**對外網站資安強化措施檢核表**

**網站基本資料**

|  |  |  |  |
| --- | --- | --- | --- |
| **網站名稱** |  | **網站負責人** |  |
| **網址** |  | **網站類別** | * 前台 * 後台 |
| **防護需求**  **等級** | * 普 * 中 | **填表日期** | 年 月 日 |
| **填表人身分** | * 網站負責人 □ 代理人 □ 廠商 | **填表人姓名** |  |

強化措施項目

[【帳號管理】 3](#_Toc163749193)

[措施1：密碼長度強制至少8字元以上 3](#_Toc163749194)

[措施2：密碼強制最低複雜度，至少三種字元變化 3](#_Toc163749195)

[措施3：密碼最短使用期限 4](#_Toc163749196)

[措施4：強制密碼最長效期 4](#_Toc163749197)

[措施5：設定密碼變更不可與前3次使用過之密碼相同 5](#_Toc163749198)

[【日誌管理】 6](#_Toc163749199)

[措施6：日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊 6](#_Toc163749200)

[【後台管理】 6](#_Toc163749201)

[措施7：檔案上傳限「必要」且「特定類型」的檔案 6](#_Toc163749202)

[措施8：後台限制帳號登入來源 7](#_Toc163749203)

[措施9：資料庫/檔案須加密「使用者密碼」資訊 8](#_Toc163749204)

[措施10：帳號授權採最小權限原則 8](#_Toc163749205)

[措施11：定期審查(至少每年一次)「網站」、「主機」、「資料庫」帳號 9](#_Toc163749206)

[措施12：刪除已逾期之臨時帳號、緊急帳號及閒置帳號 9](#_Toc163749207)

# 【帳號管理】

## 措施1：密碼長度強制至少8字元以上

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **舉證以提供「程式碼」為原則，或可提供「主機設定」資訊** |
| **舉證** |  |

## 措施2：密碼強制最低複雜度，至少三種字元變化

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **密碼應有字元變化，如使用：**   1. **英文大寫字元（A 到Z）** 2. **英文小寫字 元（a 到z）** 3. **10 個基本數字（0 到9）** 4. **非英文字母字元（如！、 ＄、＃、 ％）**   **舉證以提供「程式碼」為原則，並提供系統上的「網站密碼設定畫面」** |
| **舉證** |  |

## 措施3：密碼最短使用期限

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **在使用者變更密碼之前，密碼必須使用的期限，如1日**  **舉證以提供「程式碼」為原則，或可提供「主機設定」資訊** |
| **舉證** |  |

## 措施4：強制密碼最長效期

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **至少要求密碼每180天要變更一次**  **舉證以提供「程式碼」為原則，或可提供「主機設定」資訊** |
| **舉證** |  |

## 措施5：設定密碼變更不可與前3次使用過之密碼相同

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **舉證以提供「程式碼」為原則，並提供系統上的「密碼設定畫面」資訊** |
| **舉證** |  |

# 【日誌管理】

## 措施6：日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **日誌應詳細描述所觸發事件，如：使用者帳號、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。**  **惟須注意應避免在日誌內留下個人資料及涉及隱私內容，以符合我國個人資料保護法相關規定。**  **舉證可摘錄日誌「表頭」完整內容及部分LOG資訊(有特殊考量部分，請遮蔽)** |
| **舉證** |  |

# 【後台管理】

## 措施7：檔案上傳限「必要」且「特定類型」的檔案

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **舉證以提供「程式碼」為原則，並提供系統上的「檔案上傳的說明」資訊** |
| **舉證** |  |

## 措施8：後台限制帳號登入來源

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **舉證請提供「系統限定特定IP連線之設定」資訊** |
| **舉證** |  |

## 措施9：資料庫/檔案須加密「使用者密碼」資訊

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **舉證請提供資料庫「使用哪種加密方式」與「資料庫加密後」資訊(有特殊考量部分，請遮蔽)** |
| **舉證** |  |

## 措施10：帳號授權採最小權限原則

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **依網站使用需求，給予各類人員必要之系統存取權限，如：一般使用者應避免使用業務負責人權限或最高權限。**  **舉證請提供「權限申請流程」、「權限申請單」、「權限清單」、「權限角色類型」、「最高權限名稱&數量」(有特殊考量部分，請遮蔽)** |
| **舉證** |  |

## 措施11：定期審查(至少每年一次)「網站」、「主機」、「資料庫」帳號

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **舉證請分別提供「網站」、「主機」、「資料庫」的審查紀錄表(有特殊考量部分，請遮蔽)** |
| **舉證** |  |

## 措施12：刪除已逾期之臨時帳號、緊急帳號及閒置帳號

|  |  |
| --- | --- |
| **結果** | **□有做到(請將佐證貼至【舉證】處)**  **□未做到，預計\_\_\_\_年\_\_\_\_月\_\_\_\_日完成改善**  **□不適用，理由：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **舉證說明** | **舉證可提供「定期審查紀錄表」中，哪一些屬於臨時帳號、緊急帳號及閒置帳號，並舉證是否已刪除，或有設定預計刪除時間(有特殊考量部分，請遮蔽)** |
| **舉證** |  |