○○股份有限公司個人資料檔案安全維護計畫

(游離輻射設備製造業)

(註：標題○○處請填寫公司名稱，以下全文內容得依貴公司營運實務自行增修) (範本)(V1120920 修正)

○○○年○○月○○日訂定
○○○年○○月○○日修正一版
○○○年○○月○○日修正二版

一、個人資料保護政策**(註：項目名稱依據「安全維護管理辦法」第四條)**

(一)○○股份有限公司(以下簡稱「本公司」)為落實個人資料之保護管理，並遵循「個人資料保護法」(以下簡稱「個資法」)之規定，依據「游離輻射設備製造業個人資料檔案安全維護管理辦法」(以下簡稱「安全維護管理辦法」)之規定，訂定「個人資料檔案安全維護計畫」(以下簡稱「本計畫」)。**(註：○○處請填寫公司名稱)**

(二)本計畫之目的，在兼顧個人隱私權的保護及個人資料的合理利用，建立本公司對個人資料蒐集、處理及利用之程序，落實對個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，並尊重當事人對權利之行使及諮詢。**(註：得依貴公司既有宣告之政策增修)**

二、個人資料之範圍及項目**(註：項目名稱依據「安全維護管理辦法」第四條)**

(一)特定目的：

本公司個人資料蒐集、處理及利用之範圍，為游離輻射設備製造及其相關之銷售與代理銷售、○○○○○○之業務，包括契約相關文書、法律關係事務、客戶管理與服務、○○○○○○，及本公司人事管理與依法辦理之員工健康檢查。**(註：○○處請依實務增修)**

(二)客戶個人資料：

指本公司依前項特定目的之需求，包含本公司所屬人員為執行業務所需，蒐集客戶之個人資料，包含姓名、國民身分證統一編號、護照號碼、聯絡方式、○○○○○○，及其他得以直接或間接方式識別該個人之資料。

(註：○○處請依實務增修)

(三)所屬人員個人資料

(含員工、業務、兼職、委外、派遣、顧問、○○等人員)：

指本公司依前項特定目的之需求，蒐集所屬人員之人事管理、教育訓練、○○○○○○、依法辦理之員工健康檢查等個人資料，包含姓名、出生年月日、國民身分證統一編號、護照號碼、婚姻、家庭、教育、職業、健康檢查、聯絡方式、○○○○○○，及其他得以直接或間接方式識別該個人之資料。**(註：○○處請依實務增修)**

三、個人資料之蒐集、處理及利用方式**(註：項目名稱依據「安全維護管理辦法」第四條)**

(一)依前條個人資料蒐集之特定目的及必要性，蒐集、處理及利用個人資料，並定期清查所保有之個人資料現況。**(註：依據「安全維護管理辦法」第六條)**

(二)本公司所屬人員為執行業務所蒐集之個人資料，均視為本公司所蒐集持有；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，並受本公司監督。**(註：依據「安全維護管理辦法」第七條)**

(三)本公司委託他人蒐集、處理或利用個人資料之全部或一部時，均視為本公司所蒐集持有；本公司應對受託者依個資法施行細則第八條規定為適當之監督，並於委託契約或相關文件明確約定其內容。**(註：依據「安全維護管理辦法」第九條)**

(四)對所蒐集、處理及利用之個人資料包括特種個人資料者，檢視其特定目的，及是否符合個資法第六條「不得蒐集、處理或利用」及「明確告知當事人」之規定。**(註：以下(四)~(十一)項均依據「安全維護管理辦法」第十條)**

(五)檢視個人資料之蒐集，是否符合個資法第八條或第九條應明確告知，或得免為告知之規定；並應明定告知之內容及方式。

(六)檢視個人資料之蒐集、處理，是否符合個資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，並應確保符合個資法第七條規定。

(七)檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合個資法第二十條規定；經當事人同意者，並應確保符合個資法第七條規定。

(八)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。

(九)進行個人資料國際傳輸前，應檢視有無核安會依個資法第二十一條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域，同時本公司對資料接收方為下列事項之監督：

1. 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。
2. 當事人行使個資法第三條所定權利之相關事項。

(十)對當事人行使個資法第三條所定權利之相關事項：

1. 對當事人身分之確認。
2. 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。
3. 對當事人請求之審查方式，並遵守個資法有關處理期限之規定。
4. 有個資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。

(十一) 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，應依個資法第十一條規定辦理。

(十二) 指定專責人員定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之個人資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他停止蒐集、處理、利用之適當處置。**(註：依據「安全維護管理辦法」第六條)**

