統一超商個人資料檔案安全維護計畫

第一章 管理責任

壹、目的

本計畫係為統一超商股份有限公司（以下稱「本公司」）為所蒐集、處理、利用及國際傳輸之個人資料，訂定適當保護之相關事項，以提升並維護本公司有關個人資料的管理為目的。

貳、適用範圍

本計畫所稱本公司個人資料保護管理制度保護管理對象之「個人資料」，係以本公司所蒐集、處理、利用及國際傳輸之所有個人資料，該個人資料包含自然人姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

本計畫之適用範圍包含本公司之董監事、定期、不定期職員，派遣職員，部分工時、全時職員均適用，並適用全公司之組織。

第二章 個人資料保護管理制度與政策

本公司為保護所持有之個人資料，依中華民國對個人資料保護相關法規(包含個人資料保護法、零售業個人資料檔案安全維護管理辦法等)及「臺灣個人資料保護與管理制度」規範（Taiwan Personal Information Protection and Administration System, TPIPAS）(2021 版)，建置本公司之個人資料保護管理制度與個人資料保護管理政策。

壹、個人資料保護管理制度建置與運作

為有效運作個人資料保護管理制度，本公司制訂個人資料保護管理制度相關文件，並依以下工作排程協助各部門有效運作；每年第四季擬定下年度專案年度計畫，工作時程得視實際作業情況，調整預訂之執行時間。

貳、本公司個人資料保護管理政策

統一超商股份有限公司(簡稱本公司)除積極創造與提供超越顧客滿意之服務並善盡企業社會責任外，為確保顧客、員工及合作廠商個人資料之合理利用且避免人格權受侵害，將努力推動以下措施以落實個人資料之保護。

1. 法令遵循

本公司願恪遵中華民國保護個人資料安全之相關法規要求。

2. 個人資料管理制度

本公司依臺灣個人資料保護法令等規範，決定與個人資料管理制度有關且可能影響制度運行有效性之內部與外部議題，以及與利害關係人有關之要求事項，建立與公告全體事業人員周知本公司之個人資料管理制度，以明確訂定公司內個人資料保護管理相關之規範、作業準則，並跨部門成立個資專案管理小組、分配適當人員透過定期檢查、內評、檢視，以確保管理制度有效運作與持續改

善，落實個人資料之保護與管理。

3. 個人資料之蒐集、處理與利用

本公司將依中華民國保護個人資料相關法規之要求，在特定目的範圍內蒐集、處理與利用個人資料，並為不逾越當事人提供個人資料達成之利用目的必要範圍所為之處理、利用採取之適切措施。

4. 提供於第三人之限制

本公司不會非法或隨意提供或公開個人資料予第三人。

5. 維持個人資料之正確性與保障當事人權利之行使

為維持個人資料之正確性與保障當事人權利之行使，本公司針對個人資料與清冊建立定期盤點機制，並訂定個人資料當事人申請、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除個人資料之規則與流程，以確實、迅速回應當事人之相關申請。

6. 安全適當管理措施

本公司將依據各部門所持有個人資料之風險分析，採取適當對策與安全管理措施，以防止個人資料不當存取、外洩、滅失、毀損等問題。

運用電腦或自動化機器設備蒐集、處理或利用個人資料時，訂定使用可攜式設備或儲存媒體規範。

保有之個人資料內容如有加密需要，應於蒐集、處理或利用時，採取適當加密機制。

作業過程有備份個人資料之需要時，對備份資料予以適當保護。

使用網路磁碟機或雲端空間時，須注意個資資料保護，不得任意上傳，若有違反時將依公司獎懲規定辦理。

7. 緊急事故應變措施

本公司對個人資料的不當存取、遺失、破壞、竄改及外洩事故應變措施，於確認發生個資外洩事故時，將迅速採取適切相關措施作為，並將事實通知當事人及提供相關查詢與處理管道，以避免個資外洩事故對當事人造成重大不利益及影響。

