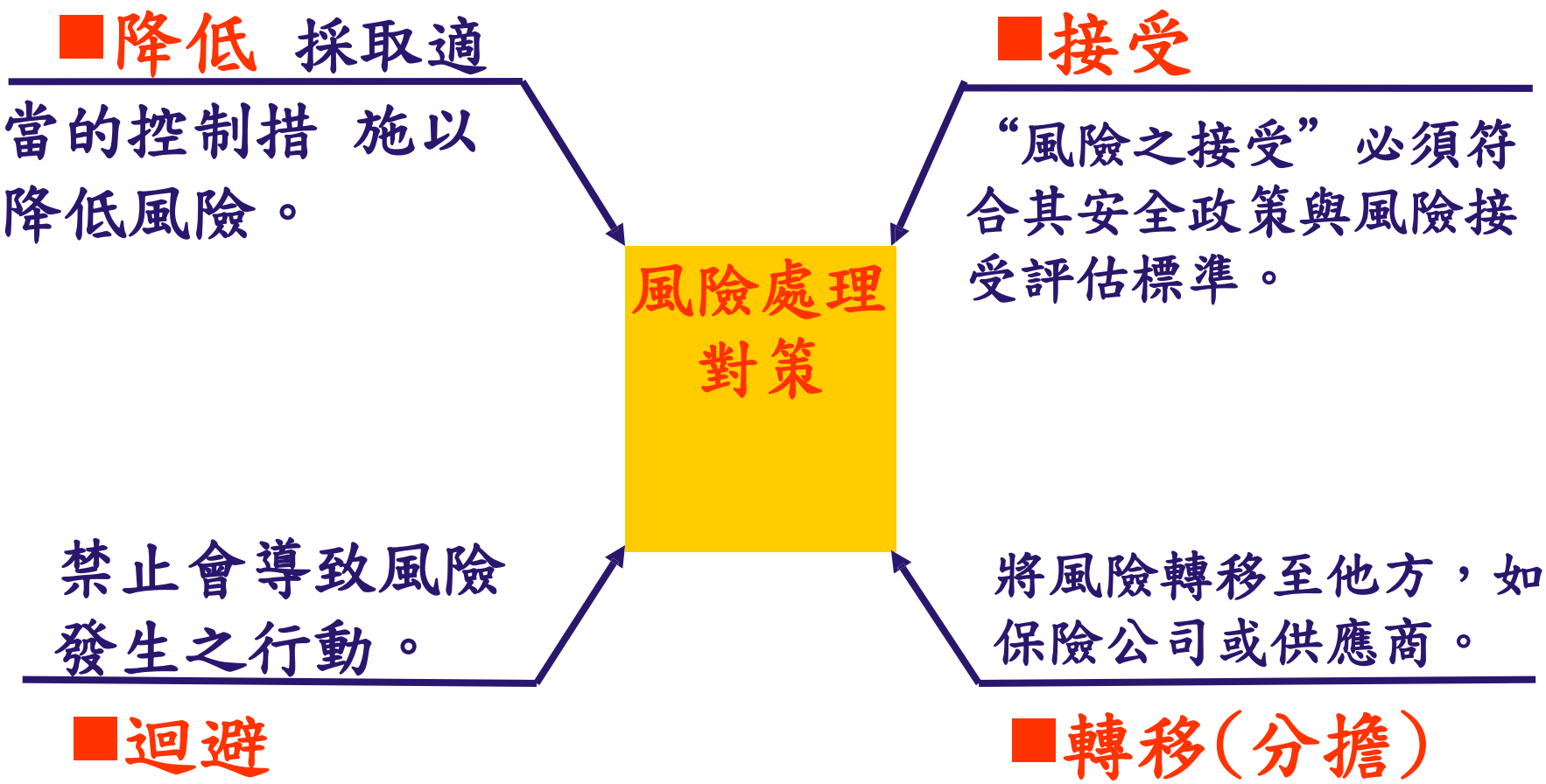
公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

風險管理之重點

◆控制不可接受風險與監督剩餘風險

- 剩餘風險包含未經鑑別出之風險、可接受之風險或因組織之限制因素必須承受之風險。
- 已進行控制之風險可能隨時間與技術演進會發生變化。
- 必須定期或因應不同之事件檢驗組織之風險。

決定風險與對策-風險處理對策



個人資料事件風險管理的目的

不是”100%”避開風險

而是去瞭解會面臨哪些風險，並藉由適當的手段與方法予以降低或轉移。

也不是去追求”最小風險”

