

睿信電子股份有限公司

資通安全檢查之控制作業

目的

第一條

降低系統中斷對公司電腦資訊處理作業所造成之傷害及損失，並於異常狀況發生時能迅速回復正常作業及使用狀態。

範圍

第二條

資通安全檢查之控制作業均屬之。

權責

第三條

需求單位：設置電腦資訊系統檢查機制，有效確保資訊安全。

名詞解釋

第四條

無。

控制重點

第五條

是否建置資產清冊且隨時更新。

- 二、是否設置防火牆及安裝防毒軟體。
- 三、是否定期向員工宣達資訊安全政策及規定。
- 四、委外廠商或第三方簽訂合約中，是否包括公司資訊安全政策規範及法律要求。
- 五、防火牆之日誌檔是否定期檢核，並經適當主管核閱。
- 六、資安項目之系統日誌，是否有追蹤異常之情形，並建立檢核表定期覆核各項日誌。

流程圖

第六條

無

作業內容

第七條

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，以防止駭客或電腦病毒之侵害。

二、通訊與操作管理：

1. 使用網路防火牆 (Fire Wall)，其設定應定期檢查，並經適當核准後補強防火牆軟體。
2. 防火牆之日誌檔定期檢核，並經適當主管核閱。
3. 各項網路服務之使用應依據資訊安全政策執行，關閉不必要之網路服務。如有裝置須提供其它網路服務應提出申請核准。

- 三、 不定期向員工宣達資訊安全政策及規範員工應避免透過公司網路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。
- 四、 公司員工非經權責主管授權，禁止將公司相關資訊經由電子郵件對外傳送。
- 五、 重要機密性之軟體及檔案應予以加密處理，以避免遭挪用或剽竊。
- 六、 與委外廠商或第三方簽訂合約中，應包括公司資訊安全政策規範及法律要求。
- 七、 遠端登入管理資訊系統需有適當之核准。
- 八、 本公司之「資通安全檢查表」應由資訊管理單位人員不定期執行。
- 九、 公司應每年安排資訊管理單位相關人員接受與資訊安全相關之教育訓練。

參考文件

第八條

無

附件/表單

第九條

- (一) 資通安全檢查表