|  |  |
| --- | --- |
| 文件編號：SMS-4-001-001-001 | 機密等級：□普 ☑中 □高  |
| 文件名稱：文化部網站(系統)作業申請表 | 版次：10.3 |
| 表單編號：SMS-4-001-001-001-12-\_\_\_\_ | 日期：112/03/06 |

文化部網站（系統）主機建置作業申請表

|  |
| --- |
| **網站（系統）名稱：** |
| 預定上線日期：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日（如有分內外部上線日不同請特別說明） |
| 預定下架日期：□非屬專案性質，無定有下架日期。□屬專案性質，預定於\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日下架。（計畫專案結束等） |
| 預定存置機房： 由管理單位(資訊處資安科)決定。(※預設都存置於「新莊機房」。) □新莊機房。 □國光機房。 □HiCloud雲端機房。 □其他機房：\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |
| □已完成整併主機評估，本次申請主機無法併入，其原因：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |
| 類別：□新網站 □舊網站移機 □其它(請於申請用途欄位中說明) |
| 網站使用對象：□僅內部同仁(即擺放在Trust) □民眾及內部同仁(即擺放在DMZ) □其他：(※如果主要使用對象是民眾，內部同仁僅作瀏覽或管理後台，請勾選「民眾及內部同仁」。) |
| 申請用途說明：(請說明網站或系統設立依據、目的、目標使用範圍及數量。) |
| 機關名稱：業務單位(司處/科組室)：業務聯絡人：　聯絡電話：　電子郵件： | 維護廠商名稱：維護廠商聯絡人：　　　聯絡電話：　　　電子郵件：維護廠商工程師：　　　聯絡電話：　　　電子郵件： |
| 1. **系統架構：**

**1.1VM硬體規格：**(原則上4C4G，得依系統使用情況彈性增減，如超過預設請填寫說明)* CPU:\_\_\_\_\_core。
* Memory: \_\_\_\_\_GB。
* 說明(超過預設才需填寫原因)：

**1.2硬碟容量：**(原則上作業系統區50 GB、資料存放區50GB，鑒於硬碟空間資源有限，請填寫實際需要量，未來若有空間不足情形，得再擴充)【Windows】* 作業系統區(Disk C)容量: \_\_\_\_\_GB。
* 資料存放區(Disk D)容量: \_\_\_\_\_GB。

 【Linux】* 作業系統區(根目錄)容量: \_\_\_\_\_GB。
* 資料存放區容量: \_\_\_\_\_GB。(路徑：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

 ※如為一般網站僅填寫作業系統容量即可，不分區。  說明(超過預設才需填寫原因)：**1.3作業系統：** (請勾選，如特殊版本需求請另註明)□Windows Server 2019 64bit(含)以上□Linux Ubuntu 22.04 LTS（含）以上□其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * Hostname：
* 登入帳號：

(原生最大管理者由本部掌管，維護廠商帳號另外建立)**1.4資料庫：** (請勾選，本部資料庫採共構集中管理，另本部資料庫平台與AP主機分屬不同網段，不對外開放，僅能透過AP主機存取資料，DB由本部機房工程師負責建置與管理。如有特殊版本需求請另註明。)□無資料庫，屬靜態網頁。□MS SQL Server 2019。□MariaDB 10.4.11。* DB名稱：
* 存取帳號：

**1.5程式語言及執行套件說明**：(請勾選，如無使用該項則無需勾選填寫，若有使用則務必填寫預計使用版本。下方僅列常見工具，若使用工具不在列表上則請自行擴充填寫。)

|  |  |  |  |
| --- | --- | --- | --- |
| 是否使用 | 程式語言或開發工具 | 版本(※請使用最新版本) | 備註 |
| □是 □否 | Apache |  |  |
| □是 □否 | Tomcat |  |  |
| □是 □否 | PHP |  |  |
| □是 □否 | Nginx |  |  |
| □是 □否 | IIS | 10 | Windows Server 2019預設內建 |
| □是 □否 |  |  | (請自行增列) |