(十三) 本公司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。

本公司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。**(註：依據「安全維護管理辦法」第八條)**

四、個人資料之安全管理及稽核措施**(註：項目名稱依據「安全維護管理辦法」第四條)**

(一)資料安全管理

1. 管理措施**(註：依據「安全維護管理辦法」第十一條)**

(1)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。

(2)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。

(3)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。

(4)對所保有個人資料傳輸作業時，採取適當之保護措施。

(5)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。

2. 電腦個人資料存取

(1)儲存個人資料檔案之電腦設備，應設置使用者代碼(帳號)及識別密碼、螢幕保護程式密碼之登入及相關安全措施。

(2)本公司所屬人員如因其工作執掌相關而須輸出、輸入個人資料時，均須以其個人之使用者代碼(帳號)及識別密碼登入，同時在使用範圍及權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

(3)個人資料檔案使用完畢應即登出系統或關閉檔案，不得任其停留於電腦螢幕上。

(4)重要個人資料應另加設管控密碼，非經陳報所屬主管同意，並取得密碼者，不得存取。

(5)定期進行電腦系統防毒、掃毒、安全性更新等資訊安全措施。

(6)禁止使用私人可攜式電腦設備(例如筆記型電腦、平板電腦等)、儲存媒體(例如外接式硬式磁碟、光碟、隨身碟、記憶卡等)或行動裝置(例如行動電話等)儲存本公司所保有個人資料檔案。

3. 紙本個人資料保管

(1)對於各類委託書、契約書件(含個人資料表)應存放於公文櫃內並上鎖，所屬人員非經所屬主管同意不得任意複製或影印。

(2)對於記載個人資料之紙本丟棄時，應先以碎紙設備或水銷等方式進行處理。

(二)人員權限管控(註：依據「安全維護管理辦法」第十五條)

1. 識別本公司接觸個人資料人員，與相關人員約定保密義務，並簽訂保密切結書(如在任職時之相關勞務契約已有所約定時，亦屬之)。
2. 依本公司執行業務之必要，得設定相關人員之權限，以控管其個人資料之存取，並定期檢視修正。
3. 本公司所屬人員應定期變更識別密碼，並於變更識別密碼後始可繼續使用電腦。
4. 本公司所屬人員應妥善保管個人資料之儲存媒體，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。
5. 本公司所屬人員離職及終止僱傭或委任契約時，立即取消其使用者代碼(帳號)及識別密碼，並要求返還所保有之個人資料及載體，不得攜離並切結。
6. 本公司所屬人員所簽訂之相關勞務契約或承攬契約均訂定保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務(含契約終止後)。

(三)設備安全管理(註：依據「安全維護管理辦法」第十六條)

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：

1. 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。

(1)儲存個人資料檔案之電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。

(2)儲存個人資料檔案之電腦設備，不得直接作為公用電腦使用。

(3)個人資料檔案應定期備份，重要個人資料備份應異地存放，並防止資料滅失或遭竊取。

(4)儲存個人資料檔案之電腦設備及儲存媒體需報廢、汰換或轉作其他

用途時，所屬主管應檢視該電腦設備及儲存媒體所儲存之個人資料是否確實刪除或破壞。

2. 對儲存設備或媒體，訂定適當之保管及管理權限。

(1)儲存個人資料檔案之電腦設備、儲存媒體及資料檔案，應指派專責人員管理，非經所屬主管同意並作成紀錄，不得攜帶外出或拷貝複製。

(2)儲存個人資料檔案之電腦設備，應設置使用者代碼(帳號)及識別密碼、螢幕保護程式密碼之登入及相關安全措施。

3. 針對存放儲存設備或媒體之環境，實施適當之門禁管制。

(四)資訊服務系統採取之資訊服務安全措施**(註：依據「安全維護管理辦法」第十七條)(若未使用「資訊服務系統」，本項不適用，請刪除)**

1. 使用者身分確認及保護機制：

針對資通系統或個資檔案存取，提供使用者識別、鑑別及身分驗證管理機制，例如：帳號及密碼管制、多重認證技術、帳戶鎖定機制、密碼具一定複雜度等。

2. 個人資料顯示之隱碼機制：

系統呈現介面上，如有個資資訊，應評估使用情境，予以適當且一致性之遮蔽，例如「＊」、「○」等符號，以為資訊保護。

3. 網際網路傳輸之安全加密機制：

當個人資料進行網路傳輸時，應採用加密機制，包含使用加密傳輸管道、資料加密傳輸等。

4. 個人資料檔案、資料庫之存取控制及保護監控措施：

針對個人資料檔案及資料庫之儲存，應適當加密。存取時，應提供使用者識別、鑑別及身分驗證管理機制。留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。

5. 防止外部網路入侵對策：

針對可能來自於網路的入侵，採取相關的偵測或防護作為。例如個人電腦安裝防毒軟體、使用電子郵件過濾機制、設定網路防火牆、架構

應用程式防火牆、採用入侵偵測及防禦機制或進階持續性威脅攻擊防禦措施等。

6. 非法或異常使用行為之監控及因應機制：
   針對資通系統或個資檔案之存取，留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。

(五)監督及稽核措施(註：依據「安全維護管理辦法」第十八條)

