滿心企業股份有限公司

零售業個人資料檔案安全維護計畫

壹、零售業之組織及規模

一、名稱：滿心企業股份有限公司

二、地址：新北市五股區五權六路 18 號

三、負責人：李俊良

四、資本額：新臺幣 646,268,780 元

五、經營事業：百貨專櫃/加盟店/電商

貳、個人資料檔案安全維護管理措施

一、依據：

個人資料保護法第 27 條第 3 項及零售業個人資料檔案安全維護管理辦法第 4 條規定。

二、個人資料檔案安全維護計畫之訂定及修正

(一)訂定目的：為防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰訂定「個人資料檔案安全維護計畫」(下稱本計畫)，本零售業員工應依本計畫辦理個人資料檔案安全管理及維護事宜。

(二)本計畫將參酌業務規模及特性，衡酌經營資源之合理分配等因素，檢視其合宜性，並經負責人或其授權人員於核定後予以修正。

三、專責人員及資源配置

(一)專責人員：

1.姓名：蔡尚權

2.職責：電腦設備維護

(1)規劃、訂定、修正、執行安全維護計畫及其他相關事項。

(2)定期(每年至少 1 次)就執行前開任務情形向負責人或經其授權人員提出書面報告。

(二)稽核人員/單位：

1.姓名/單位：楊又霖/稽核室

2.職責：資料安全稽核機制

(1)不得與專責人員為同一人。

(2)定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向代表人或經其授權之人員提出報告。

(三)預算：每年新臺幣 2,150,000 元。

四、個人資料蒐集、處理及利用之內部管理程序

(一)向當事人蒐集個人資料時，明確告知當事人以下事項：

1.本公司名稱。

2.蒐集目的。

3.個人資料之類別。

註：可參考法務部「個人資料保護法之特定目的及個人資料之類別」(https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=fl010631)

(二)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，應立即停止處理、利用其個人資料。

(三)另本公司保有之個人資料利用期限屆滿時，除因法令規定、執行業務所必須或經當事人書面同意者外，將主動刪除或銷毀其個人資料，並留存相關紀錄。

(四)指定管理人員每季清查本公司所保有之個人資料是否符合特定目的，若有非屬特定目的必要範圍之資料或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置，並留存相關紀錄。

(五)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二十條第一項但書之規定。

(六)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。

五、個人資料之範圍及項目

(一)個人資料範圍：指本公司蒐集、處理及利用之自然人姓名、出生年月日、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：可參考個人資料保護法第二條第一款填寫

(二)特定目的：消費者、客戶管理與服務〇九〇等運用。

註：本項請依「個人資料保護法之特定目的及個人資料之類別」，說明特定目的項目，例如：人事管理(〇〇二)、全民健康保險、勞工保險、國民年金保險或其他社會保險(〇三一)、消費者、客戶管理與服務(〇九〇)等。

(三)指定管理人員每季定期清查本公司所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件。

六、資料安全管理

(一)資通訊系統存取個人資料之管控：

1. 依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之必要性及適當性。

2. 檢視各相關業務之性質，規範個人資料蒐集、處理、利用及其他相關流程之負責人員。

3. 蒐集、處理或利用個人資料之電腦、相關設備或系統設備，應採取適當之安全機制，定期檢測並因應系統漏洞所造成之威脅。

4. 個人資料檔案使用完畢應即關閉檔案，不得任其停留於螢幕上。

5. 對內或對外從事個人資料傳輸時，加強管控避免外洩。

6. 重要個人資料檔案應另加設密碼，非經陳報董事長核可不得存取。

7. 每日進行防毒、掃毒等必要之安全措施。

8. 所屬人員非經本公司董事長核可，不得任意複製本公司保有之個人資料檔案。

9. 本公司蒐集、處理或利用個人資料時，應設置使用者身分確認及保護機制、個人資料顯示之隱碼機制（如將身分證字號末 4 碼以****標示，或將姓名其中 1 個字以〇標示）、網際網路傳輸之安全加密機制、個人資料檔案與資料庫之存取控制及保護監控措施，防止外部網路入侵對策及非法或異常使用行為之監控及因應機制。