**1.6系統架構圖：**(得以附件方式提供，並請標示網站之前台、後台、File主機、DB主機等角色，俾瞭解資料存取路徑。) (※此為範例)1. **防火牆開通：**(請條列系統上線後需對外提供之service (protocol)以及port號等，俾利進行防火牆開通設定。)(註：原則不開放廠商遠端連線及電子報SMTP服務，請由業務單位另案申請！)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 來源 | 目的 | 服務/協定 | TCP/UDP | 埠號 | 備註 |
| Any | AP主機 | HTTPS | TCP | 443 | 為提高網站安全性，請務必啟用HTTPS服務，並把私密金鑰檔提供給本部機房工程師，俾進行閘道端防護設定 |
| AP主機 | DB主機 | MS-SQL | TCP | 1433 | 資料庫請二擇一(如：用MSSQL，則刪MariaDB，反之)。 |
| AP主機 | DB主機 | MariaDB | TCP | 3306 | 資料庫請二擇一(如：用MariaDB，則刪MSSQL，反之)。 |
| 廠商IP(同7.) | AP主機 | RDP | TCP | 9938 | 遠端請二擇一(如：Windows主機，則刪SSH，反之)。(※本部將原預設port 3389改掉。) |
| 廠商IP(同7.) | AP主機 | SSH | TCP | 22 | 遠端請二擇一(如：Linux主機，則刪RDP，反之)。 |
|  |  |  |  |  | (請自行增列) |

 ※AP及DB主機IP由本部配發。1. **主機啟動與關機時需注意事項：**(請務必將相關程序設定為開關機自動啟用，避免本部因特殊原因須重啟設備時導致系統或網站服務不正常。)

 □無注意事項，該自動帶起服務或程式皆已完成設定。 □請注意以下事項： 1. **備份機制：**(請勾選，請評估系統或網站資料寫入頻繁度選擇。)

【新莊/國光機房】□ A每日差異備份/每週六完整備份。□ B每季完整備份。【HiCloud機房】★會影響費用。□ C每日快照□ D每週六快照□ G自訂快照：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。□ H保留\_\_\_\_\_\_代。1. **網站檔案大小**：（原則以GB計，若為移機系統或網站，請填寫目前檔案大小。）
2. 網站程式碼大小（含資料）：\_\_\_\_\_\_\_\_ □GB □MB。
3. 網站資料庫大小：\_\_\_\_\_\_\_\_ □GB □MB。
4. 未來網站資料量預估成長量（By年）：\_\_\_\_\_\_\_\_ □GB □MB。
5. **網站網址（DNS）設定：**(網站須強制啟用HTTPS，並強制關閉TLS 1.1以下版本。另網站通過弱掃檢測後，方能對外開放，詳下方之網站上線前標準作業流程。)

 □前台網址：https ://\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □內部用 □內外部用 □後台網址：https ://\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □內部用 □內外部用 □非系統或網站類或不使用網址(※不得使用IP網址)。1. **遠端連線來源IP：**(考量資安，原則只開1組，若有第2組，請說明原因，且以2組為限。另須採固定IP，不可為浮動IP。本申請表僅限開放廠商為網站佈署之2個星期遠端連線，若廠商需延長使用期，請業務單位至EIP電子表單塡寫「遠端連線申請單」。)

