國軍網站管理作業規定

民國 95 年 12 月 8 日捷拓字第 0950003195 號令頒
民國 110 年 1 月 13 日國通資安字第 1100010344 號令頒
民國 113 年 8 月 7 日國通軟資字第 1130211521 號修正

一、為律定國軍軍、民網網站管理權責區分、範圍、設置及管理原則與作業流程，以為各級單位網站管理作業依據，特訂定本規定。

二、適用範圍：

國軍各單位於軍、民網設置網站（含提供網頁式服務之各式資訊系統）提供服務者均適用，專屬網路部分由主管單位另令訂之。

三、本規定用詞，定義如下：

（一）國軍網路：指國軍使用 TCP/IP 網路通信協定標準之網路總稱。

（二）國軍資訊網路(MINET，以下簡稱軍網)：指國軍網路內提供國軍人員資訊作業之網路環境。

（三）民網：包括行政民網（單一閘口民網）、專線民網（非單一閘口民網）、軍事院校學術網路（學網 TANET）及國軍醫院醫療網路等四類網路環境。

（四）專屬網路（簡稱專網）：指國軍網路內所有自主運作且與他網隔離之專用網路，包括戰情、情報及捷訊網等。

（五）網頁（Web Page）：指使用者透過瀏覽器（如 Edge、Chrome、Firefox 等）存取相關資訊之頁面，主要由文字、聲音、圖像、動畫及影片等元素所組成。

（六）網站（Web Site）：網站為在網路上，根據一定的規則，使用 HTML 等格式運行在網頁伺服器上，展示特定內容網頁之集合。

（七）網站服務（Web Service）：以服務導向架構的技術，透過標準的 Web 協定提供服務，目的是保證不同平臺的應用服務可以互相操作。

（八）雲端服務提供者（Cloud Service Provider, CSP）：提供雲端

式平臺（Cloud Platform）、基礎結構（Infrastructure）、應用程式（Application）、可擴式運算資源（Scalable Computing Resource）及儲存設備（Storage）服務的廠商。

四、權責劃分：

（一）國防部政務辦公室（以下簡稱政辦室）：

1.國防部民網網站內容政策指導、規劃、建置及管理。

2.國軍各單位民網網站內容政策指導及規劃。

3.國軍各單位民網網站建置申請審核、網站評鑑及不定期內容檢核。

4.國防部全球資訊網網站資安檢測作業。

（二）國防部參謀本部通信電子資訊參謀次長室(以下簡稱通次室)：

1.國軍網站管理政策制訂、管理與督考。

2.列管國軍已核定軍、民網網站。

3.國軍各單位網站建置架構技術指導。

4.提供國軍各單位網站原始碼掃描服務。

5.國軍民網雲端標準資安架構管理。

（三）國防部政治作戰局（以下簡稱政戰局）：

1.國軍各單位網頁內容保密安全諮詢與複審。

2.國軍各單位網頁資料線上監審。

3.國軍各單位網站肇生洩（違）密事件通報及查察。

（四）國防部資通電軍指揮部(以下簡稱資通電軍)

1.網站資安監控及稽核作業。

2.駭侵事件調查。

3.協助各單位駭侵事件查察。

4.每月辦理各單位網站弱點掃描。

（五）國防部部本部、參謀本部及直屬機關（單位）、各司令部及軍

事學校（以下簡稱管理機關）：

1.所屬單位網站管理與督考。

2.所屬單位網站建置申請審核及資安檢測作業。

3.所屬單位網站資訊安全稽查。

4.所屬單位網站違規事件查處及駭侵事件查察。

（六)管理機關所屬各級通電資業務單位(以下簡稱通電資業務單位)：

1.網站需求初審及申請。

2.協助網站需求單位網站建置作業。

3.業管網站違規事件處理及駭侵事件查察。

（七）網站需求及管理單位（以下簡稱網站需求單位）：

1.網站建置需求申請、發展及管理維護。

2.網站網頁內容管理及網頁資料線上監審（網頁內容保密安全審查）。

3.網站資訊安全定期自我檢測。

4.業管網站違規事件處理及駭侵事件查察。

五、網站設置及管理原則：

（一）嚴禁私自架設聊天室、個人網站、部落格(Blog)等各式服務，網站設置目的應以公務交流協調為主。

（二）編階中校主官以下、未編設資訊（安）人力且無專屬機房、網路資安防護環境之單位，不得設置網站。

（三）討論區或留言板，應於奉核設立後，指派專人定期檢視或解答，避免肇生不法言論或資安事件；並掌握登入者來源資料，如發現違反行政中立原則、影響國軍形象等不當言論及色情圖文等，應立即刪除討論內容與留存紀錄，並依情節轉由相關人員勸導處理。

