資安管理自主檢核表

本所1110429版本

填表日期：　　年　　月　　日

資安管理自主檢核

| 序號 | 稽核項目 | | 自我檢核 | | | | | | | 說明 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 符合 | | 部分符合 | | 不符合 | | 不適用 |
| 資訊安全維護措施 | | | | | | | | | | |
| 1 | 遠端資料存取(如掃描)，是否有儘速下載並刪除檔案? |  | |  | |  | |  | |  |
| 2 | 是否避免將機密公文以遠端資料存取方式進行(如掃描)? |  | |  | |  | |  | |  |
| 3 | 因業務涉及機密、個資之系統，是否設定密碼或其他加密程式? |  | |  | |  | |  | |  |
| 4 | 相關電子資訊系統密碼是否避免過於簡陋易於破解 |  | |  | |  | |  | |  |
| 5 | 系統之帳號、密碼，是否避免多人共用。 |  | |  | |  | |  | |  |
| 6 | 是否知悉遭遇系統異常或其他資安事件應儘速通報單位主管應變？ |  | |  | |  | |  | |  |
| 7 | 是否定期更新防毒軟體及病毒碼? |  | |  | |  | |  | |  |
| 8 | 是否知悉涉及個資及帳號密碼等資料，須避免張貼易於察見之處? |  | |  | |  | |  | |  |
| 9 | 承上題，是否確實避免張貼密碼於易於察見之處? |  | |  | |  | |  | |  |
| 10 | 電腦是否設置螢幕保護機制，並須登錄密碼後才能使用？ | |  | |  | |  | |  |  |
| 11 | 電腦是否設置於10分鐘內產生螢幕保護程式？ | |  | |  | |  | |  |  |
| 12 | 是否定期執行各項作業系統或安裝軟體執行更新？執行更新前是否評估或測試其影響性？ | |  | |  | |  | |  |  |
| 13 | 機密性、敏感性資料是否妥善收存? | |  | |  | |  | |  |  |
| 14 | 公務上使用社群軟體，是否留意避免將機密資料於該等軟體傳送？ | |  | |  | |  | |  |  |
| 15 | 除有其他緊急需求並經核准，是否避免於個人用手機或自家電腦辦理公務？ | |  | |  | |  | |  |  |

業務負責人： 主管：

附表-資通系統防護需求分級原則

|  |  |  |  |
| --- | --- | --- | --- |
| **防護需求等級**  **構面** | 高 | 中 | 普 |
| **機密性** | 發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。 | 發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。 | 發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。 |
| **完整性** | 發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。 | 發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。 | 發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。 |
| **可用性** | 發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。 | 發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。 | 發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。 |
| **法律遵循性** | 如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。 | 如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。 | 其他資通系統設置或運作於法令有相關規範之情形。 |

備註：

* 資通系統之防護需求等級，以 與該系統相關之 機密性、完整可用及 法律遵循性構面中，任一之防護需求等級最高者定之。
* 靜置資訊，指資訊位於資通系統特定元件，例如儲存設備上之狀態，或與系統相關需要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。