○○公寓大廈管理維護股份有限公司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(草案範例)

一、依據：

依個人資料保護法（以下簡稱本法）第二十七條第三項規定，及內政部110.11.30台內營字第1100817867號令訂定發布，訂定本公司「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」。

二、目的：

為維護個人資料檔案安全，特依據內政部所令頒之「個人資料檔案安全維護管理辦法及業務終止後個人資料處理方法」，訂定本公司之個人資料檔案安全維護計畫，以防止員工個人資料遭竊取、竄改、毀損或洩漏。

三、本公司就現有員工之個人資料由人事部門統一集中保管，並由各事業部門將個人資料予以分類保管，且設置專櫃儲存；有關安全維護管理依據內政部所頒「指定營建類非公務機關個人資料檔案安全維護管理辦法」第五條至第二十三條規定，訂定適當之安全維護管理措施，本計畫包括如后：

(一)組織規模方面：本公司資本額○仟萬元整，公司運作設董事長(總經理)、副董事長(副總經理)，下設內勤(業務部：總務、人事、會計)，外勤(勤務部：勤務隊、機動小組、稽核小組)，分屬內勤與外勤經理，負責指導、協調、調度與指揮，個人資料檔案之安全維護及管理由內勤業務部人事承辦人負責。

(二)個人資料檔案安全維護管理措施：

1.公司由副總經理負責規劃、訂定、修正及執行計畫或業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。

2.錄取之員工個人資料（包含家庭狀況、連絡電話、身份背景等）由人事檔案員將個人資料建立人事電腦系統內，並分類各事業部門人資，俾利檔案管理。

3. 鑑別個人資料所存在之各項衝擊及威脅所導致之風險，並依據風險評估之傑果採取技術面之對策(接受降低轉移迴避風險)或安全控制措施，以防止個人資料被竊取、竄改、滅失、或洩漏。
4. 保有之個人資料發生被竊取、洩漏、竄改或其他侵害事故時，迅速處理以保護當事人之權益,控制事故對當事人造成損害,查明事故發生原因及損害狀況，並以適當方式通知當事人事故事實、因應措施及諮詢服務專線(02-00000000),若有發生重大個人資料事故者，應於發生後七十二小時內，以書面通報主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關；如為直轄市、縣（市）主管機關接獲通報，並應副知中央主管機關。(通報格式如附件一)
5. 個人資料之蒐集存取應與本身業務範圍相關，任何人未經授權不得存取與個人業務無關之個人資料，針對存有個人資料之紙本文件及可攜式儲存媒體，如資料有加密之必要，即採取適當之加密機制；對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖；或實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體，處理勤務主管應確實注重保密，嚴禁對非相關人員洩漏個資。
6. 確保個人資料存放環境與設備之安全，避免未經授權之人員進出辦公環境,若發現身份不明或可疑的人員,應主動詢問其身份,並視需要通知副總經理處理。處理或儲存個人資料之資訊設備,應規劃安全防護程序,或採取適當隔離控管措施，留意陌生人員進出辦公環境,訪客(應徵人員)應指定之區域內活動。

7. 人事（檔案）管理人員需確實遵守本辦法規定，嚴禁對非相關人員透漏員工個人資料，若有洩漏個資之情形，將依個人資料保護法第 41 條規定辦理。
8. 設備安全暨資料安全管理，統一由負責人事之人員負責檔案人員管理，並由副總經理稽核，確認個人資訊管理制度實施之有效性與落實情形。每年至少辦理一次內部稽核,並針對控管結果之不符合事項與潛在風險，規劃改善及預防措施。
9. 人事（檔案）管理人員，將員工之資料存檔於人資系統後，應建立備份資料，離職員工應另設資料存檔，以保存證據。
10. 個人資料安全維護之整體作業及規劃,人事系統檔案需建立密碼，除承辦人員使用外，任何人不得任意操作，檔案人員應定期及不定期應審查有無缺失,一經發現有作業上之問題,應即採取因應作為，以防堵資料外洩之情形。
11. 業務終止後之個人資料之處理，統一造冊登錄後銷毀，並由副總經理監督。

四、本計畫訂後報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

五、本公司辦理本法配置人事（檔案）管理人員，並由副總經理負責規劃、訂定、修正及執行計畫或業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。

