

| 00000000000000000000公司 | | |
|------------------------|----------------------|---------------------------------|
| 威脅弱點清單 | | |
| 流水編號：YYY-XXXX | | 更新日期： |
| 群組 | 威脅 | 脆弱點 |
| 流程 | 人員不足 | 工作負荷過重 |
| 流程 | 人員不足 | 職責分工不當 |
| 流程 | 支援之公用設施失效(空調/水電) | 缺乏保養/維護程序或不足 |
| 流程 | 支援之公用設施失效(空調/水電) | 缺乏備援電力或備援電力不足或不穩定的供電 |
| 流程 | 支援之公用設施失效(空調/水電) | 維護服務回應時間過長 |
| 流程 | 環境損害(火、水災、地震、颱風等) | 位於特殊敏感的區域 |
| 流程 | 環境損害(火、水災、地震、颱風等) | 存放易燃物 |
| 流程 | 環境損害(火、水災、地震、颱風等) | 消防設施的不足或缺乏消防器材的保護 |
| 流程 | 失竊 | 人員安全訓練不足缺乏安全警覺 |
| 流程 | 失竊 | 外部人員缺乏人員陪同作業 |
| 流程 | 失竊 | 未經控管之資料複製 |
| 流程 | 失竊 | 建築物、房間的實體進出控制不足 |
| 流程 | 失竊 | 資料銷毀機制或程序不夠嚴謹 |
| 流程 | 失竊 | 識別與認證機制不足 |
| 流程 | 未經授權存取或使用 | 未確實陪同外部人員執行相關作業 |
| 流程 | 未經授權存取或使用 | 存取權限授與不當或未定期審查 |
| 流程 | 未經授權存取或使用 | 缺乏對資料、文件或檔案的保存、維護 |
| 流程 | 未經授權存取或使用 | 缺乏對資料複製、作廢的控管 |
| 流程 | 未經授權存取或使用 | 缺乏監督與稽核機制 |
| 流程 | 未經授權存取或使用 | 缺乏稽核軌跡 |
| 流程 | 未經授權存取或使用 | 通行碼管理不足 |
| 流程 | 未經授權存取或使用 | 通訊線路未適當保護 |
| 流程 | 未經授權存取或使用 | 離開設備(工作站/PC/NB/HOST..)未進行「登出」作業 |
| 流程 | 未經授權存取或使用 | 識別與認證機制不足 |
| 流程 | 未經授權的使用儲存媒介 | 缺乏對儲存媒介維護與監控 |
| 流程 | 使用非法軟體 | 未使用合法版權軟體或下載受控管之軟體 |
| 流程 | 使用非法軟體 | 未定期審查軟體使用情形 |
| 流程 | 社交工程 | 缺乏或不足的身份確認的機制 |
| 流程 | 社交工程 | 缺乏或不足的提供資訊的規範 |
| 流程 | 社交工程 | 缺乏或不足的資安訓練 |
| 流程 | 非法使用軟體 | 未使用合法版權軟體或下載受控管之軟體 |
| 流程 | 非法使用軟體 | 未定期審查軟體使用情形 |
| 流程 | 非法使用軟體 | 缺乏安全警覺 |
| 流程 | 非故意的疏失、修改或誤用行為導致服務中斷 | 缺乏或不足的資通安全意識 |
| 流程 | 訊息路徑錯誤或被繞道 | 缺乏正確使用通訊設備與訊息控管 |
| 流程 | 訊息路徑錯誤或被繞道 | 網路管理不足 |
| 流程 | 軟體失效 | 未適當執行軟體測試 |
| 流程 | 軟體失效 | 缺乏有效變更控制 |
| 流程 | 軟體失效 | 缺乏開發之管理或安全控制要求 |
| 流程 | 軟體失效 | 缺乏監督與稽核機制 |