而是讓企業組織選擇所能容忍的 風險水準，並排除無法承擔的風險。

風險管理應注意事項

- 進行風險管理應界定出管理之範圍。
- 風險不因任何控制措施而消滅、因此組織沒有零風險，即沒有百分之百安全。
- 風險管理在於適當識別出風險加以控 管，避免為分析而分析。
- 風險應該加以宣導並進行溝通，有效的 風險管理仰賴全體同仁共同維護。

第二章營運持續管理簡介

2-1 營運持續管理簡介

2-2 災難復原計畫簡介

2-1 營運持續管理簡介

營運持續計畫vs. 災難復原計畫

營運持續計畫

策略性

技術性

業務運作

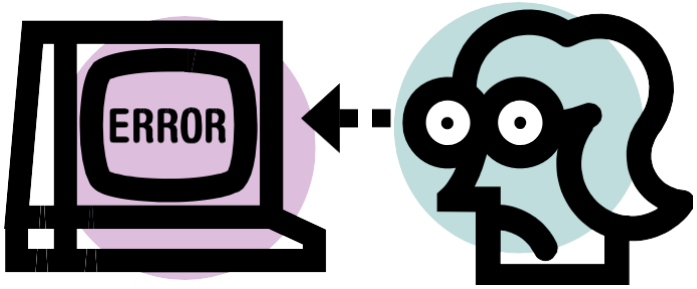
資訊運作

災難復原計畫

組織運作之風險

- **營運風險（Business Risk）**
  - 內部風險
  - 外部風險

- **作業風險（Operation Risk）**
  - 內部控制不足
  - 人為錯誤
  - 系統失效
  - 不當程序



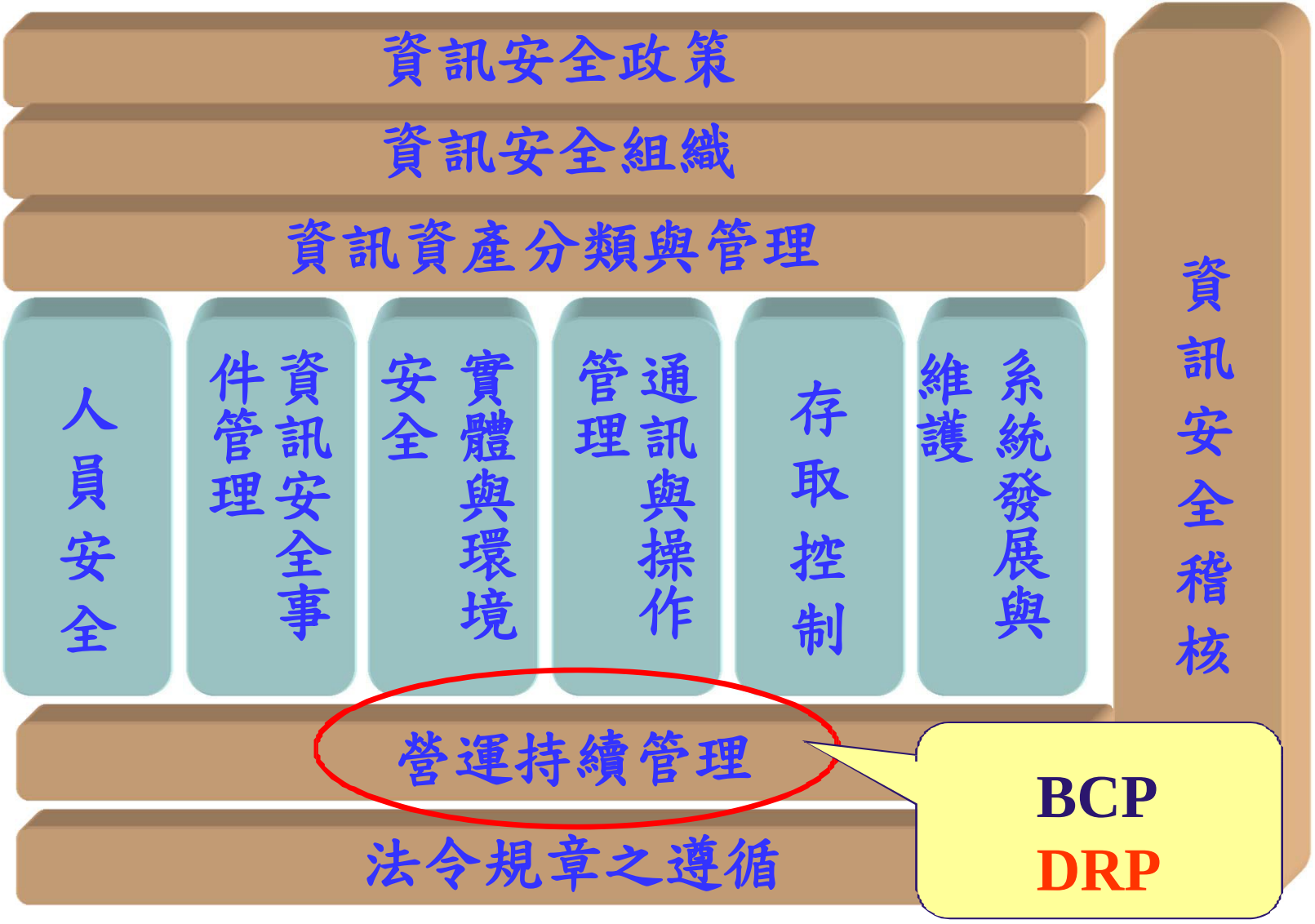
營運持續管理之重點

- 全面性的管理流程
- 機密性、完整性及可用性（CIA）保障與回復
- 法規法令的遵循
- 需要高層主管的全力支持!!

營運持續管理之目標

- 防止業務活動中斷，確保重要業務流程不受重大故障和災難的影響。
- 結合預防和復原措施，將風險造成的影響降低到可以接受的等級。
- 分析災難、安全缺失和服務損失的後果。制訂和實施應變計畫，確保在要求的時間內恢復作業。
- 選用控制措施降低風險，限制破壞性事件造成的後果，確保重要作業能及時復原。

CNS 27001對營運持續管理之要求



營運持續管理的分類

營運持續計畫（BCP）

