旺玖科技股份有限公司

文件名稱：		總頁數包含此頁：
MIS 資訊安全管理辦法		5

文件號碼：	版本：	建立日期：	發行日期：
MIS-013	1.0	2021/06/24	2021/06/24

內容表

核准：	覆核：	建立：
		施淑瑜

部門經辦人(建立)→部門主管和相關部門主管(覆核)→總經理(核准)

文件履歷表

文件名稱：MIS 資訊安全管理辦法

文件號碼：MIS-013

ID	版本	更改原因/內容	經辦	發行日期	總頁數
1	1.0	新建立	施淑瑜	2021/06/24	5
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

1 目的

1.1 制訂 MIS 資訊安全管理辦法，以便符合內控之要求。

2 適用範圍

2.1 全公司資訊安全管理作業。

3 權責

3.1 MIS 應依職責檢視需求內容是否合理，以便確保符合公司政策。

4 管理原則

4.1 資訊安全政策

4.1.1 面對瞬息萬變的資安威脅，MIS 應隨時掌握，擬定應變機制，公告資訊安全相關訊息。

4.2 組織人員安全

4.2.1 依一般使用者、系統管理者、系統擁有者等不同職務分別訂定其安全責任。

4.2.2 訂定各項資訊設備的安全作業程序，並規範員工的資訊安全作業程序與權責，且與資訊服務廠商、電力系統廠商及電信單位建立聯絡管道。

4.2.3 可存取機密性、敏感性資訊或系統之員工應適當分工，分散權責，並建立備援機制。

4.2.4 MIS 應進行適當的資訊安全教育訓練及宣導，員工應了解資訊安全事件發生之通報及處理程序。

4.2.5 人員異動、離職或退休，應立即停用其系統帳號及存取權限。

4.3 資產分類與控管

4.3.1 資產應列帳及設定保管人，並定期盤點。

4.3.2 關鍵資訊系統使用之儲存媒體應依使用年限定期汰換。

4.3.3 資訊設備故障時，應由 MIS 進行檢測，確認不堪使用進行報廢程序時應填寫【列管資產報廢單】。

4.3.4 資訊設備報廢之清運應配合固定資產管理單位年度計劃統一處理。

4.4 實體與環境安全

4.4.1 重要資訊設備應放置電腦機房，並控管人員進出，非權責人員需要進出時，由 MIS 全程陪同，並在【MIS 機房訪客登記表】詳實記錄進出事由、日期及時間。

4.4.2 權責人員進出電腦機房，應遵循【電腦機房使用規範】。

4.4.3 電腦機房應設置空調設備及消防設施。

4.4.4 電腦機房內嚴禁存放易燃物及未經核准之電器或其他物品。

4.4.5 電腦機房應使用環境監控系統，掌握機房溫度及溼度狀況。

4.4.6 定期檢視電腦機房進出入記錄，審查進出權限之合理性。

4.4.7 電腦機房應設置不斷電系統，以確保市電異常時有足夠的電力讓機房設備以正常程序關機，以避免不正常斷電造成系統損毀及資料遺失。

4.4.8 資訊設備外送必須填寫【物品外送保管單】，並經廠商用印完成。

4.4.9 具機密性、敏感性之手寫或影印公文廢紙及已過保存期限之公文需予以銷毀。

4.4.10 設備報廢後如確定不再使用時，需將儲存之資料及軟體移除後，將報廢硬碟委外進行消磁與物理破壞。

4.4.11 重要資訊系統應定期備份並且異地存放儲存裝置。

4.5 通訊與作業管理

4.5.1 建置網路防火牆(Firewall)，透過防火牆機制，控管公司內網與網際網路的存取安全。

4.5.2 定期檢測網路運作環境之安全漏洞。

4.5.3 針對關鍵資訊系統建立安全漏洞與更新管理機制，包含定期稽核與更新測試。

4.5.4 電子郵件系統應建置防毒、垃圾郵件過濾系統，以便防範電子郵件夾帶的病毒、木馬、蠕蟲及網路釣魚郵件。

4.5.5 電腦設備以中央控管方式導入防毒軟體，並即時更新病毒碼。

4.6 存取控制

4.6.1 需求單位依職能別申請所需的存取權限經權責主管核准後，由 MIS 人員依其業務職責及職能分工原則設定使用者權限，以避免未授權之存取。

4.6.2 定期檢視職能別與使用權限之合理性。

4.6.3 使用者之帳號密碼應定期變更。

4.6.4 資訊系統帳號密碼的設定需滿足密碼複雜度原則，帳號登入失敗達一定次數時，系統自動鎖定帳號。

4.6.5 根據服務性質劃分獨立的邏輯網域(內部網路、非軍事區及外部網路)，每一網域設定不同的防護機制並有通訊閘道管制過濾網域間資料的存取。

4.6.6 定期檢視關鍵資訊系統的系統日誌。

4.6.7 新導入的資訊設備，在安裝完成後應立即變更系統預設帳密。

4.7 系統開發及維護

4.7.1 應用系統在規劃分析時需將資訊安全納入考量，並控管系統之維護、更新、上線及版更以避免不當使用危害系統安全。

4.7.2 委外廠商基於實際作業需要，MIS 得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

4.7.3 委外廠商建置及維護重要軟硬體設施時，應在當責單位人員協同 MIS 人員之監督及陪同下處理。

4.7.4 系統變更後，MIS 應主動公告異動範圍、時間、影響層面。

4.7.5 版本更新後，對於舊版軟體及系統文件應妥善管理並詳實紀錄版更異動歷程。

4.8 符合性

4.8.1 軟體取得(含自行開發、委外開發、購置或租用)依智慧財產權規定或合約要求確實辦理。

4.8.2 相關人員(使用者、系統管理者、資產持有者、資訊持有者及管理階層等)應落實執行組織所訂之所有安全程序。

4.9 內稽內控

4.9.1 定期以【資通安全檢查表】檢視資訊安全執行力及符合性。

4.9.2 每一次的查核紀錄應妥善保存。

4.9.3 由專業且獨立於資安工作單位的資安稽核人員進行查核。

4.10 預防措施

4.10.1 依照【IT-2-42-001D 電腦備份管制程序】執行備份作業，以防資安風險可能造成的損失。

5 本辦法經呈 總經理核准後公布實施，修正時亦同。

6 本辦法其它相關未盡事項，依權責部門訂定之相關規定辦理。