 第一組：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 第二組：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，申請原因：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_1. **依資通安全管理法子法「資通安全責任等級分級辦法」規定，資通系統應依其辦法之附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施，請填寫「資通系統防護需求等級評估表」(如附件)。**
2. **其他：(特殊軟體或其他需求)**
3. **網站上線前標準作業流程如下：**
4. 資訊處依據申請表需求，完成虛擬機環境建置。
5. 維護廠商完成資訊網站(系統)之應用程式佈署與測試。**(首次安裝，須到部佈署，之後開放1次2周遠端連線，以利佈署)**
6. 維護廠商遠端連線時間如超過2周方能完成佈署，請業務單位塡寫「EIP電子表單/資訊類/遠端連線申請單」。（※張志誠，02-85126000#6674，marcochang@moc.gov.tw）
7. 維護廠商應自行辦理主機及網頁弱點掃描，降低整體掃描時間並加速上線時間。
8. 業務單位填寫「EIP電子表單/資訊類/弱點掃描服務申請單」，由資訊處進行「準備階段」之主機及網頁弱點掃描。（※陳煥民，02-85126000#6677，soc@moc.gov.tw）
9. 維護廠商修補漏洞，完成漏洞修補後，再次執行上開步驟(5)，需修補到無中級以上風險方可申請憑證。另此階段因尚未申請憑證，故可暫時允許SSL憑證相關弱點。
10. 業務單位填寫「EIP電子表單/資訊類/GTLSCA伺服器應用軟體憑證申請單」，由資訊處申發GTLSCA伺服器應用軟體憑證，以啟用HTTPS。（※胡永明，02-85126000#6672，ymh@moc.gov.tw）
11. 業務單位填寫「EIP電子表單/資訊類/弱點掃描服務申請單」，由資訊處進行「上線階段」之主機及網頁弱點掃描。（※陳煥民，02-85126000#6677，soc@moc.gov.tw）
12. 維護廠商修補漏洞，完成漏洞修補後，再次執行上開步驟(8)，需修補到無中級以上風險方可申請正式上線。
13. 網站正式上線：業務單位填寫「EIP電子表單/資訊類/共構DNS服務申請單」，對外公告網站網址。（※張志誠，02-85126000#6674，marcochang@moc.gov.tw）
14. **注意事項：**
	* 網站如有發送系統通知信或電子報需求，請於網站完成建置後，由業務單位洽本部電郵系統承辦人，申請SMTP relay server。（※陳冠豪，02-85126000#6667，rogerchen@moc.gov.tw）
	* 網站如有設置客服信箱需求，請逕向各機關公務信箱帳號管理員申請。（請注意！本部嚴禁利用公務信箱進行電子報發送作業，以免本部電郵系統被列為垃圾信主機黑名單。）
	* 為提高主機安全性，**本機防火牆需開啟**，維護廠商不得隨意關閉。
	* 後台網站應僅提供本部內部同仁存取，如有對外開放之必要，請務必限制可存取之來源IP。
 |
| **需求單位審核區****(請核章，由需求單位自行評估審核層級)** |
|  |
| **預計提供軟硬體環境資源****(以下欄位起，由資訊處填寫)** |
| 系統IP/軟體資訊 | 硬體資源 |
| 存置機房： □ 新莊機房 □ 國光機房  □ 其他機房：\_\_\_\_\_\_\_\_\_\_\_建置區域： □ Trust □ DMZ □其他外部IP：內部IP：系統帳號：資料庫IP： 資料庫版本：資料庫名稱：資料庫帳號： | CPU：每台\_\_\_\_\_\_\_顆。(※預設給4顆)RAM：每台\_\_\_\_\_\_\_GB。(※預設給4GB)OS：□Windows：□Linux：HDD： |
| **資訊處需求審核區** |
|  |
| **執行結果(請檢附相關佐證資料)** |
| 請確認執行以下作業：●依主機出廠標準設定【Windows】 □安裝防毒軟體，預設為Trendmicro ApexOne，核心系統安裝Trendmicro DSA(全模組)。□啟用WSUS：**(新莊機房)DMZ(AP/DB)設定為10.40.100.204；Trust(AP/DB)設定為10.1.1.204。****(國光機房)設定為10.30.50.204。****(HiCloud機房)設定為10.60.2.9。**□啟用本機防火牆，僅開啟系統所需通訊埠，其餘一律關閉。□啟用密碼原則，設定為複雜度為4選3、密碼長度為12碼以上及密碼有效期為60天等。□將原生管理者改名。□將遠端連線(RDP)埠改為9938。【Linux】□安裝防毒軟體，預設為Trendmicro DSA(防毒)，核心系統安裝Trendmicro DSA(全模組)。□啟用OS Update。 □啟用本機防火牆，僅開啟系統所需通訊埠，其餘一律關閉。 □啟用密碼原則，設定為複雜度為4選3、密碼長度為12碼以上及密碼有效期為60天等。【通用】□啟用時間校時(NTP)： **(新莊機房)設定為10.1.1.192。****(國光機房)設定為10.30.40.101。****(HiCloud機房)設定為10.60.2.9。**□設定主機備份排程。□安裝EDR/MDR軟體：**(新莊/國光機房)安裝**Xensor EDR軟體。(HiCloud機房)安裝FirEye MDR軟體。□安裝ForeScout軟體。□更新本部主機服務資源清單及機櫃圖。 |
| **資訊處執行審核區** |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | 表單編號： |
| **「ＯＯＯ資通系統」防護需求等級評估表** |
| **功能說明：** |
| **業務屬性：□行政類□業務類　　 日期：\_\_\_年\_\_\_月\_\_\_日****共同性系統：□是 □否** |
| **影響構面** | **資通系統防護需求等級****(取其四大影響構面安全等級最高者)** |
| **1.機密性** | **2.完整性** | **3.可用性** | **4.法律遵循性** |
| 　 | 　 | 　 | 　 | 　 |
| 步驟：設定影響構面等級 |
| 影響構面 | 防護需求等級(普、中、高) | 原因說明 |
| **1.機密性** | 初估 | 　 | 　 |
| 異動 | 　 | 　 |
| **2.完整性** | 初估 | 　 | 　 |
| 異動 | 　 | 　 |
| **3.可用性** | 初估 | 　 | 　 |
| 異動 | 　 | 　 |
| **4.法律遵循性** | 初估 | 　 | 　 |
| 異動 | 　 | 　 |
| 步驟➋：識別業務屬性 |  |  |  |  |  |  |
| 項目 | 業務屬性(行政或業務) | 原因說明 |
| 識別業務屬性 | 初估 | 　 | 　 |  |
| 異動 | 　 | 　 |
| 備註 | 　　 |
| 承辦人 | 複核人員(1) | 複核人員(2) | 複核人員(3) | 承辦單位主管 |
| 　 | 　 | 　 | 　 | 　 |
| 註：請各機關依本身實際陳核流程調整簽核欄位。註：**共同性系統**，包含共用性系統與共通性系統，共用性系統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作，如國稅系統。共通性系統指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資料主要儲存於使用機關，如公文電子交換系統。 |