負責在遭到破壞或系統中斷後支持組織的業務功能。

業務復原計畫（BRP）

負責緊急事件發生後，業務處理的復原。

災難復原計畫（DRP）

用於災難事件，在一段時間內對正常設備不能使用的情況下，在異地復原目標系統或IT設備的運轉。

異常事件回應計畫（IRP）

一套針對組織IT系統網路攻擊的處理過程，通常包括對惡意事件的識別、規避和恢復。

2-2災難復原計畫簡介

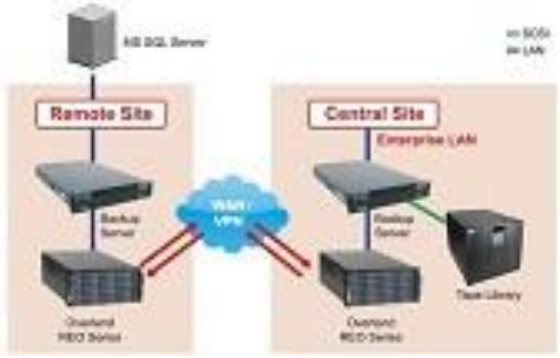
災難復原計畫的啟動時機

災難復原計畫之目的

- 災難復原的目的是將災難造成的影響減少到最小程度，並採取必要的步驟來保證資源、員工和業務流程能及時地繼續運行。
- 著重於面臨災難時如何回復資訊的完整和系統的正常運作。

災難復原計畫範例

- 確認損害原因
- 確認損害程度及影響範圍
- **選擇災難復原方案**
  - 人力復原
  - 環境復原
  - 硬體復原
  - 作業系統復原
  - 應用系統復原
  - 資料復原
- 測試運作
- 復原報告及紀錄



第三章營運衝擊分析與營運持續管理策略

3-1 營運衝擊分析

3-2 營運持續管理策略

3-1 營運衝擊分析

營運持續管理流程


設定營運持續管理目標
・辨識核心業務
・確立營運目標
營運衝擊分析
・辨識可能風險
・評估衝擊影響
營運持續計畫之撰寫與實施
・考量架構完整
・教育訓練
營運持續計畫測試與維護
・定期測試
・定期檢視更新

營運衝擊分析

- 原文：Business Impact Analysis，簡稱BIA。
- 衡量意外災難如果發生，它對系統的破壞會造成組織多大的損失。
- 可以用定量化或定性化的方法進行分析。
- 徵詢管理至使用者階層對資源的使用需求，來判別其依賴程度和重要性。

