○○租賃住宅服務業個人資料檔案安全維護計畫及業務終止後個人資料處理方法(範本)

111年1月3日修正

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「內政部指定地政類非公務機關個人資料檔案安全維護管理辦法」之規定，非公務機關應訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法)。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，爰訂定本計畫及處理方法。

壹、租賃住宅服務業之組織、規模及特性

一、組織型態：股份有限公司、有限公司

二、經營型態：直營或加盟

三、資本額：新台幣○○○萬元整

四、處所地址：○○市○○區○○路（街）○段○號○○樓

五、代表人（負責人)：○○○

六、員工人數：（可記載一定範圍之人數)

七、特性：執行租賃住宅之屋況與設備點交、收租與押金管理、日常修繕維護、糾紛協調處理及其他與租賃住宅管理有關之事項。

貳、個人資料檔案之安全維護管理措施

一、管理人員及資源

（一）管理人員：

1、配置人數：○人。(不分直營或加盟體系，亦或是自有品牌之業者，建議至少配置1名管理人員)

2、職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項，並向負責人提出報告。

（二）預算：每年新台幣○○萬元。(依實際狀況填寫)

（三）個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、篡改、毀損、滅失或洩漏。

二、界定蒐集、處理及利用個人資料之範圍

（一）特定目的：本公司個人資料蒐集、處理及利用之範圍，為租賃住宅管理、租賃住宅包租及轉租、物業管理、課程推廣之業務，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。

（二）客戶個人資料：

本計畫所稱之客戶個人資料，除係指客戶姓名、出生年月日、國民身分證統一編號(護照號碼、外僑統一證號)、婚姻、家庭、教育、職業、聯絡方式外及其他得以直接或間接方式識別該個人之資料。

（三）租賃住宅管理人員或所屬員工個人(含員工、業務、兼職、委外、派遣、顧問、講師等人員)資料：指本公司依特定目的之需求，蒐集所屬人員之人事管理、教育訓練等個人資料，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、聯絡方式，及其他得以直接或間接方式識別該個人之資料。

三、風險評估及管理機制

（一）風險評估

1、經由本公司電腦下載或外部網路入侵而外洩。

2、經由接觸書面契約書類而外洩。

3、本公司與各營業處所間或商業間互為傳輸時外洩。

4、員工故意竊取、毀損或洩漏。

（二）管理機制

1、藉由使用者代碼、識別密碼設定及文件妥適保管。

2、定期進行網路資訊安全維護及控管。

3、電磁資料視實際需要以加密方式傳輸。

4、加強對員工之管制及設備之強化管理。

四、事故之預防、通報及應變機制

（一）預防：

1、本公司員工或所屬之租賃住宅管理人員如因其工作執掌而須輸

出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。

2、非承辦之租賃住宅管理人員或員工參閱契約書類時，應得公司負責人、營業處所主管或經指定之管理人員同意。

3、個人資料於本公司與各營業處所間或受委託之公司或商業間互為傳輸時，加強管控避免外洩。

4、加強員工教育宣導，並嚴加管制。

（二）通報及應變：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向公司負責人、營業處所主管或經指定之管理人員通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

2、對於個人資料遭竊取之客戶，以書面或通常方式通知使其知悉及本公司已採取之處理措施及諮詢服務專線。

3、個人資料事故發生後以書面通報○○市（縣）政府地政局(處)。遇有達1,000筆以上之個人資料事故時，應於發現後72小時內，以書面（格式如附件一）通報○○市（縣）政府地政局(處)，並副知內政部。

4、針對事故發生原因研議改進措施。

五、個人資料蒐集、處理及利用之內部管理措施

（一）直接向當事人蒐集個人資料時，應明確告知以下事項：a.公司名稱、加盟品牌名稱。b.蒐集目的。c.個人資料之類別。d.個人資料利用之期間、地區、對象及方式。e.當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

（二）所蒐集非由當事人(或客戶)提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。

（三）與客戶簽訂之委託書，如獲得客戶書面同意，得進行個人資料蒐集、處理及利用。

（四）利用個人資料為行銷時，當事人（或客戶）表示拒絕行銷後，應立即停止利用其個人資料行銷。當事人表示拒絕接受行銷之日起7日內，直營店應將拒絕情形通報總公司彙整後再周知所屬各部門；加

盟店應通知內部其他業務人員；加盟店所蒐集之個人資料若有上傳加盟總部者，亦應同時通知加盟總部。

（五）中央主管機關對租賃住宅服務業為限制國際傳輸個人資料之命令或處分時，通知所屬人員遵循辦理。所屬人員於個人資料進行國際傳輸時，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域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.當事人行使本法第3條所定權利之相關事項。

（六）客戶表示拒絕行銷或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，連絡窗口為：○○○ ；電話為：○○○○○○。並將聯絡窗口及電話等資料，揭示於本公司營業處所或公司網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

（七）負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

（八）本公司員工或所屬之經紀人員如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（九）由指定之管理人員定期查核確認所保有之個人資料現況，並界定納入本計畫及業務終止後之個人資料處理方法之範圍。

（十）本公司要求所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合個人資料保護法（以下簡稱個資法）第19條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合個資法第20條第1項但書情形。

（十一）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、處理或利用等適當之處置。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

（十二）本公司如有委他人（或他公司）蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。

（十三）本公司因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

六、設備安全管理、資料安全管理及人員管理措施

（一）、設備安全管理

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、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。