10. 就防止外部網路入侵對策及非法或異常使用行為之監控及因應機制，應定期（每年至少 1 次）進行演練及提出檢討改善報告。

11. 個人資料有加密之必要者，應於蒐集、處理或利用時，採取適當之加密措施。

12. 個人資料有備份之必要者，應對備份資料採取適當之保護措施。

13. 資通訊系統存有個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。

14. 評估使用情境，採行個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。

15. 資通訊系統與網路相連存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。

16. 對存有個人資料之資通訊系統，設定異常存取資料行為之監控及定期演練因應機制。

(二)紙本資料之保管：

1. 記載有個人資料之紙本文件，在未使用時存放於電腦機房內。所屬人員非經董事長核可，不得任意複製、拍攝或影印。

2. 丟棄記載有個人資料之紙本文件時，應先以碎紙設備進行處理。

七、人員管理

(一)所屬人員登錄電腦之識別密碼，每 3 個月變更 1 次。

(二)所屬人員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。

(三)本公司與所屬人員間之勞務、承攬及委任契約均列入保密及個資條款及違約罰則，以促使其遵守個人資料保密等相關義務（含契約終止後）。

(四)所屬人員離職時，應即取消其登錄電腦之使用者代碼（帳號）及識別密碼。其在職期間所持有之個人資料應確實移交，不得私自複製、留存並在外繼續利用。

八、認知宣導及教育訓練

(一)每年對所屬人員施以個人資料保護法基礎認知宣導及教育訓練，使其明瞭個人資料保護相關法令之規定、責任範圍與各種個人資料保護事項之機制、程序及管理措施。前述教育宣導及訓練應留存相關紀錄或佐證資料（例如：簽到表或登錄紀錄等佐證資料）。

(二)對於新進人員給予特別指導，確保其明瞭個人資料保護相關法令規定及責任範圍。

九、事故之預防、通報及應變機制

(一)預防措施

1. 指定專人辦理安全維護事項，防止本公司保有之個人資料被竊取、竄改、毀損、滅失或洩漏。

2.加強管控本公司所屬人員對內或對外之個人資料傳輸，避免外洩。

3.加強所屬人員教育宣導，並嚴加管制。

(二)應變措施

1.發現本公司有個人資料遭竊取、洩漏、竄改或其他侵害事故者之情形，應立即通報代表人或經其授權之人員並查明發生原因及損害狀況，及依實際狀況採取相關應變措施，以控制事故對當事人之損害。

2.儘速以適當方式通知當事人或其法定代理人個人資料被侵害之事實、本公司已採取之因應措施及聯絡電話窗口等資訊。

3.針對事故發生原因檢討缺失，並研議預防及改進措施，避免類似事故再次發生。

(三)通報措施

本公司應自發現事故時起算 72 小時內，填具「個人資料侵害事故通報與紀錄表」，以電子郵件方式向經濟部通報，並將視案情發展適時通報處理情形，以及將整體查處過程、結果及檢討等函報經濟部。

十、設備安全管理

(一)指派專人管理儲存個人資料之電腦及其他儲存媒介物，定期清點、保養維護。

(二)電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

(三)建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

(四)指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經董事長同意並作成紀錄不得攜帶外出或拷貝複製。

(五)本公司保有之個人資料檔案應每日(NAS)備份。

(六)重要個人資料備份應異地存放，並應建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。

(七)電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。

(八)更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。

(九)依據作業內容及環境之不同，實施必要之安全環境管制，以妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備。

(十)資通系統避免使用真實個人資料進行測試，若有使用真實個人資料進行時，應訂定使用規範並確實遵守。

(十一)本公司處理個人資料之資通系統有變更時，將確保其安全性未降低。

(十二)本公司將每月檢視處理個人資料的資通系統，評估其使用狀況及存取個人資料的情形；前述檢視作業時併確認蒐集、處理或利用個人資料的電腦、相關設備或系統是否具備必要的安全性，並採取適當的安全機制。

十一、資料安全稽核機制

(一)不定期（每年至少 1 次）稽核個人資料安全維護計畫之執行情形及成效，檢查本公司是否落實本計畫規範事項，針對檢查結果不符合及潛在風險事項規劃改善措施，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.提出改善及預防方案。