營運衝擊分析之目的

- 依照重要程度來定義不同作業程序的重要次序。
- 定義各資訊系統的最大可容忍停機時間；又或稱之為目標修復時間（RTO）。
- 在組織內形成營運持續的資安共識。
- 提供管理階層在訂定業務持續性策略和購置支援設備時的參考資料。

營運衝擊分析之步驟

- 確認組織核心業務。
- 確認核心業務所需資源。
- 確認可容許中斷時間和衝擊影響。
- 確立修復優先次序。

3-2 營運持續管理策略

營運持續管理策略之考量重點

- 資源分配
- 可行性分析
- 替代方案
- 成本效益分析
- 建議方案
- 管理階層之認可

營運持續管理策略之選擇

- **規避**：修改資訊作業方式或採用技術以避開風險。
- **轉嫁**：購置保險，將風險轉嫁另一個組織或機制。
- **接受**：認可風險之存在而不加以控制。
- **降低**：參考CNS 27001標準選擇適當之控管措施以降低風險。

第四章個人資料事件應變演練計畫擬定與實施

- 4-1個人資料事件應變演練計畫擬定
- 4-2個人資料事件應變演練計畫實施

4-1個人資料事件應變演練計畫擬定

應變程序及預防措施

- 可藉由平時定期之檢查與演練，降低事件發生後的衝擊程度，內容包括：
  - 建立應變程序。
  - 人員訓練

    藉由定期演練，提高相關人員危機意識及警覺心，亦能在個資事件發生後，迅速完成各項處理工作。

應變程序及預防措施

建立「個人資料事件應變演練計畫」，並定期演練，以利發生個資事件時，能夠立即通報各單位個人資料保護專責人員及相關人員，並掌握個資事件等級、通報程序、後續處理等事項。

個人資料事件應變演練計畫內容

- 計畫啟動條件
- 職責說明
- 緊急程序
- 備援程序
- 復原程序
- 維護時間表
- 認知教育訓練

組織及權責劃分

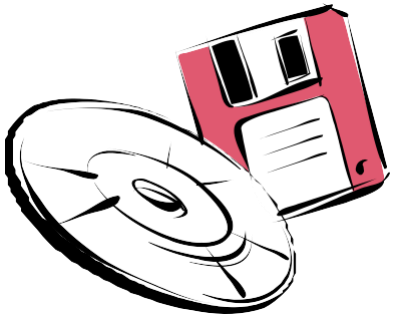
- 個資事件緊急應變演練小組成員由各單位主管、個資管理小組、個人資料保護專責人員編成。
- 分組職掌
  - 主管：管理個人資料事件。
  - 各單位個人資料保護專責人員：負責個人資料事件通報及擔任單位窗口。
  - 個資管理小組：協助各單位個人資料保護專責人員執行個人資料事件處理作業，管理及追蹤個人資料事件。

個人資料事件應變演練計畫宣導及訓練

- 計畫目標／作業標準
- 跨部門溝通協調
- 安全性考量
- 事件通報程序
- 個人責任與職責

預防性措施考量重點

- 實體性預防措施
- 資料備份
  - 資料備份系統
  - 替代性備援系統
  - 系統備品
- 人員管理
  - 人員角色和責任
- 預防成本vs. 應變成本
- 把修復機制設計在系統當中



4-2個人資料事件應變演練計畫實施

個人資料事件應變演練計畫實施注意事項

- 確定各項應變處理程序及權責。
- 與廠商或客戶間業務關係及合約的適切性。
- 處理程序及流程應文件化。
- 進行適當的員工訓練。
- 檢查並更新計畫。

- 計畫應著重具體的業務目標方面。
- 確定所需服務和資源，包括人員、非資訊處理資源的相關資源，以及資訊處理設備等項目。

應注意事項

- 相關單位之配合。
- 公告執行日期與時間。

第五章個人資料事件應變演練計畫測試、維護及再評估

- 5-1個人資料事件應變演練計畫之測試
- 5-2個人資料事件應變演練計畫之維護及再評估

5-1個人資料事件應變演練計畫之測試

執行演練

- 標準作業程序演練
- 團隊運作演練

測試方法

◆結構化排練測試：

– 由相關權責單位共同對處理方式進行逐項討論，並確認可行。

◆計畫表測試：

– 制訂計劃表，以便相關權責單位能夠利用此計畫表做測試。

◆模擬測試：

– 建立一個模擬的情境進行測試。

測試範圍及影響評估

- 有效性及風險
- 作業流程數量
- 資訊系統數量

5-2個人資料事件應變演練計畫之維護及再評估

定期檢視

- 定期檢討可用性
  - 實體環境
  - 安全性/技術性
  - 軟硬體設備/替代方案和備援系統
  - 人員
- 檢視外部支援的資源狀況
  - 委外廠商合約
  - 軟體合法授權

