愛山林建設開發股份有限公司
資訊作業管理辦法

制訂日:108.08.01

壹、主旨：為強化本公司資訊安全管理，確保資料、系統、設備及網路安全，特訂定本辦法。

貳、組織及權責：

一、由資訊部門主管擔任召集人，成員包括資訊部門，負責各資訊相關安全需求之研議、管理及保護事項。

二、資訊部門職掌為執行下列作業程序之資訊安全政策，並每年至少針對釐訂之資訊安全政策評估 1 次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

參、作業程序

一、資訊系統管理

1. 對於程式及檔案存取使用，應按權限區分。
2. 如遇有因系統問題或操作不當，導致資料錯誤需直接異動資料庫須填具《MIS服務申請單》，註明異動原因經單位主管及資訊單位主管核可後方可異動。
3. 人員職務異動時應依其資訊權限表即時更新，若特殊權限則由各單位提出申請填寫《MIS服務申請單》呈經權責主管核准交資訊單位執行。
4. 電腦程式之增新與修改須由各單位提出申請，填寫《MIS服務申請單》呈經權責主管核准交資訊單位執行。
5. 資訊單位於完成驗收後(含新購、版本更新等)，應將供應廠商所提供或系統自行開發/修改而編製之技術文件及操作手冊等，按序歸檔存查。
6. 密碼應以亂碼方式儲存。

二、使用者帳號及密碼管理

1. 使用者應適時更換密碼，以降低資安風險。
2. 授權使用密碼者應造冊列管，密碼應定期更換，個人之密碼不得借他人使用。
3. 委外人員之電腦通行使用權利應適當控管，委外期間結束後應立即收回該項權利。

三、機房管理

1. 重要電腦主機及網通設備應放置於機房，以便防護。
2. 除資訊單位人員外，未經授權者不得進入電腦機房。進出機房須於《機房進出管制表》上登錄。
3. 電腦機房應設有備援供電系統、滅火設備，並設置於遠離高溫及潮濕之環境，附近不應放置易燃或爆裂等危險物品。
4. 對機房各項委外軟硬體維護，廠商需填寫《維護紀錄單》。
5. 禁止擅自利用資訊中心系統設備，處理與本身業務無關之作業。
6. 對機房各項軟硬體做設定修改，均需記錄於《機房維護記錄表》

四、網路系統安全管理

1. 應定期評估自身網路系統安全。
2. 定期或適時修補網路運作環境之安全漏洞及宣導有關電腦網路安全事項。
3. 各電腦主機重要軟硬體設備應有專人負責。
4. 資料經由電子郵件傳送或接收時，應於電腦系統設置防火牆及防毒軟體以防駭客或電腦病毒之侵害。

五、資料備份管理

1.資訊單位應將重要系統檔案、程式及資料檔案定期進行備份。

2.備份檔案應適當命名，以利辨識備份內容。

3.備份檔案不得借調。

4.資料庫備份檔案應異地備份。

六、電腦病毒及惡意軟體之防範

1.應安裝防毒軟體，並適時更新程式及病毒碼。

2.應定時對電腦系統及資料儲存進行病毒掃描。

3.防毒應涵蓋個人端及網路伺服器端電腦。

4.外來資料隨身碟需先經使用者防毒偵測。

5.防火牆應由專人執行控管設定。

七、應評估與指定適當之內部人員或委外，不定期抽查公司資通安全相關規定之遵循情形。

八、使用單位如因業務需要，需調閱相關資料時，應填寫《MIS服務申請單》，經權責主管核准後始得調閱。

九、若發現未經適當核准而外流公司資料檔案者，公司得依情節重大及對公司之損害程度，懲處相關員工或進行索賠。

十、 若發生資訊安全事件，應先向資訊人員通報。資訊人員先採取適當反應措施後記錄於《MIS服務申請單》。若有情節重大者，則聯繫檢警調單位協助偵查。

肆、本辦法經總經理核准公告後施行，修正時亦同。