4、儲存個人資料檔案之公司雲端儲存設備(例如 NAS、伺服器等)，應指派專責人員管理，限定連線人員名單已最小權限原則來給予使用權限，非經所屬主管同意不得連線使用查閱公司雲端儲存設備，不得擅自發送公司雲端儲存設備連結。

5、個人資料檔案應定期備份，重要個人資料備份應異地存放，並應置有防火設備及保險箱等防護設備，以防止資料滅失或遭竊取。

6、防火牆設備設定增加黑名單與白名單，名單外一律禁止。

7、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物需報廢汰換或轉作其他用途時，本公司負責人、營業處所主管或經指定之管理人員應檢視該設備所儲存之個人資料是否確實刪除。委託他人執行者，當對受託者為適當之監督並與其明確約定相關監督事項。

（二）資料安全管理

1、電腦存取個人資料之管控：

（1）個人資料檔案儲存在電腦硬式磁碟機上者，應在個人電腦設置識別密碼、保護程式密碼及相關安全措施。

（2）本公司員工或所屬租賃住宅管理人員如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別

密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（3）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。

（4）個人資料檔案使用完畢應即退出，不得任其停留於電腦終端機上。

（5）定期進行電腦系統防毒、掃毒之必要措施。

（6）重要資料(例如 Excel、Word、PDF 等)應加設管控密碼以及公司浮水印，非經權責單位主管、各營業處所主管或經指定之管理人員核可，不得被閱讀、修改、以及重製。

2、紙本資料之保管：

（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，員工或所屬租賃住宅管理人員非經公司負責人、營業處所主管或經指定之管理人員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，應先以碎紙設備進行處理。

3、因本公司所使用資通訊系統蒐集、處理或利用消費者個人資料達1萬筆以上，爰針對該資通訊系統，採取下列資訊安全措施，並針對第5目及第6目措施定期演練及檢討改善：

（1）使用者身分確認及保護機制。

（2）個人資料顯示之隱碼機制。

（3）網際網路傳輸之安全加密機制。

（4）個人資料檔案及資料庫之存取控制與保護監控措施。

（5）防止外部網路入侵對策。

（6）非法或異常使用行為之監控與因應機制。

（三）人員管理

1、員工需依其業務、職務需求設定不同之權限，以控管其個人資料蒐集、處理與利用之情形。

2、資訊部門應檢視各相關業務之性質，指派人員負責規範個人資料蒐集、處理及利用等流程。

3、員工應妥善保管個人資料之儲存媒介物，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。

4、員工離職應立即取消其使用者帳號及識別密碼。其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書。

5、員工所簽訂之相關勞務契約或承攬契約均列入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，保密義務期限包含至契約終止後。

6、員工電腦設備應定期6個月變更識別密碼1次，並於變更識別密碼後始可繼續使用電腦。

7、員工使用紙本個人資料應隨時收藏整理，未用時應存放於櫃內並上鎖，不得任意放置於桌上或第三人可以任意取得之處。

七、認知宣導及教育訓練

(一)本公司每年進行個人資料保護法相關教育訓練至少1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1年備查。

(二)教育訓練內容得以法規宣導、專題演講、網路影音等形式辦理。

(三)對於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、資料安全稽核機制

（一）本公司定期(每半年至少1次)辦理個人資料檔案安全維護稽核，查察本公司是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1、確認不符合事項之內容及發生原因。

2、提出改善及預防措施方案。

3、紀錄查察情形及結果。

（二）前項查察情形及結果應載入稽核報告中，由公司負責人或其授權指定主管人員簽名確認，稽核報告至少保存5年。

九、使用記錄、軌跡資料及證據保存

(一)公司建置個人資料之電腦，其個人資料使用查詢紀錄檔，每年定期

備份加密1次，留存相關軌跡資料、相關證據及紀錄，並將該紀錄檔之儲存媒介物保存於適當處至少5年。

(二)個人資料電子簽章使用紀錄檔，每年定期備份加密1次，留存相關軌跡資料、相關證據及紀錄，並將該紀錄檔之儲存媒介物保存於適當處至少5年。

(三)個人資料存證使用紀錄檔，每年定期備份加密1次，留存相關軌跡資料、相關證據及紀錄，並將該紀錄檔之儲存媒介物保存於適當處至少5年。

(四)紙本個人資料之使用與調閱，應以系統表單提出需求，非經權責單位主管、各營業處所主 管或經指定之管理人員同意，不得任意取出，並將表單需求與主管授權紀錄等相關紀錄，儲存媒介物保存於適當處至少5年。

十、個人資料安全維護之整體持續改善

（一）本公司將隨時依據計畫執行狀況，注意相關社會輿情、技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正，並於規定期限內報請所在地直轄市、縣（市）主管機關備查。

（二）針對個資安全稽核結果不符合法令之虞者，規劃改善與預防措施。

十一、業務終止後之個人資料處理方法

本公司業務終止後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，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合法依據。

（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。

租賃住宅服務業名稱：　　（簽章）

法定代表人：

統一編號　：

聯絡電話　：

電子信箱　：

通訊地址　：

附件一

<table>
<tr><td colspan="3">個人資料事故通報及紀錄表</td></tr>
<tr><td>非公務機關名稱
_____

通報機關

_____</td><td colspan="2">通報時間：
年　月　日　時　分
通報人：
簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個人資料_____筆
□特種個人資料_____筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後七十二小時內通報</td><td colspan="2">□是　□否，理由：</td></tr>
</table>

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。