1. 使用紀錄、軌跡資料及證據保存，包含個人資料使用及查詢紀錄、電腦設備之軌跡資料、○○○○○○，應製作備份，保存於適當處所。
   (註：○○處請依實務增修)
2. 每年定期辦理個人資料檔案安全維護稽核，以落實本計畫之執行，針對缺失及潛在之風險，應規劃改善及預防措施，並依下列方式辦理：
   (1)確認缺失及潛在風險之內容及發生原因。
   (2)提出改善及預防措施。
   (3)紀錄稽核情形及結果。
3. 前項稽核情形及結果應載入稽核報告中，公司負責人或授權主管須簽名確認，相關紀錄至少保存五年備查。
4. 針對個人資料檔案安全維護稽核結果不符合法令之虞者，規劃改善與預防措施，並就缺失納入安全維護計畫之檢討修正。

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(註：項目名稱依據「安全維護管理辦法」第四條，內容依據「安全維護管理辦法」第十二條)

(一)發現個人資料遭竊取、竄改、毀損、滅失或洩漏事件時，立即向公司負責人或授權主管通報。

(二)採取適當之措施，控制事件對當事人造成之損害。

(三)查明事件發生原因及損害狀況，以適當方式通知當事人，說明本公司已採取之處理措施，並設立服務窗口提供諮詢專線。

(四)針對事件發生原因研議改進措施，避免事件再度發生。

(五)依規定，自發現事件時起 72 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 1 個月內，將處理方式及結果，通報核安會備查。

六、業務終止後其保有個人資料之處理方法**(註：項目名稱依據「安全維護管理辦法」第四條，內容依據「安全維護管理辦法」第十三條)**

本公司業務終止後，不得繼續使用所保有之個人資料，應依下列方式處理，並留存相關文件、照相、錄影紀錄備查：

(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。

七、對所屬人員之個人資料保護教育訓練**(註：項目名稱依據「安全維護管理辦法」第四條，內容依據「安全維護管理辦法」第十四條)**

(一)本公司每年進行個人資料保護法相關教育訓練至少一次，使所屬人員知悉應遵守之規定，課程資料及簽到名冊等相關紀錄，至少保存五年備查。

(二)教育訓練內容得以專題演講、網路影音、○○○○等形式辦理，內容包括：**(註：○○處請依實務增修)**

1. 個人資料保護相關法令規定、資訊及案例。
2. 安全維護計畫各項管理程序、機制及措施之要求。
3. 所屬人員之責任範圍。

(三)對新進人員應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

八、專責人員及聯絡窗口**(註：項目名稱依據「安全維護管理辦法」第四條)(註：○○處請填寫)**

本公司專責人員為○○部門(部門名稱)○○○職稱(姓名)

連絡電話：(00) 0000-0000 轉 000

行動電話：0000-000-000

電子郵件信箱：XXX@XXX.com.tw

九、紀錄保存**(註：依據「安全維護管理辦法」第二十條)**

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。

十、本公司將隨時依據計畫執行實務、技術發展及法令修正等，定期檢視本計畫是否合宜，並予必要之修正後，報請主管機關備查後實施。**(註：依據「安全維護管理辦法」第十九條)**

【行政院國家發展委員會建議事項】

事業單位得加入台灣電腦網路危機處理暨協調中心(TWCERT/CSIRT)以獲得適當情資與強化防護能量。

附表

<table>
<tr><th colspan="3">游離輻射設備製造業個人資料外洩事件監督通報紀錄表</th></tr>
<tr><td rowspan="6">通報公司名稱：
○○股份有限公司
通報機關：
核能安全委員會</td><td colspan="2">通報時間：　　年　　月　　日　　時　　分</td></tr>
<tr><td colspan="2">通報人：　　簽名(蓋章)</td></tr>
<tr><td colspan="2">職　稱：</td></tr>
<tr><td colspan="2">電　話：</td></tr>
<tr><td colspan="2">E-mail：</td></tr>
<tr><td colspan="2">地　址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2">年　　月　　日　　時　　分</td></tr>
<tr><td>事件發生種類</td><td>☐ 竊取
☐ 洩漏
☐ 竄改
☐ 毀損
☐ 滅失
☐ 其他侵害事件</td><td>個人資料侵害之總筆數(大約)
＿＿＿＿＿筆
☐ 一般個人資料＿＿＿＿＿筆
☐ 特種個人資料＿＿＿＿＿筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2">【註】依個資法規定，委託單位應監督受託單位採取之安全維護措施是否適當等，並做成紀錄。非僅敘述受託單位之缺失及改善措施，亦應說明委託單位對受託單位採行之監督措施。</td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2">【註】依個資法規定，發生個資外洩事件時應將個人資料被侵害之事實及已採取之因應措施通知當事人。非僅提醒當事人勿被詐騙，並未確實告知。</td></tr>
<tr><td>是否於發現個人資料外洩後 72 小時內通報</td><td colspan="2">☐是
☐否，理由：</td></tr>
</table>