|  |  |  |
| --- | --- | --- |
|  | 資通安全事件通報單 | 　管制編號： |
| 事件通報單位聯絡資料 |
| 通報人 |  | 單位名稱 |  |
| 電 話 |  | 電子郵件 |  |
| 事件通報事項 |
| 事件發現時間 | \_\_\_年\_\_\_月\_\_\_日\_\_\_時\_\_\_分 | 通報日期 | \_\_\_年\_\_\_月\_\_\_日\_\_\_時\_\_\_分 |
| 事件類別 | □資通安全事件 □個人資料事件 □重大緊急事件 □其他事件\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 事件說明 |  |
| 設備資料(發生事件之資訊系統的詳細資訊) | IP位址 |  | Web位址 |  |
| 設備廠牌、機型 |  | 作業系統/版本 |  |
| 已裝置之安全機制 |  |
| 事件影響等級(以C, I, A最高級別為事件等級) | 機密性衝擊(單選) | □密級或敏感公務資料嚴重洩漏或國家機密資料遭洩漏(4級)□密級或敏感公務資料遭輕微洩漏(3級)　　□核心業務(含關鍵資訊基礎設施)一般資料遭洩漏(2級) □非核心業務一般資料遭洩漏(1級)　　　 □無資料遭洩漏(無需通報) |
| 完整性衝擊(單選) | □關鍵資訊基礎設施系統或資料遭嚴重竄改(4級) □核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改(3級)□非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改(2級)□非核心業務系統或資料遭竄改(1級) □無系統或資料遭竄改(無需通報) |
| 可用性衝擊(單選) | □關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作(4級)□核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(3級)□非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(2級)□非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(1級)□無系統或設備運作受影響(無需通報) |
| 事件等級判定 | □1級 □2級□3級 □4級　　(3級及4級須呈核至執行秘書以上管理階層) |
| 破壞程度 | □服務中斷 □資料庫毀損 □資料遭竊取及竄改 □系統當機 □軟硬體故障 □病毒感染□個資被竊取、竄改、毀損、滅失或洩漏 □其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 事件影響範圍及損失評估 |  |
| 事件之應變與處置 |
| 損害控制及復原作業之歷程 |  |
| 系統服務終止紀錄(必填) | □系統維持運作，無須終止服務。 □系統需終止服務(起迄時間： 年 月 日 時 分 ～ 年 月 日 時 分)，總停機時間： 日 時 分。 |
| 期望支援項目 | □是（請續填期望支援內容） □否（免填期望支援內容） |
| 期望支援內容 |  |
| □另填寫「矯正及預防處理單」將此問題列管並防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施(預防措施)，及預定完成時程和成效追蹤機制納入管制。 |
| 完成損害控制或復原作業之時間 |  \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日\_\_\_\_\_時\_\_\_\_\_\_分 |
| 承辦人員 | 單位主管 | 資安處理小組 | 執行秘書 | 資通安全長 |
|  |  |  |  |  |