8. 教育訓練

本公司對所屬員工實施必要教育訓練，使其瞭解本公司個人資料保護政策及相關管理措施。

9. 監督委託廠商

在委託廠商蒐集、處理或利用個人資料情形者，本公司將盡法定義務監督受委託廠商。

10. 政策之公告與維護

本公司將以適當之方式公告個人資料保護政策，並定期檢視政策進行必要之改善。

第三章 個人資料保護管理制度建置

本公司為保護所持有之個人資料，依中華民國關於個人資料保護相關法規(包含個人資料保護法、零售業個人資料檔案安全維護管理辦法)、「臺灣個人資料保護與管理制度」規範(TPIPAS 2021 版)及本公司個人資料保護政策，建置本公司之個人資料保護管理制度。

壹、法規盤點

本公司應就以下事項並依法情通報與法規鑑別作業程序調查個人資料保護法及其他相關

規範並遵守之。

一、調查與取得法令及其他規範一、進行鑑別與結果報告

二、法令及其他規範檢視修訂

貳、個人資料盤點程序

本公司為清查與識別所保有之個人資料檔案，及蒐集、處理或利用該等資料之現況，定期進行個人資料檔案與作業流程盤點，並將盤點結果彙整為「個資盤點清冊」。

一、個人資料盤點作業

二、個資盤點清冊建立

三、個資盤點清冊檢視修訂

參、風險管控程序

本公司所盤點出之個人資料，將公司內外部議題、利害關係人需求納入考量，規劃風險管理之原則及框架，辨識相關風險與因應管控措施，執行風險分析並採取必要的對策。

一、個人資料的風險分析程序

二、檢討對策方案

三、風險分析清冊檢視修訂

肆、事故之緊急應變

於本公司所持有之個人資料被竊取、洩漏、竄改、其他侵害，或其他違反個人資料保護相關法令或「臺灣個人資料保護與管理制度」規範(2021 版)之情事發生時，本公司依以下程序進行事故之查明程序及其對應：

一、個資緊急事故應變組織、功能執掌與運作原則

1. 公司同仁應於發生事故時，除迅速通報當事人權利維護組，並依本公司危機事件處理規範，對該個資緊急事故進行處理。

2. 發生事故時，由危機事件權責部門做為緊急事故應變單位，負責個資事故發生時之事故分析、跨單位聯繫、通知當事人知悉事故發生並提供後續查詢與處理管道，並於查明後告知當事人等事宜。

3. 當事人權利維護組或由其指派危機事件權責部門自發現事故時起算 72 小時內(若其他目的事業主管機關另有時限者，依其規定)，填具「個人資料侵害事故

通報及紀錄表」，以電子郵件方式向政府主管機關通報，並將視案情發展適時通報政府主管機關處理情形。

4. 由資安制度維運組負責將事故通報 TPIPAS 授證機關。

5. 教育訓練組得將事故處理狀況，納入個資管理人員教育訓練，以為日後內部檢討學習之教案。

6. 制度內評組得將事故原因納入日後稽核範圍，避免類似事件再次發生。

二、事故預防

1. 當事人權利維護組依法及本計畫防止公司保有之個人資料被竊取、竄改、毀損、滅失或洩漏，並加強管控公司所屬人員對內或對外之個人資料傳輸，避免外洩。

2. 資安制度維運組及制度內評組共同監督各部門，依各項標準作業程序控管各該部門內個人資料使用狀況。

3. 教育訓練組負責加強公司同仁教育宣導，以減少個資事故發生之頻率。

三、事故處理

1. 如公司同仁發現疑似與個資外洩有關的異常癥兆時，發現人員應立即通知當事人權利維護組，並由危機事件權責部門了解該異常發生之原因，並分析判斷是否為個資事故。

2. 如判斷非為個資事故，當事人權利維護組安排相關權責單位負責持續監控，直到該異常解除或排除；如判斷為個資事故，則應進行以下評估:

(1)影響範圍，有那些系統、應用程式或個人資料檔案受影響。

(2)事故發生來源與原因。

(3)損失情形。

(4)可採取應變措施。

(5)所需協助應變之支援。

四、避免類似事件再次發生

當事人權利維護組負責將個資事故處置復原過程中之事故發生原因分析及檢討改善方案、防止類似事件再次發生之具體方案以及事故稽查軌跡、分析相關證據加以記錄建檔，協助教育訓練組做成日後內部檢討學習之教案。