定期檢視（續）

- 定期檢討遵循性
  - 相關法規
  - 運作策略
- 定期檢視營運風險變化
  - 作業面
  - 財務面

不定期檢視

- 組織運作策略變動時。
- 採購新的設備，或是更新作業系統。
- 使用新的問題偵測及控制技術（例如火災偵測）。
- 使用新的環境控制技術。
- 人員及組織上的調整變動。
- 單位、人員地址及電話號碼的異動。

不定期檢視（續）

- 契約當事者或是供應商的調整變動。
- 業務流程的變動，新建或是撤銷作業流程。
- 實務作業的變更。
- 法規上的變更。

再評估

- 各部門之個人資料事件應變演練計畫是否與營運持續管理之目標相符。
- 所有重要及關鍵性風險是否已辨識。
- 是否有完整確實之教育訓練。
- 是否有足夠之操作手冊。
- 是否確實掌握應變措施之所有資源。
- 是否掌握組織最新資訊（人員及設備）。
- 是否掌握外界最新資訊。

個人資料事件應變演練計畫更新

- 再評估結果中前述各項因素改變，則應進行計畫更新。
- 更新計畫應依循原有程序進行各項作業。

營運持續管理之重要性

◆天災、人禍、意外…

◆風險無所不在，未雨綢繆，有備無患。

結論

- 營運持續管理可幫助組織通過關鍵考驗。
- 營運持續管理不僅限於資訊層面，組織所有運作均應納入考量。
- 應定期執行營運持續計畫測試並依現況調整。
- 應落實宣導及教育訓練。

情境演練

演練情境一

假想本校○○○單位將含有當事人個人資料（員工姓名、身份證字號、薪資水平、教育程度、技能證照、身心障礙手冊影本）之資訊系統委託給某委外廠商進行維護。

惟承辦人員未依個資法善盡監督與管理之責，委外廠商人員藉此監督漏洞謀私利，販售當事人個人資料給民間放款公司，且民間放款公司向當事人推廣放款資訊，新聞媒體收到消息並披露本案，導致本校個人資料保護形象受到質疑與面臨當事人向本校提出損害賠償主張。

情境演練

演練情境二

假想本校○○○單位將個人資料檔案（職稱、姓名、身份證字號、健康檢查紀錄）經由電子郵件寄送本校職員，因一時失察未將檔案加密且未選擇適當收件者後再寄出，導致該資料提供給本校所有同仁，造成個人資料外洩，並面臨當事人向本校提出損害賠償主張。

情境演練

演練情境三

假想本校○○○單位之個人資料（員工姓名、身份證字號、教育程度、戶籍謄本影本）存放於某資訊系統，已於100年6月下線，不再使用該資訊系統，惟仍發生個人資料外洩問題，新聞媒體收到消息並披露本案，導致本校個人資料保護形象受損與面臨當事人向本校提出損害賠償主張。

情境演練

演練情境四

假想本校○○○單位之個人資料（員工姓名、身份證字號、教育程度、工作紀錄）存放於辦公室儲物櫃，該辦公室儲物櫃於xxx年x月遭外力破壞並取走個人資料，新聞媒體收到消息並披露本案，導致本校個人資料保護形象受損與面臨當事人向本校提出損害賠償主張。

情境演練

演練情境五

假想本校○○○單位人員無權限取得個人資料（學生姓名、身份證字號、教育程度、手機連絡電話、歷年成績、考試證照），惟經由人際網絡間接獲得個人資料，並且兜售給民間公司，新聞媒體收到消息並披露本案，導致本校個人資料保護形象受損與面臨當事人向本校提出損害賠償主張。

Q&A

如有任何問題，歡迎隨時來電詢問 .....

SafeLink

博創資訊科技股份有限公司

臺中市西屯區國安一路208巷6號

TEL： 886-4-25250535

FAX： 886-4-24615268

http://www.safelink.com.tw/

E-mail: sam@safelink.com.tw