**「全球資訊網(參考範例)」防護需求等級評估表**

|  |
| --- |
| **功能說明：機關官方網站，提供機關簡介及政策措施介紹，並無提供線上申辦等服務。** |
| **業務屬性：□行政類**■**業務類 　　　　　日期：\_\_年\_\_月\_\_日****共同性系統：□是 □否** |
| **影響構面** | **資通系統防護需求等級** |
| **1.機密性** | **2.完整性** | **3.可用性** | **4.法律遵循性** |
| 普 | 普 | 普 | 普 | 普 |
| 步驟：設定影響構面等級 |
| 影響構面 | 防護需求等級 | 原因說明 |
| **1.機密性** | 初估 | 普 | 網站資訊均為可公開之一般性資料 |
| 異動 | 　 | 　 |
| **2.完整性** | 初估 | 普 | 本網站主要提供資訊公告 |
| 異動 | 　 | 　 |
| **3.可用性** | 初估 | 普 | 本網站提供一般性資料瀏覽 |
| 異動 | 　 | 　 |
| **4.法律遵循性** | 初估 | 普 | 本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果 |
| 異動 | 　 | 　 |
| 步驟➋：識別業務屬性 |  |  |  |  |
| 項目 | 業務屬性 | 原因說明 |
| 識別業務屬性 | 初估 | 業務類 | 本系統提供機關簡介、政策措施介紹等對外資訊服務，無涉及機關業務線上申辦等其他服務，屬機關業務類系統 |
| 異動 | 　 | 　 |
| 備註 | 　 |
| 承辦人 | 複核人員(1) | 複核人員(2) | 複核人員(3) | 承辦單位主管 |
| 　 | 　 | 　 | 　 | 　 |

註：請各機關依本身實際陳核流程調整簽核欄位。

註：**共同性系統**，包含共用性系統與共通性系統，共用性系統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作，如國稅系統。共通性系統指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資料主要儲存於使用機關，如公文電子交換系統。

附表九 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、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

附表十 資通系統防護基準

|  |  |  |  |
| --- | --- | --- | --- |
| 系統防護需求分級控制措施 | 高 | 中 | 普 |
| 構面 | 措施內容 |
| 存取控制 | 帳號管理 | 一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。三、應依機關規定之情況及條件，使用資通系統。四、監控資通系統帳號，如發現帳號違常使用時回報管理者。五、等級「中」之所有控制措施。 | 一、已逾期之臨時或緊急帳號應刪除或禁用。二、資通系統閒置帳號應禁用。三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。四、等級「普」之所有控制措施。 | 建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 |
| 最小權限 | 採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。 | 無要求。 |
| 遠端存取 | 一、遠端存取之來源應為機關已預先定義及管理之存取控制點。二、等級「普」之所有控制措施。 | 一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。二、使用者之權限檢查作業應於伺服器端完成。三、應監控遠端存取機關內部網段或資通系統後臺之連線。四、應採用加密機制。 |
| 事件日誌與可歸責性 | 記錄事件 | 1. 應定期審查機關所保留資通系統產生之日誌。

