MARTAS 振躍精密滑軌股份有限公司

文件編號	C1MQ0009	版　本	C	制定日期	3-MAY-2017
作業項目	資訊循環內部控制制度			修訂日期	14-Sep-2018

CC-110-1	作業程序及控制重點	依據資料及使用表單
資通安全檢查控制	一、作業程序： 1.訂定或適時修定適當之資訊安全政策，並定期向員工宣達資訊安全政策及規定。 2.建立防火牆(Firewall)作為安全控管以預防外部網路對內部資訊管理系統侵入。 3.防火牆系統軟體、防火牆之日誌檔，應定期檢查，留存相關紀錄供主管覆核，必要時經適當核准後補強防火牆軟體。 4.防火牆之日誌檔應定期檢核，系統異常記錄並由主管不定期查核。 5.各項網路服務之使用依據資訊管制程序執行。 6.定期查核各項網路服務之 System log，並追蹤異常情形並檢討防範之。 7.每日自動定時掃描電腦並自動偵測病毒。並於每週一透過防毒軟體監控，查看各人 PC 中毒及更新狀況，將其記錄登記在「防禦病毒記錄表」，表格記錄應「加密」處理。 8.每三小時定期更新防毒軟體之病毒碼版本，如有最新版本應立即更新。 9.員工應避免透過公司網站收發或下載與業務無關之郵件或軟體，以避免佔用公司之網路資源及增加電腦病毒感染機會。 10.公司員工非因營業所需，禁止將公司相關資訊經由電子郵件對外傳送。 11.使用者所使用之軟體均須為經授權之軟體，不得自行輸入、下載或使用非法軟體。 12.公司員工應確實遵守保密相關規定，防止本公司內部機密文件外洩，以落實公司內部資訊安全管制。 13. 訂定適當之資訊安全政策。並定期向員工宣達資訊安全政策及規定。宣導資訊安全觀念以強化員工 資訊安全意識。 14. 網路使用人員之管理 14.1 使用人員利用網路使用任何電腦資源，均需遵守被授權的權限。 14.2 使用人員不得將自己的登入身份識別與登入網路的密碼交付他人使用。 14.3 使用人員不得以任何方法竊取他人登入網路的身份識別與網路密碼。 15.電子郵件之使用應有適當之申請程序，並告	A.依據資料： (1)資訊系統管理程序 B.使用表單： (1)F1IT001 資訊平台權限申請單 (2)F1IT002 生管專家使用者權限申請單 (3) F1IT003 貿易專家使用者權限申請單 (4) F1IT004 庫存專家使用者權限申請單 (5)F1IT006 防禦病毒記錄表

	知員工使用電子郵件之規定。 16.關閉不必要之網路服務，如須提供其它網路服務應提出申請應經核准。 17.遠端登入管理資訊系統應經適當之核准。 18. 與委外廠商或第三方簽訂合約中，應包括符合公司資訊安全政策規範及法律要求。	

文件編號	C1MQ0009	版　本	C	制定日期	3-MAY-2017
作業項目	資訊循環內部控制制度			修訂日期	14-Sep-2018

CC-110-2	作業程序及控制重點	依據資料及使用表單
資通安全檢查控制	二、控制重點： 1.是否定期檢核防火牆日誌檔及防火牆設定，並經適當主管核閱。 2.防毒軟體病毒碼版本是否適時更新，並定時自動偵測病毒。 3.是否已適當考量執行資通安全檢查之人員獨立性，並已接受適當之教育訓練。 4.對於資通安全檢查之各項書面要求(如工作底稿、查核報告)是否訂定規範予以執行？管理階層應定期檢視該書面記錄，以瞭解其對規範之遵循與編製之完整性。並對檢查所提出之發現與問題，予以瞭解、追蹤及覆核改善之情形？ 5.資通安全檢查之文件是否由專責人員保管，並擬定適當之保存程序。 6.公司郵件伺服器應裝設防火牆及防毒軟體以隔絕外來侵害。 7.資訊單位應定期檢視伺服器上郵件收發情形，若有異常情況應呈報權責主管處理 8.資訊單位是否不定期提供員工資訊安全相關資訊，加強員工資訊安全之觀念。 9.是否關閉不必要之網路服務，如須提供其它網路服務應提出申請應經核准。 10.遠端登入資訊系統是否經核准。 11.是否定期覆核各系統紀錄，並加以追蹤。 12.資訊室應定期檢查非法使用之軟體應並立即移除。 13.是否訂定適當之資訊安全政策。並定期向員工宣達資訊安全政策及規定。 14.與委外廠商或第三方簽訂合約中，是否包括符合公司資訊安全政策規範及法律要求。	A.依據資料： 同上頁 B.使用表單： 同上頁