欣欣大眾市場股份有限公司資訊安全管理辦法

壹、依據

行政院及所屬各機關資訊安全管理要點

貳、目的

為落實資訊安全管理，公司成立資訊安全組織(資訊室)，由公司董事長督導及推動全般資訊安全作業

參、執行方式：

一、資訊室職掌

(一)資訊安全政策之核定及督導。

(二)資訊安全責任之分配及協調。

(三)資訊資產保護事項之監督。

(四)資訊安全事件之檢討及監督。

(五)其他資訊安全事項之核定。

(六)每季召開資訊安全檢討會議。

(七)每季召開資訊安全災損演練。

(八)每半年辦理資訊安全教育訓練。

二、帳號管理

(一)資訊系統均需有帳號及密碼登入管理功能，依業務功能不同，區分帳號種類，每一種類每一同仁使用一組帳號及密碼。

(二)使用者須妥善保管個人帳號、密碼，密碼至少六個字元及應三個月更換乙次。個人密碼應絕對保密，若發現外洩應即更改，以確保資訊安全。

(三)同仁異動經權責主管核定後，應依其異動狀況停用或刪除其帳號及許可權

三、資料存取

(一)系統資料庫由資料庫管理者依使用者群組訂定不同使用權限，無權限者不得直接存取資料庫內容。

(二)系統應依資料之重要性設定安全機制，並應可追蹤資料流及使用者操作記錄。

(三)系統資料儲存異常時，應有自動警報或回復功能。

(四)資料依重要性區分，設定不同的保存或銷毀期限，除另有規定外，保存期限至少為五年以上。

(五)使用單位經由系統所取得之機密性資料均應嚴加管制，限制傳閱、影印、複製、攝影、轉出或以其他方式記錄。

(六)系統資料轉出應填寫「資訊服務單」，經權責主管核定後始得辦理。

(七)系統存取及應用之監督

1、應建立及製作異常事件及資訊安全事項的稽核軌跡，並妥善保存，以作為日後調查及監督之用。

2、系統稽核軌跡應包括下列事項：

(1)使用者識別碼。

(2)登入及登出系統之日期及時間。

(3)儘可能記錄端末機的識別資料或其位址。

四、網路安全管理

(一)網路應安裝監控系統，監控通訊線路、通訊協定、資料流量、資料內容及使用物件，由資訊部門指定專人辦理。

(二)重要伺服器均應裝置於公司受到保護的網路內，內、外網路須安裝安全防護設備(防火牆)區隔，並依業務所需設定安全存取權限。

(三)防火牆安全權限之異動申請，經資訊部門核定後，由專責人員修改，並紀錄異動歷程。

(四)資訊部門應定期檢討防火牆安全權限及電腦網路安全事項，並應建立網路入侵偵測系統，以有效偵測惡意入侵事件。

(五)經由公眾網路傳輸機密資料時，應採取資料加密機制。

(六)防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。

五、為確保公司資訊系統資料完整，須定時備份，備份資料須另存於異地機房的主機。

六、病毒防治

(一)公司所有伺服器主機、個人電腦、筆記型電腦均應安裝防毒軟體，所有伺服器亦應按月執行掃毒作業，並將紀錄留存備查，以防制及偵測電腦病毒與惡意軟體等的侵入。

(二)使用防毒軟體，應依下列原則辦理：

1、定期更新版本及病毒碼。

2、定期或即時掃描電腦系統及資料儲存媒體。

3、使用之防毒軟體由資訊部門審核後，方可使用。

4、對來路不明及內容不確定的資訊媒體，應在使用前詳加檢查是否感染電腦病毒。

5、定期將必要的資料及軟體予以備份。

(三)電腦設備如遭病毒感染，應立即離線(拔除網路線連結)，並通知資訊人員處理，直到確認病毒已消除後，方可重新連線。

七、個人資料保護

資訊系統之運作功能及資料存取應符合個人資料保護規範，依據「個人資料保護作業要點」相關規定辦理。

八、資安要求

(一)資訊部門應制定系統使用規範，並防止內、外非相關人員取得機密資訊或影響系統正常運作；同仁不得利用系統進行非正常或未經許可之作業，以獲取不當之資訊或利益。

(二)同仁應遵守公司資訊安全政策之相關規定，違者按情節輕重依「同仁獎懲辦法」相關規定予以處分。

(三)同仁應遵守業務機密之相關法令規定

，在職及離退職後均不得洩漏所知悉之資訊機密，或為不當之使用，違者按情節輕重依「同仁獎懲辦法」相關規定予以處分，必要時並得追究相關法律責任。

九、有關資訊安全之事項，除另有規定外，悉依本辦法辦理。