二、等級「普」之所有控制措施。 | 一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。三、應記錄資通系統管理者帳號所執行之各項功能。 |
| 日誌紀錄內容 | 資通系統產生之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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。 |
| 日誌儲存容量 | 依據日誌儲存需求，配置所需之儲存容量。 |
| 日誌處理失效之回應 | 一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。二、等級「中」及「普」之所有控制措施。 | 資通系統於日誌處理失效時，應採取適當之行動。 |
| 時戳及校時 | 一、系統內部時鐘應定期與基準時間源進行同步。二、等級「普」之所有控制措施。 | 資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 |
| 日誌資訊之保護 | 一、定期備份日誌至原系統外之其他實體系統。二、等級「中」之所有控制措施。 | 一、應運用雜湊或其他適當方式之完整性確保機制。二、等級「普」之所有控制措施。 | 對日誌之存取管理，僅限於有權限之使用者。 |
| 營運持續計畫 | 系統備份 | 一、應將備份還原，作為營運持續計畫測試之一部分。二、應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。三、等級「中」之所有控制措施。 | 一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。二、等級「普」之所有控制措施。 | 一、訂定系統可容忍資料損失之時間要求。二、執行系統源碼與資料備份。 |
| 系統備援 | 一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。 | 無要求。 |
| 識別與鑑別 | 內部使用者之識別與鑑別 | 一、對資通系統之存取採取多重認證技術。二、等級「中」及「普」之所有控制措施。 | 資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。 |
| 身分驗證管理 | 一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。三、等級「普」之所有控制措施。 | 一、使用預設密碼登入系統時，應於登入後要求立即變更。二、身分驗證相關資訊不以明文傳輸。三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。五、密碼變更時，至少不可以與前三次使用過之密碼相同。六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。 |
| 鑑別資訊回饋 | 資通系統應遮蔽鑑別過程中之資訊。 |
| 加密模組鑑別 | 資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。 | 無要求。 |
| 非內部使用者之識別與鑑別 | 資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。 |
| 系統與服務獲得 | 系統發展生命週期需求階段 | 針對系統安全需求（含機密性、可用性、完整性）進行確認。 |
| 系統發展生命週期設計階段 | 一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。 | 無要求。 |
| 系統發展生命週期開發階段 | 一、執行「源碼掃描」安全檢測。二、系統應具備發生嚴重錯誤時之通知機制。三、等級「中」及「普」之所有控制措施。 | 一、應針對安全需求實作必要控制措施。二、應注意避免軟體常見漏洞及實作必要控制措施。三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 |
| 系統發展生命週期測試階段 | 一、執行「滲透測試」安全檢測。二、等級「中」及「普」之所有控制措施。 | 執行「弱點掃描」安全檢測。 |
| 系統發展生命週期部署與維運階段 | 一、於系統發展生命週期之維運階段，應執行版本控制與變更管理。二、等級「普」之所有控制措施。 | 一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。二、資通系統不使用預設密碼。 |
| 系統發展生命週期委外階段 | 資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。 |
| 獲得程序 | 開發、測試及正式作業環境應為區隔。 | 無要求。 |
| 系統文件 | 應儲存與管理系統發展生命週期之相關文件。 |
| 系統與通訊保護 | 傳輸之機密性與完整性 | 一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。二、使用公開、國際機構驗證且未遭破解之演算法。三、支援演算法最大長度金鑰。四、加密金鑰或憑證應定期更換。五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。 | 無要求。 | 無要求。 |
| 資料儲存之安全 | 資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。 | 無要求。 | 無要求。 |
| 系統與資訊完整性 | 漏洞修復 | 一、定期確認資通系統相關漏洞修復之狀態。二、等級「普」之所有控制措施。 | 系統之漏洞修復應測試有效性及潛在影響，並定期更新。 |
| 資通系統監控 | 一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。二、等級「中」之所有控制措施。 | 一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。二、等級「普」之所有控制措施。 | 發現資通系統有被入侵跡象時，應通報機關特定人員。 |
| 軟體及資訊完整性 | 一、應定期執行軟體與資訊完整性檢查。二、等級「中」之所有控制措施。 | 一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。 | 無要求。 |