

資訊通訊安全政策

1 目的

友通資訊股份有限公司(以下簡稱本公司)為確保資訊作業之機密性、完整性、可用性及適法性，避免遭受內、外部之侵擾與威脅，並衡酌本公司之業務需求，訂定本政策。

2 適用範圍

本公司員工、臨時雇員、訪客與本公司有業務往來之廠商(含員工、臨時雇員等)於維護、保管、使用、管理本公司資訊資產時，皆應遵守本政策。

3 作業內容

3.1 資訊安全目標

本公司之資訊安全目標如下：

- 3.1.1 確保本公司資訊資產之機密性，落實資料存取控制，資訊需經授權人員方可存取。
- 3.1.2 確保本公司資訊作業管理之完整性，避免未經授權之修改或作業錯誤。
- 3.1.3 確保本公司資訊持續運作之可用性，符合營運服務水準。
- 3.1.4 確保本公司資訊作業均符合相關法令規定要求。

3.2 資訊安全控制措施

- 3.2.1 本公司之資訊安全控制措施如下：
- 3.2.2 成立資訊安全管理組織，督導資訊安全管理制度之運作。
- 3.2.3 管理階層承諾維護資訊安全，持續提升資訊安全品質，避免資訊安全異常事故發生，保障客戶權益。
- 3.2.4 資訊安全管理制度文件應權衡外在變化適時更新。
- 3.2.5 定期進行資訊風險評鑑。
- 3.2.6 本公司全體人員(含業務員)皆有責任及義務保護其擁有、保管或使用之資訊資產。
- 3.2.7 工作分派應考量職能分工，職務責任範圍應予區分，以避免資訊或服務遭未經授權修改或誤用。
- 3.2.8 對於與本公司有業務往來之相關團體及其員工、臨時雇員有使用或存取本公司資訊資產之需求時，應進行必要之審核，並遵循本公司相關規範。其人員負有保護其所擁有、保管或使用本公司資訊資產之責任。
- 3.2.9 依業務需求訂定資訊作業持續運作計畫，並定期檢視調整。

- 3.2.10 訂定資訊安全指標，定期檢測，以維持資訊安全管理制度及管控程序實施之有效性。
- 3.2.11 確保工作區域場所之安全，以防範資訊資產遭竊取或毀損，落實通訊安全管理。
- 3.2.12 資訊作業或程序之開發、修改及建置，皆須符合並遵循資訊安全目標之規定。
- 3.2.13 本政策適用對象應隨時注意是否有發生資訊安全事件及違反安全政策與規範之情事，並依程序進行通報。
- 3.2.14 遵循內、外部相關法令規定，建立應有之管控程序或納入內控，定期執行資訊安全查核作業。
- 3.2.15 行動裝置之使用應與業務相關，並依程序申請後開放使用，且應採用行動裝置安全措施，以管理使用行動裝置所導致之風險。
- 3.2.16 應於資訊作業專案管理中納入資訊安全相關議題。

3.3 年度檢討

本政策每年至少檢討一次，以符合相關法令規定及資訊發展現況，並適時修正之。

3.4 罰則

- 3.4.1 本公司員工違反本政策者，其主管應要求限期改善，如限期未見改善或案件情節重大者，由當事人所屬單位部門主管、人力資源部及其他相關單位研議獎懲內容後，依本公司獎懲辦法之規定，報請權責主管核定後予以議處。
- 3.4.2 與本公司有業務往來之團體違反本規定者，應依雙方訂定之合約或約定辦理。
- 3.4.3 違反本政策並觸犯法律者，須自負民事賠償與刑事責任。若造成公司損失而賠償者，公司將逕予追償。

4 文件制修廢權責

資訊安全政策管理辦法規範由 ITS 製訂，經總經理核准後公佈實施；修訂時亦同。