3.記錄檢查情形及改善與預防措施方案執行結果。

(二)前項檢查情形及執行結果應載入稽核報告中，由代表人或經其授權之人員簽名確認，稽核報告至少保存5 年。

十二、使用紀錄、軌跡資料及證據保存

(一)本公司建置個人資料之電腦，其個人資料使用紀錄，需每日(NAS)備份並設定密碼，儲存該紀錄之儲存媒介物保存於適當處所以供備查。

(二)個人資料使用紀錄以紙本登記者，應存放於電腦機房內，非經董事長核可，不得任意取出。

(三)本公司應保存以下紀錄：

1.個人資料提供或移轉第三人。

2.當事人行使個資法第三條之權利及處理過程。

3.個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀。

4.人員權限新增、變動及刪除。

5.消費者個人資料之蒐集、處理及利用紀錄，以及自動化機器設備之軌跡資料。

(四)以上使用紀錄、軌跡資料及相關證據至少留存5 年。

十三、業務終止後之個人資料處理方法

本公司於業務終止後，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：

(一)銷毀：方法、時間、地點及證明銷毀之方式。

(二)移轉：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)刪除、停止處理或利用：方法、時間或地點。以上處理措施應製作紀錄，其保存期限至少 5 年。

十四、個人資料安全維護之整體持續改善方案

(一)本公司每年應參酌安全維護計畫執行狀況、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性，並予必要之修正。

(二)針對個資安全稽核結果有不符合法令之虞者，規劃改善與預防措施並納入安全維護計畫。

十五、當事人權利行使

當事人或其法定代理人行使個人資料保護法第三條規定之權利時，採取下列方式辦理：

(一)提供聯絡窗口及聯絡方式。

(二)確認為個人資料當事人本人、法定代理人或經其委託之人。

(三)有個人資料保護法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人或其法定代理人行使權利之事由者，併附理由通知當事人或其法定代理人。

(四)遵守個人資料保護法第十三條處理期限之規定。

(五)告知依個人資料保護法第十四條規定得酌收必要成本費用。

十六、委託作業

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，應依個人資料保護法施行細則第八條規定對受託人為適當之監督，並於委託契約或相關文件中，明確約定其內容，以及採取下列方式辦理：

(一)選擇受託人前，應確認需要委外的範圍，並以適當評估方式選擇具適當個資安全維護能力的受託人。

(二)應與受託人締結委託契約，要求受託人依本公司應適用之個資管理規定執行契約。

(三)於委託契約或相關文件明確約定適當之監督事項及方式。

(四)要求受託者僅得於本公司指示之範圍內，蒐集、處理或利用個人資料。

(五)要求受託者認本公司之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知本公司，並於契約中訂定委外廠商於知悉資通或個資安全事件情況時，應即向本公司權責人員或通報窗口，以指定之方式進行通報。

(六)對受託者應定期查核受託者執行之狀況，並將確認結果記錄之。(如委外查核報告以及查核缺失追蹤情形)

(七)委託關係終止或解除時，受託者應將個人資料載體之返還或將個人資料刪除。

十七、行銷

(一)本公司依個人資料保護法第二十條第一項規定利用個人資料為行銷時，應明確告知當事人本公司名稱及個人資料來源。

(二)本公司首次利用個人資料為行銷時，應提供當事人或其法定代理人表示拒絕接受行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受行銷者，應立即停止利用，並周知所屬人員。

十八、表單

個人資料侵害事故通報與紀錄表，如附件。

附件

<table>
<tr><td colspan="4">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td rowspan="5">事業名稱
_____
通報機關
_____</td><td colspan="3">通報時間：　　年　　月　　日　　時　　分</td></tr>
<tr><td colspan="3">通報人：　　（簽名/蓋章）</td></tr>
<tr><td colspan="3">職稱：</td></tr>
<tr><td colspan="3">電話：</td></tr>
<tr><td colspan="3">E-mail：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="3"></td></tr>
<tr><td rowspan="5">事件發生種類</td><td>□竊取
□洩漏
□竄改</td><td colspan="2">個資侵害之總筆數(大約)
_____</td></tr>
<tr><td>□毀損
□滅失
□其他侵害事故</td><td colspan="2">□一般個資_____筆
□特種個資_____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="3"></td></tr>
<tr><td>損害狀況</td><td colspan="3"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="3"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="3"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="3"></td></tr>
<tr><td>是否於發現個資外洩時起算七十二小時內通報</td><td colspan="3">□是 □否，理由：</td></tr>
</table>