本公司依據個人資料保護管理之政策，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於公佈欄內，並用公司網站揭露於網站首頁，使所屬人員及個人資料當事人均能知悉。

六、本公司在對於個人之彙整及處理及利用個人資料之類別及範圍，每季清查所保有個人資料檔案之現況。

依前項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，人事（檔案）管人員並應留存相關紀錄。

七、本公司在界定蒐集、處理與利用個人資料之類別、範圍及流程，分析評估可能發生之風險，擬訂定適當之管控措施，以杜絕個人資料外洩情事發生。

八、因應保有之個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱個人資料事故），應採取下列應變、通報及預防機制：

(一)採取適當之應變措施，以控制個人資料事故對當事人之損害，並通報內部有關單位。

(二)查明個人資料事故之狀況並以適當方式通知當事人有關個人資料事故事實、所為因應措施及諮詢服務專線等內容。

(三)研議預防機制，避免類似個人資料事故再次發生。

九、本公司勤務主管及人事（檔案）管理人員，為執行業務蒐集個人資料時，應檢視符合蒐集要件及特定目的之必要範圍，並接受副總經理之監督。

十、本公司在蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求勤務主管及人事（檔案）管理人員確實辦理。

十一、依據中央主管機關依本法第二十一條規定「對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。

十二、本公司將個人資料作國際傳輸者，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，且對資料接收方為下列事項之監督：

（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。

十三、本公司於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：

(一)提供聯絡窗口及聯絡方式。

(二)確認為個人資料當事人之本人，或經其委託者。

(三)認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由，應檢附理由通知當事人。

(四)收取必要成本費用者，應告知當事人收費基準。

(五)遵守本法第十三條有關處理期限規定。

十四、本公司維護所保有個人資料之安全，使用存有個人資料之各類設備或儲存媒體，應採取下列資料安全管理措施：

（一）運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定各類設備或儲存媒體之使用規範。(二)電子資料檔案存放之電腦、可攜式設備或儲存媒體，配置安全防護系統或加密機制。

（二）針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。

（三）作業過程有備份個人資料之需要時，該備份資料比照原件，依本法規定予以保護之。

（四）存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，於報廢、汰換或轉作其他用途時，應採適當防範措施，以避免由該媒介物洩漏個人資料；委

託他人執行者，非公務機關對受託人之監督依第二十二條規定辦理。

十五、非公務機關使用資通訊系統蒐集、處理或利用個人資料，且其資料庫保有個人資料數量達五千筆以上者，應採取下列措施：

（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）個人資料檔案與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）非法或異常使用行為之監控及因應機制。

前項第五款及第六款所定措施，應定期演練及檢討改善。

十六、非公務機關對保有個人資料之環境及實體設備安全，應採取下列措施：

（一）依據作業內容之不同，實施適宜之進出管制方式。

（二）訂定媒介物之管制方式，並檢視其保管情形。

（三）針對不同媒介物存在之環境，建置適度之保護設備或技術。

前項所稱環境，指第十四條所定各類設備、儲存媒體或媒介物之存放區域。

十七、非公務機關為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。

前項管理措施，應包括下列事項：

（一）依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。

（二）檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。

（三）要求所屬人員妥善保管存有個人資料之媒介物，並約定保管及保密義務。

（四）所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

十八、本公司應訂定個人資料檔案安全維護稽核機制，每半年定期或不定期檢查計畫執行情形，檢查結果並應向負責人提出報告，並留存相關紀錄，其保存期限至少五年。

前項經主管機關檢查結果發現計畫不符法令或不符政府令之虞者，本公司應即改善。

十九、本公司應採行適當措施，留存個人資料使用紀錄、或其他相關之證據資料，其保存期限至少五年。

二十、本公司執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。

本公司依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

（一）刪除、停止處理或利用之方法、時間或地點。

（二）將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。

前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

廿一、本公司應隨時參酌業務與本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定本計畫及處理方法，必要時予以修正；修正時，應於十五日內將修正後之本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

廿二、本公司業務終止後，保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年：

（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。

廿三、本公司倘因業務需要委託他人蒐集、處理或利用個人資料之全部或一部份時，應依本法施行細則第八條規定為適當監督。

廿四、本計畫依規定呈報所在地之直轄市、縣（市）主管機關備查，並隨時參酌業務及計畫執行狀況予修正，如有增修訂亦同。

附件　個人資料事故通報及紀錄表

<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。