|  |
| --- |
| 範例十五：個資流程作業風險評估表 |

|  |  |
| --- | --- |
| 單位名稱 |  |
| 單位主管 |  |
| 評估人員 |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 作業流程名稱 | | 風險控管分類 | | | 衝擊值(A) | 個資侵害風險發生可能性(B) | 風險值 | 備註 | 單位名稱 |
| 主要業務、職掌 | 細部作業名稱 | 風險大分類 | 風險子分類 | 個資檔案控管措施(風險情境) | 從個人資料衝擊分析表將衝擊值帶入 | 5：控管嚴謹度低、經常被忽略、現行個資檔案控管方式沒有詳細規範。 | 風險值=個資作業流程衝擊值(A)×風險發生可能性(B) |
| 3：控管嚴謹度中等、偶發性被忽略、現行個資檔案控管方式僅有部分規範。 |
| 1：控管嚴謹度高、充分落實，現行個資檔案控管方式已有詳細規範。 |
| 0：不適用 |
|  |  |  |  |  |  |  |  |  |  |

|  |
| --- |
| 個資流程作業風險評估表填寫說明 |

|  |  |
| --- | --- |
| 欄位 | 填寫說明 |
| 主要業務、職掌 | 依個資流程衝擊分析表之「主要業務、職掌」欄位填寫。 |
| 細部作業名稱 | 依個資流程衝擊分析表之「細部作業名稱」欄位填寫。 |
| 風險大分類 | 依「細部作業名稱」囊括之個人資料檔案形態填入，詳細內容請參考風險情境表。  若「細部作業名稱」囊括之個人資料檔案含委外作業，則需加入委外作業類。 |
| 風險子分類 | 依前欄之風險大分類展開風險子分類逐一填入，詳細內容請參考風險情境表。 |
| 個資檔案控管措施(風險情境) | 依前欄之風險子分類展開該類別風險情境，詳細內容請參考風險情境表。 |
| 衝擊值 | 從個人資料衝擊分析表將衝擊值填入。 |
| 個資侵害風險發生可能性評估 | 以「個資侵害風險發生可能性」欄位所述級距進行評估。  於受評估之個資作業流程中，該風險情境不存在者，填「0」(不適用)。 |
| 風險值 | 個資作業流程衝擊值×風險發生可能性。 |
| 備註 | 任何可補充說明的資訊。 |
| 單位名稱 | 個資檔案所屬之單位名稱。 |

|  |
| --- |
| 個資流程作業風險評估表-填寫範例 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 作業流程名稱 | | 風險控管分類 | | | 衝擊值(A) | 個資侵害風險發生可能性(B) | 風險值 | 備註 | 單位名稱 |
| 主要業務、職掌 | 細部作業名稱 | 風險大分類 | 風險子分類 | 個資檔案控管措施(風險情境) | 從個人資料衝擊分析表將衝擊值帶入 | 5：控管嚴謹度低、經常被忽略、現行個資檔案控管方式沒有詳細規範。 | 風險值=個資作業流程衝擊值(A)×風險發生可能性(B) |
| 3：控管嚴謹度中等、偶發性被忽略、現行個資檔案控管方式僅有部分規範。 |
| 1：控管嚴謹度高、充分落實，現行個資檔案控管方式已有詳細規範。 |
| 0：不適用 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.1處理 | 1.1.1紙本文件於內部處理過程中，長時間不使用或下班時收存於辦公室上鎖之資料櫃。 | 12 | 1 | 12 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.2保存 | 1.2.1紙本文件之保存(含暫存區)地點具備進出管控措施。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.2保存 | 1.2.2紙本文件歸檔、入倉(庫)或集中保管前，確實清點數量及內容。 | 12 | 1 | 12 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.2保存 | 1.2.3紙本文件存放地點有消防、滅火、溫度控制等設施。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.3傳遞 | 1.3.1紙本文件於內部傳遞過程中，具有簽收/點收等控管措施。 | 12 | 5 | 60 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.3傳遞 | 1.3.2紙本文件提供外部利用均有公文往返等使用紀錄。 | 12 | 1 | 12 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.4銷毀 | 1.4.1包含個資之紙本文件均不進行回收使用。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.4銷毀 | 1.4.2紙本文件於內部進行銷毀時，均銷毀致無法辨識。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.4銷毀 | 1.4.3紙本文件交由受委託廠商銷毀前，已簽訂包含雙方權利義務及賠償條款之契約或保密協議。 | 12 | 5 | 60 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 1.紙本類 | 1.4銷毀 | 1.4.4紙本文件交由受委託廠商進行銷毀時，妥善進行監銷並留存紀錄。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.1選商 | 5.1.1委外案件均會評估及選擇可提供符合組織對個人資料保護需求之受委託廠商(如一年內未曾發生個資外洩事件、重大資安事件或有無通過ISO 27001、BS10012、TPIPAS、ISO29100等驗證)。 | 12 | 5 | 60 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.2簽約 | 5.2.1在委託外部單位處理個人資料有簽訂契約，並包含適當安控措施是否足夠。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.2簽約 | 5.2.2組織與受委託廠商所簽訂之契約中包含是否得將個人資料處理作業進行轉包/分包之規定。 | 12 | 1 | 12 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.2簽約 | 5.2.3若允許轉包/分包，受委託廠商與其複委託廠商(下包商)所簽訂之契約已要求複委託廠商實行與受委託廠商相同等級之安控措施。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.2簽約 | 5.2.4組織與受委託廠商所簽訂之契約中明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.3履約 | 5.3.1於委託外部單位處理個人資料契約期間內，定期監督或實地審查受委託廠商之安控措施是否落實執行。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.3履約 | 5.3.2組織定期依據與受委託廠商所簽訂之契約進行監督，當資料逾保存期限或契約終止時確認有關個人資料之銷毀、交還原組織或其他處理之方式。 | 12 | 3 | 36 | N/A | ○○科 |
| ○○○業務之規劃、推動與輔導 | ○○○活動報名作業 | 5.委外作業類 | 5.4小額採購 | 5.4.1如以小額採購方式委託外部單位蒐集、處理、利用或銷毀個人資料時，均簽訂書面協議並落實監督作業。 | 12 | 0 | 0 | N/A | ○○科 |