**106年上半年度資訊安全廉政平台重要資訊安全案例彙整表**

|  |  |  |
| --- | --- | --- |
| 編號 | 重要資安案例概述 | 建議因應方式 |
| 1 | 系統「後台管理者權限」帳號「admin」，密碼未設定，導致容易遭有心人士嘗試帳號、密碼後，輕易取得「後台管理者權限」 | 帳號、密碼勿使用預設之「admin」，如有可能，密碼盡量複雜化。 |
| 2 | 「數位看板播放器」之儲存空間可被「網路芳鄰通訊協定」存取，且設定為「分享模式」（無密碼），導致任意使用者可任意上傳及下載檔案 | 對於相關儲存空間，應留意「網路芳鄰」之設定，並宜設定密碼。 |
| 3 | 上傳公文附件於機關網站後，移除前開附件，惟因於附件移除前，遭Google儲存為庫存頁面，故即便該附件業已移除，仍得透過「庫存頁面」功能，連結至刪除附件前之網頁，並下載該公文附件 | 於上傳任何檔案至網際網路時，應確認該檔案未涉個人資料或其他應秘密事項。 |
| 4 | 久未管理維護之網站遭行政院國家資通安全會報技術服務中心通報存有系統漏洞 | 對於所管理之網站應定期自行維護或洽相關專業廠商維護，如無使用必要，宜檢討是否需關閉相關網站。 |
| 5 | 機關上傳於公開網站之公務出國考察報告中，列出相關出國考察人員之姓名、職稱、行動電話號碼，而遭行政院國家資通安全會報技術服務中心通報。 | 行動電話號碼如連結姓名，恐遭判定屬個人資料之範疇，為避免衍生相關爭議，建議勿將行動電話納入上傳於公開網站之公務出國考察報告，或中間號碼以「X」代替。 |