| 群組 | 威脅 | 脆弱點 |
|----|-----------------------|---------------------|
| 流程 | 軟體失效 | 維護服務回應時間過長 |
| 流程 | 通訊服務失效 | 通訊線路未適當保護或失效 |
| 流程 | 通訊設備或元件失效 | 缺乏硬體耗損控管 |
| 流程 | 通訊設備或元件失效 | 維護服務回應時間過長 |
| 流程 | 惡意軟體攻擊 | 人員安全訓練不足缺乏安全警覺 |
| 流程 | 惡意軟體攻擊 | 未適當執行軟體測試或弱掃 |
| 流程 | 惡意軟體攻擊 | 缺乏安全警覺 |
| 流程 | 惡意軟體攻擊 | 缺乏有效變更控制 |
| 流程 | 惡意軟體攻擊 | 缺乏開發之管理或安全控制要求 |
| 流程 | 惡意軟體攻擊 | 軟體漏洞 |
| 流程 | 硬體失效 | 缺乏有效變更控制 |
| 流程 | 硬體失效 | 缺乏硬體耗損控管 |
| 流程 | 硬體失效 | 維護服務回應時間過長 |
| 流程 | 超載、失效、事故或營運活動意外導致服務中斷 | 缺乏或不足的資通安全意識 |
| 流程 | 超載、失效、事故或營運活動意外導致服務中斷 | 專案規劃不完整 |
| 流程 | 資料外洩或不當揭露 | 人員安全訓練不足缺乏安全警覺 |
| 流程 | 資料外洩或不當揭露 | 文件或檔案未適當存放 |
| 流程 | 資料外洩或不當揭露 | 外部人員缺乏人員陪同作業 |
| 流程 | 資料外洩或不當揭露 | 未經控管之資料複製 |
| 流程 | 資料外洩或不當揭露 | 缺乏人員安全審查程序 |
| 流程 | 資料外洩或不當揭露 | 缺乏安全警覺 |
| 流程 | 資料外洩或不當揭露 | 資料銷毀機制或程序不夠嚴謹 |
| 流程 | 資料外洩或不當揭露 | 儲存媒體的報廢或再使用未適當處理 |
| 流程 | 資料外洩或不當揭露 | 識別與認證機制不足 |
| 流程 | 資料外洩或不當揭露 | 系統已知或未知的弱點 |
| 流程 | 資料外洩或不當揭露 | 防毒軟體功能不足 |
| 流程 | 資料外洩或不當揭露 | 缺乏或不足惡意碼與行動碼之安全防護機制 |
| 流程 | 電源供應中斷 | 不穩定的電壓 |
| 流程 | 蓄意破壞 | 人員安全訓練不足缺乏安全警覺 |
| 流程 | 蓄意破壞 | 建築物、房間的實體進出控制不足 |
| 流程 | 蓄意破壞 | 缺乏安全警覺 |
| 流程 | 蓄意破壞 | 缺乏備份 |
| 流程 | 環境損害(火、水災、地震、颱風等) | 缺乏建築物、門、窗等物質的保護 |
| 流程 | 線路受損或滲透 | 未適當保護通訊線路 |
| 流程 | 操作失誤 | 缺乏有效的組態控制 |
| 流程 | 操作失誤 | 教育訓練不足 |
| 流程 | 操作失誤 | 操作文件不足 |
| 流程 | 操作失誤 | 缺乏文件操作手冊 |
| 流程 | 遺失 | 人員安全訓練不足缺乏安全警覺 |
| 流程 | 遺失 | 缺乏適當管理機制 |
| 流程 | 儲存媒體變質 | 缺乏對儲存媒介維護與監控 |
| 流程 | 儲存媒體變質 | 缺乏備份管理機制 |
| 流程 | 儲存媒體變質 | 儲存媒體維護不足或瑕疵 |

| 群組 | 威脅 | 脆弱點 |
|----|-------------------|------------------------|
| 流程 | 環境損害(火、水災、地震、颱風等) | 缺乏備份管理機制 |
| 流程 | 環境損害(火、水災、地震、颱風等) | 儲存環境控制不當 |
| 流程 | 軟體失效 | 缺乏備份管理機制 |
| 流程 | 惡意軟體攻擊 | 缺乏備份管理機制 |
| 流程 | 硬體失效 | 缺乏備份管理機制 |
| 流程 | 系統處理過程錯誤 | 品質不佳或成熟度不足 |
| 流程 | 系統處理過程錯誤 | 缺乏或不足的系統說明文件、紀錄與系統稽核軌跡 |
| 流程 | 系統處理過程錯誤 | 缺乏或不足資訊及資訊處理設施之備份與還原測試 |
| 流程 | 系統處理過程錯誤 | 設定錯誤(Mis-Config) |
| 流程 | 系統處理過程錯誤 | 硬體效能不足 |
| 流程 | 系統處理過程錯誤 | 資訊處理組態及版本控制不良 |
| 流程 | 系統處理過程錯誤 | 資訊處理變更控管不良 |
| 流程 | 系統處理過程錯誤 | 維護不當或安裝錯誤 |
| 流程 | 軟體處理過程錯誤 | 不清楚或不完整之開發規格 |
| 流程 | 軟體處理過程錯誤 | 未實施程式碼檢驗(Code Review) |
| 流程 | 軟體處理過程錯誤 | 系統發展生命週期程序或安全開發程序不足 |
| 流程 | 軟體處理過程錯誤 | 缺少有效的型態管理控制 |
| 流程 | 軟體處理過程錯誤 | 缺少有效的問題管理控制 |
| 流程 | 軟體處理過程錯誤 | 缺少有效的變更管理控制 |
| 流程 | 軟體處理過程錯誤 | 缺乏或不足的系統說明文件、紀錄與系統稽核軌跡 |
| 流程 | 軟體處理過程錯誤 | 缺乏或不足的系統開發安全管理或專案管理 |
| 流程 | 軟體處理過程錯誤 | 缺乏或不足資訊及資訊處理設施之備份與還原測試 |
| 流程 | 軟體處理過程錯誤 | 軟體系統流程設計不當 |
| 流程 | 軟體處理過程錯誤 | 測試不完整或品管不良 |
| 流程 | 軟體處理過程錯誤 | 測試計畫不完善 |
| 流程 | 軟體處理過程錯誤 | 缺乏開發之管理或安全控制要求 |
| 流程 | 系統處理過程錯誤 | 缺乏管理或安全控制要求 |