

麗豐股份有限公司
個人資料保護之管理辦法

一、通則

1. 本辦法適用於本公司及其子公司。
2. 個人資料之蒐集、處理及利用，應符合相關法令規定，包括提供資料當事人下列權利：
 - 2.1 查詢或請求閱覽。
 - 2.2 請求製給複製本。
 - 2.3 請求補充或更正。
 - 2.4 請求停止蒐集、處理及利用。
 - 2.5 請求刪除。
3. 個人資料之蒐集、處理及利用，應依誠實及信用方法為之，不得逾越特定目的之必要範圍。

二、書面文件之保護

1. 蒐集載有個人資料之書面文件時，應有適當防護措施，包括在書面文件上註明使用目的或範圍等。
2. 處理或利用載有個人資料之書面文件時，應妥善保管之，不得任意置放。
3. 因業務需要提供載有個人資料之書面文件予外部單位時，待委外事務完成後，應予以收回。
4. 載有個人資料之書面文件，如屬可銷毀文件，應定期執行文件銷毀作業。

三、電子儲存檔案之保護

1. 個人資料以電子方式儲存時，儲存之電子設備應設置使用者代碼及登入密碼，且於應用程式關閉後，有自動登出之功能。
2. 使用者代碼及登入密碼禁止與他人共用，且登入密碼應至少每三個月更換一次，長度應至少 8 碼，包含文字及數字。
3. 因業務需要提供載有個人資料之電子儲存檔案予外部單位時，應選擇可靠且具備保密機制之傳遞方式，例如對資料檔案壓縮加密，並對傳輸行為加以記錄。
4. 以電子設備處理或利用個人資料時，應核對個人資料之輸入、輸出、編輯或更正是否與原件相符。對資料是否相符有疑義時，應調閱原件查核。
5. 儲存個人資料之電子設備，應有防火牆與外部網路隔絕，並安裝防毒軟體，除定期更新病毒碼外，並應定期執行排程掃瞄。
6. 儲存個人資料之電子設備，應指定專人定期檢視及更新作業系統，並修補程式漏洞。
7. 儲存個人資料之電子設備，應置放於安全區域，例如有門禁控管之辦公室、上鎖之抽屜等，非經權責單位同意，不得任意攜出。
8. 儲存個人資料之電子設備，必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。
9. 儲存個人資料之電子設備，如需報廢或移轉他用時，應確實刪除該電子設備所儲存之個人資料。
10. 外部單位更新或維修儲存個人資料之電子設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

四、人員管理

1. 公司應對蒐集、處理或利用個人資料之人員施予資訊安全教育訓練（內、外訓皆可），並定期宣導個人資料保護之重要性及每日下班電腦應關機之政策。
2. 蒐集、處理或利用個人資料之人員，如有職務異動，應將所保管之書面文件列冊移交，對電子設備而言，接辦人員除應於相關系統重置登入密碼外，應視需要更換使用者代碼。
3. 蒜集、處理或利用個人資料之人員，應簽訂保密切結書，於離職時或合約終止時，確實取消或停用其使用者代碼及登入密碼，並收繳其通行證及相關證件。
4. 禁止使用即時通訊軟體、點對點傳輸軟體、雲端硬碟或其他不安全之網際網路媒體蒐集、處理或利用個人資料。
5. 禁止在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務上所知悉之個人資料。

五、系統開發及委外管理

1. 自行開發或委外處理個人資料之資訊系統，應在系統開發週期之初始階段，將個人資料的安全需求納入考量（如邏輯測試等）；系統之維護、更新、上線、及版本異動等作業，應予安全管制，避免危害個人資料安全。
2. 應避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，應經權責單位核准後，透過加密通道進行（如 VPN 等）。
3. 自行開發或委外處理個人資料之資訊系統，應將個人資料(包括測試用個人資料等)施予妥善之保護與控管。
4. 個人資料若委外列印，應於委外合約中載明個人資料之保密義務、資訊安全相關責任及違反之罰則，必要時應執行現場稽核。

六、控制重點：

(一) 書面文件之保護

1. 載有個人資料之書面文件，是否妥善保管，未有任意置放情事？
2. 提供外部單位之個人資料，於交付及收回時是否有適當記錄？
3. 載有個人資料之書面文件，如屬可銷毀之文件，是否定期執行文件銷毀作業？

(二) 電子儲存檔案之保護

1. 蒜集、處理蒐集、個人資料之電子設備，是否有設置使用者代碼及登入密碼？
2. 是否有與他人共用使用者代碼及登入密碼之情事？
3. 登入密碼是否至少每三個月更換一次？長度是否至少 8 碼，包含文字及數字？
4. 提供載有個人資料之電子儲存檔案予外部單位時，是否有先對資料檔案壓縮加密，再進行傳輸？

5. 儲存個人資料之電子設備，如需報廢或移轉他用時，是否確實刪除該電子設備所儲存之個人資料？

(三) 人員管理

1. 是否有執行資訊安全教育訓練？

2. 每日下班是否執行電腦關機？

3. 相關人員離職後，接辦人員是否於相關系統重置登入密碼，並視需要更換使用者代碼？

4. 是否有使用不安全之網際網路媒體蒐集、處理或利用個人資料？

(四) 系統開發及委外管理

1. 自行開發或委外處理個人資料之資訊系統，是否將個人資料(包括測試用個人資料等)施予妥善之保護與控管？

2. 個人資料若委外列印，是否於委外合約中載明個人資料之保密義務、資訊安全相關責任及違反之罰則？

七、依據資料或使用單據：

1. 個人資料保護法

八、實施與修訂：

本程序經呈董事會核准後實施，修正時亦同。

九、版別紀錄

版本	變更內容簡述	日期
1	新增	2014.12.19