法規名稱：游離輻射設備製造業個人資料檔案安全維護管理辦法
修正日期：民國 112 年 12 月 21 日

第 1 條

本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第 2 條

本辦法之主管機關爲核能安全委員會（以下簡稱核安會）。

第 3 條

本辦法適用對象，指依游離輻射防護法第三十條規定，經營可發生游離輻射設備製造者（以下簡稱業者）。

第 4 條

1 業者應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討、修正及執行個人資料檔案安全維護計畫（以下簡稱安全維護計畫）。

2 前項安全維護計畫，應包括下列事項：

一、個人資料保護政策。
二、個人資料之範圍及項目。
三、個人資料之蒐集、處理及利用方式。
四、個人資料之安全管理及稽核措施。
五、個人資料被竊取、竄改、毀損、滅失或洩漏時之通報及應變機制。
六、業務終止後其保有個人資料之處理方法。
七、對所屬人員之個人資料保護教育訓練。
八、專責人員及聯絡窗口。

第 5 條

1 業者申請可發生游離輻射設備之製造許可時，應訂定並檢附安全維護計畫，報請核安會備查；計畫修正時，亦同。

2 業者應自本辦法發布施行之次日起六個月內，完成安全維護計畫之訂定，並報請核安會備查；安全維護計畫因本辦法修正有配合修正必要者，應自本辦法修正施行之次日起六個月內完成修正，並報請核安會備查。

第 6 條

1 業者應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。

2 業者經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理、利用之適當處置。

第 7 條

業者所屬人員爲執行業務所蒐集之個人資料，應視爲該業者所蒐集持有；於蒐集時，應檢視是否符合蒐集要件及特定目的之必要範圍，並受業者監督。

第 8 條

1 業者與當事人簽訂之委託書，應於委託期限屆至時，主動刪除或銷毀。但因執行業務之必要或經當事人書面同意者，不在此限。

2 業者對當事人刪除或銷毀委託書之請求，認有執行業務之必要者，得不予刪除或銷毀

，並應將其理由以書面通知當事人。

第 9 條

業者委託他人蒐集、處理或利用個人資料之全部或一部時，應於委託契約或相關文件明確約定其內容，並依本法施行細則第八條規定爲適當之監督。

第 10 條

業者就個人資料之蒐集、處理及利用，應符合本法規定，並於安全維護計畫內訂定下列個人資料管理程序：

一、蒐集、處理或利用之個人資料包括特種個人資料者，檢視其特定目的及是否符合本法第六條規定。

二、檢視個人資料之蒐集，是否符合本法第八條或第九條應明確告知，或得免爲告知之規定；並應明定告知之內容及方式。

三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定之特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條規定。

四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其爲特定目的外之利用者，檢視是否符合本法第二十條規定；經當事人同意者，並應確保符合本法第七條規定。

五、利用個人資料行銷，應於首次行銷時，提供當事人免費表示拒絕接受行銷之方式；當事人表示拒絕接受行銷者，應立即停止利用其個人資料行銷。

六、進行個人資料國際傳輸前，應檢視有無核安會依本法第二十一條規定所爲之限制，並告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方爲下列事項之監督：

（一）預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

（二）當事人行使本法第三條所定權利之相關事項。

七、當事人行使本法第三條所定權利之相關事項：

（一）當事人身分之確認。

（二）提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。

（三）對當事人請求之審查方式，並遵守本法有關處理期限之規定。

（四）有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。

八、維護個人資料正確性，對資料更正、補充、爭議、特定目的消失或期限屆滿、違法蒐集，應依本法第十一條規定辦理。

第 11 條

業者爲維護所保有個人資料之安全，應於安全維護計畫內，訂定下列資料安全管理措施：

一、訂定各類儲存設備、媒體或資訊系統之使用規範，及安裝設定防毒軟體、防火牆、入侵偵測、漏洞修復、監控機制、帳號管理、存取權限與其他適當防護措施。

二、各類儲存設備、媒體或資訊系統報廢或轉作他用時，應採取防範資料洩漏之適當措施。

三、對所保有個人資料有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。

四、對所保有個人資料傳輸作業時，採取適當之保護措施。

五、對所保有個人資料備份作業過程及所備份之資料，採取適當之保護措施。

第 12 條

1 業者應於安全維護計畫內，訂定應變機制；於發生個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害事件（以下簡稱事件）時，迅速處理。

2 前項應變機制，應包括下列事項：

一、採取適當之措施，控制事件對當事人造成之損害。
二、查明事件發生原因及損害狀況，以適當方式通知當事人，並設立服務窗口。
三、研議改進措施，避免事件再度發生。

3 業者應自發現事件時起七十二小時內，填列監督通報紀錄表（如附表）通報核安會；並自處理結束之日起一個月內，將處理方式及結果，通報核安會備查。

4 核安會接獲前項通報後，得依本法第二十二條至第二十五條規定，對發生第一項事件之業者，爲適當之監督管理措施。

第 13 條

業者業務終止後，不得繼續使用其保有之個人資料，並應於安全維護計畫內，訂定下列處理方式，並留存相關紀錄：
一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之依據。
三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

第 14 條

1 業者應於安全維護計畫內訂定教育訓練計畫，定期對所屬人員施以個人資料保護認知宣導及教育訓練。

2 前項認知宣導及教育訓練內容，得包括下列事項：
一、個人資料保護相關法令規定、資訊及案例。
二、第四條所列安全維護計畫各項管理程序、機制及措施之要求。
三、所屬人員之責任範圍。

第 15 條

業者爲維護所保有個人資料之安全，應採取下列人員管理措施：
一、識別接觸個人資料人員，與相關人員約定保密義務。
二、依執行業務之必要，設定相關人員之權限及控管，並定期檢視修正。
三、人員離職時，要求返還所保有之個人資料及載體，不得攜離並切結。

第 16 條

業者保有之個人資料儲存於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒體者，應採取下列設備安全管理措施：
一、依儲存設備或媒體之特性及使用環境，採取適當之保護措施。
二、對儲存設備或媒體，訂定適當之保管及管理權限。
三、針對存放儲存設備或媒體之環境，實施適當之門禁管制。

第 17 條

業者使用資訊服務系統，應採取下列資訊服務安全措施：
一、使用者身分確認及保護機制。
二、個人資料顯示之隱碼機制。
三、網際網路傳輸之安全加密機制。
四、個人資料檔案、資料庫之存取控制及保護監控措施。
五、防止外部網路入侵對策。
六、非法或異常使用行爲之監控及因應機制。

第 18 條

業者爲確保安全維護計畫之落實，應於安全維護計畫內訂定適當之個人資料安全稽核機

制，定期或不定期稽核安全維護計畫執行情形，製作稽核報告，並就缺失納入安全維護計畫之檢討修正。

第 19 條

業者爲持續精進個人資料安全維護，應參酌執行實務、技術發展、法令變化及其他相關因素，定期檢視或修正安全維護計畫。

第 20 條

業者執行安全維護計畫之下列紀錄，至少應保存五年。但其他法令另有規定或契約另有約定者，不在此限：

一、個人資料之蒐集、處理及利用紀錄。

二、自動化機器設備之軌跡資料。

三、執行、稽核或通報等相關報告或紀錄。

四、業務終止後之個人資料銷毀、移轉或其他措施之紀錄或證據。

第 21 條

本辦法自發布日施行。