第四章 個人資料保護管理制度實施

本公司為保護所持有之個人資料，將依中華民國關於個人資料保護相關法規(包含個人資料保護法、零售業個人資料檔案安全維護管理辦法)、「臺灣個人資料保護與管理制度」規範(TPIPAS 2021 版)及本公司個人資料保護政策，建置本公司之個人資料保護管理制度，並依以下章節規定加以實施。

壹、實施程序之訂定

本公司為有效運作個資保護管理制度，將實施程序明確訂定於本計畫及相關通報中，並公告全體事業人員周知。

貳、個人資料之蒐集、處理、利用及國際傳輸之基本原則

本公司將以誠實信用方式，在未逾越特定目的之必要範圍及與蒐集之目的有正當合理關聯下，並符合以下各項要求進行個人資料之蒐集、處理、利用及國際傳輸:

一、個人資料之蒐集

所蒐集之個人資料非由當事人提供者，應於處理或利用前，向當事人告知其個人資料來源及前項應告知之事項，若當事人表示拒絕提供，應停止處理、利用其個人資料。

二、個人資料之處理

為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送等行為，應符合個人資料保護法規之要求及確立各部門得接觸資料之人員、個人資料處理專責人員之範圍與權限。

三、個人資料之利用

本公司保有之個人資料如需作特定目的外利用，應先行檢視是否符合個人資料保護法第 20 條第 1 項但書之規定。

四、個人資料之商業行銷

1. 本公司利用個人資料進行商業行銷行為，依個人資料保護法，提供當事人首次行銷得免費表示拒絕接受該行銷之方式。

2. 如當事人未於首次行銷時即提出拒絕表示，當事人嗣後仍得依本公司提供之管道及方式表示拒絕，本公司於接受當事人之拒絕表示後，將即停止利用其個人資料。

五、特種個人資料之蒐集、處理及利用限制

非有個資法第 6 條但書規定之情形，本公司不蒐集有關醫療、病歷、基因、性生活、健康檢查、犯罪前科等特種個人資料。

六、國際傳輸

傳輸個人資料時，應採取避免洩漏之必要保護措施。如將當事人個人資料為國際傳輸前，應檢視是否受中央主管機關限制，並告知當事人擬傳輸之國家或區域。

參、當事人之相關權利

個人資料當事人得依個人資料保護法向本公司行使請求查詢或閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用以及請求刪除個人資料等權利，亦可向本公司提出前揭事項之相關申訴與諮詢；本公司將以誠實迅速之態度，並依「個人資料當事人相關權利行使暨申訴處理程序」及「個人資料文件與紀錄管理規範」對應當事人之請求與作成紀錄。

肆、管理監督

本公司對所持有之個人資料，將就以下事項進行管理監督。

一、維持個人資料之正確性
二、安全管理措施與事業人員管理
三、委託處理個人資料之監督
伍、教育訓練
一、原則
本公司為確保個人資料保護管理制度有效運作，使人員對個人資料管理具有正確的認知及能力，將針對事業人員提供必要之個人資料管理教育訓練。
二、個資保護與管理教育訓練
1. 全體事業人員於任職期間內，至少接受一次有關個人資料保護法 規或管理制度之基礎訓練。
2. 個資管理專案小組成員除前項訓練外，得另參與資訊安全、隱私保護、安全維護措施有關之進階課程，並於課後向所屬部門單位進行宣導。
三、成果維持與改善措施
1. 教育訓練課程後以測驗方式進行適當之檢測，如未達檢測標準將補行訓練。
2. 教育訓練組應彙整教育訓練考核成果，向個資管理代表報告教育訓練成果之有效性。
3. 如有違反個人資料保護相關規定，將通知業務所屬主管，並列入個人考績評分與記錄事項。如違反情節重大者，將依公司內部獎懲辦法進行懲戒。

陸、業務終止個人資料處理
本公司於業務終止後，除主管機關或法律另有規定要求保留的資料外，其餘所保有之個人資料，於該業務單位個資盤點表所載保存期限內銷毀或刪除。紙本個人資料以碎紙、委外焚化或水銷等方式銷毀紙本；個人資料儲存於伺服器、磁碟陣列、磁帶、移動式儲存媒體等媒介物者，原則以格式化方式進行資料刪除，如設備不再使用該媒介物於報廢時應採取消磁、剪斷、敲擊等破壞措施，以免由該媒介物洩漏個人資料。

第五章 個人資料保護管理制度控管與改善

壹、管理責任
本公司為使個人資料保護管理制度有效控管，將設置適當人員，其權責執掌如下：
一、最高管理階層
最高管理階層為公司經營管理高層主管，責任應包括：
1.決定個人資料管理制度目標，確保符合公司需求與發展策略。
2.決定個人資料保護管理政策。
3.決定資源管理。
4.決定個人資料保護管理組織架構及權責劃分。

5.定期檢視管理制度，確保管理制度達成預期效果。
6.建立有效的溝通機制，適時指導與支援公司人員。
7.傳達落實個人資料管理制度之重要性。
二、個資管理代表
最高管理階層應指派管理階層成員之一，擔任個人資料保護制度管理代表，其應有之責任與職權包括：
1.負責維持個人資料管理制度運作之有效性，並建立必要內部人員結構。
2.確保職務執行過程之公正性與客觀性。
3.確保個人資料管理制度所需的各項過程被建立、實施與維持。
4.向最高管理階層報告個人資料管理制度之實施成效與改善措施。
三、個資管理人員
指為協助並持續本公司維運個人資料保護管理制度，由本公司受個資管理制度訓練取得之個資管理師、個人資料內評師或個人資料驗證師，或各部門受指派經過個資保護相關教育訓練負責執行各該部門個資管理專案工作，實際推動並確保個人資料管理制度之有效運作之人員。
四、個資內評人員
由取得公司內部個資管理人員資格之事業人員或個人資料內評師，擔任內評人員，內部控管事業導入個人資料管理制度之成效。
貳、有效性量測
為確保個人資料管理制度之持續與有效運作，本公司將依以下程序定期進行分析量測並作成紀錄:
一、制定量測項目
二、量測之實施
三、量測結果之效益評估
四、量測資料之保存
參、文件控管
本公司將依「個人資料文件與紀錄管理規範」，就下列構成個資保護管理制度重要文件進行製作與保管：
1. 個人資料保護管理政策。
2. 個人資料檔案安全維護計畫(個人資料保護管理手冊)以及其相關內部管理規則及其流程。
3. 其他實施個人資料保護管理制度應製作之紀錄文件。
肆、內部控管
本公司為驗證與確認個資管理制度運作符合法規要求，以及符合個人資料保護管理政策及本計畫之要求，將建立內控管理制度，每年定期依以下方式進行內部評核工作:
一、內部評核準備工作
二、內部評核作業之實施

三、個資管理代表、稽核人員或各該權責單位主管，應針對各項改善狀況持續追蹤，藉以防止再度發生。

伍、改善

一、定期檢視

為落實個人資料保護管理，個資管理代表應每年定期召開會議，召集相關權責人員，檢視個人資料保護管理制度，並紀錄檢視結果向最高管理階層報告之。

二、持續改善

最高管理階層決策調整個人資料管理制度時，應考量以下事項，並據以調整與修訂個人資料管理制度：

(1) 檢視報告。
(2) 社會情勢、國民認知、技術發展等各種環境之變遷。
(3) 事業業務領域之變化。
(4) 事業內外部之改善建議。
(5) 其他可能影響個人資料管理制度的任何變更。

三、矯正及預防措施

本公司將針對內部控管結果不符合事項及潛在不符合之風險，依所訂程序規劃改善措施及預防措施，並於執行改善與預防措施時，完成以下事項：

1.矯正措施

(1) 確認不符合事項之內容及判定發生原因。
(2) 評估需求並提出矯正方案，以確保不符合事項不再發生。
(3) 訂定合理之執行期限。
(4) 紀錄執行結果。
(5) 檢視所採取的矯正方案成果。

2.預防措施

(1) 依據公司因持有個人資料可能面臨的風險，確認各項潛在不符合事項之內容及其原因。
(2) 評估該潛在不符合事項造成之風險是否可容許，如為不可容許則應提出改善預防方案。
(3) 訂定合理之執行期限。
(4) 紀錄執行結果。
(5) 檢視所採取的預防方案成果。
(6) 持續改善個人資料管理制度。