（四）網站管理單位應定期檢查網站日誌檔（Log）、磁碟空間、依構型資料檢查檔案異動情況或設置自動化預警系統，於網站遭入

侵或置換網頁時，提出告警，並及時還原網站內容以維持正常運作，同時追查原因並循 MCERT（國軍電腦緊急應變中心）機制通報。

（五）各單位設於軍、民網環境之網站，包含內部網站及測試用網站等，均須納入國防部統籌管理，並於每半年（六月及十二月）完成網站清校作業（如附件一）。

（六）公布於網站之文件（如公文書、通報、新聞稿或活動訊息等），應經單位機密等級審查確屬可公開性資料，由權責長官核定、通過防毒軟體檢測無虞後，始可登載於網站。

（七）公開於軍、民網環境之網站應向權責單位申請網域名稱(Domain Name）以供連線（如 www.mil.tw），不得以 IP 位址直接公開。

（八）有關軍、民網網站網域名稱相關規定，以網站服務形式公開者，依規定完成網域名稱申請，軍網依軍網目錄服務系統發展指導要點完成申請；另民網網站網址註冊原則，除應向政辦室申請之網域(mnd.gov.tw)外，學校單位為 edu、機關(單位)及醫院為 gov、機關團體(財團法人、基金會、公協會等)為 org，向各管理機關申請。軍、民網網站均不得註冊為 com 網址，如因特殊任務需求而改其它分類者，需專案簽奉國防部核定後使用。

（九）民網網站設置規範、版面設計、資料更新維護及網站評鑑等項，應符合國防部全球資訊網網站服務評鑑實施計畫規範。

六、各單位視業務需要，應律定網站維護分工權責，管理方式如下：

（一）機房維運管理：

1.依國軍資訊安全政策，各網系依專網專用原則進行隔離，網系內資訊資產（含機櫃、主機、網路設備及線路等）均不得跨網系混接。

2.網站主機屬雲端化者，應在資安防護措施足夠(如防火牆、入侵

偵測系統等)下提供服務；設置於地端者，應符合國軍資訊通信及電子戰機房設置要點之通電資機房規定。

3.網站主機應律定資訊人員或資安承辦人專責維護與管理，並納入機房管理作業監控項目。

4.值勤人員應負責執行資安防護監控作業，發現入侵徵候或其他資安事件，應立即處置及通知管理人員處理，並循 MCERT 機制回報後採取復原措施。

（二）網站主機管理：

1.共同性原則：

(1)應啟動作業系統事件紀錄，維管人員或值勤人員應定期檢查日誌檔（Log），並定期備份與維護紀錄檔完整性，以保持網站正常運作，紀錄檔應保存一年以上，作為資安事件發生追查依據。

(2)網站正式上線運作後，應移除非需要程式碼檔案或多餘檔案程式（如.bak 檔）。

(3)維護網站網頁管理與值勤人員帳號，應以最低管理權限原則（Principle of Least Privilege）賦予權限，並限制管理作業之 IP 位址、建立事件紀錄及檢核機制（如來源/目的 IP、連接埠、時間紀錄等項）。

(4)主機啟用前，應完成部頒資安管控軟體與防毒軟體安裝及相關資安設定（含漏洞修補），並納入單位緊急應變等相關計畫，定期實施伺服器故障、應用服務中斷或遭駭客入侵等演練。

(5) 主機啟用後，應不定期完成作業系統及相關應用程式，漏洞修正與安全性更新等作業。

(6) 網站主機前端應部署防火牆對資料流通進行過濾與監控，

所產生之日誌均須納入資通電軍 MSOC 監控。

2.軍網管理原則：主機上線前應完成國軍營區網路管理系統註冊開通。

3.雲端管理原則：

(1)虛擬機器遷移作業完成後,應先進行網站各項安全性認證與服務一致性檢測等措施，確保成功搬遷與安全運行。

(2)應設置流量清洗及內容傳遞網路（CDN）、入侵防護及監測活動等資安管控系統，以阻止流量攻擊、提升防禦能量，並對使用者連線資源之適法性相關紀錄，進行及時監控與檢視。

(3)系統管理應配合零信任架構,提供多因子認證機制,並具有備份還原機制。

（三）網站應用服務管理：

1.網站（資訊系統）上線前，須完成原始碼檢測及弱點掃描等安全檢測作業，完成風險修正後始可上線；網站（資訊系統）上線後，須持續漏洞發布與修補、原始碼檢測及弱點掃描等作業，以確保系統服務安全。

2.網站（資訊系統）上線後，如經原始碼檢測或弱點掃描檢測出具高風險項目應於一個月內立即改正，中、低風險項目應於三個月內修正完畢。

3.網站（資訊系統）如提供行動化服務（APP），應依行政院及所屬各機關行動化服務發展作業原則第十一點規定，各機關開發之行動化服務應符合個人資料保護法及行政院訂定之政府資通安全管理相關規定，並通過經濟部產業發展署訂定行動化應用軟體檢測項目，始得提供使用者（民眾）下載。

4.網站應採用已知非具安全風險傳輸通訊協定（如：HTTPS）加密傳輸。

5.各單位因業務需要提供上傳檔案之功能應具帳號權限管制措施,並能記錄上傳來源,且於上傳檔案存放位置做好資安設定。

6.應設帳號權限管理設計機制，並有帳號申請及權限管理流程。

7.各單位網頁式應用系統設計應朝向統一服務窗口整合,例如經由各單位入口網站下提供相關連結服務;網站結構設計應以服務功能性為主、組織結構導向為輔，避免因組織調整，造成網站需大幅修改或疏於管理。

8.為強化隱私安全,各單位得參考數位發展部所定隱私強化技術應用指引，依保護目標，評估適宜保護技術機制，以降低資料遭竊風險，增進資料當事人信任及隱私防護。

（四）資料庫管理：

1.資料庫應定期執行備份作業，以防止資料遺失。

2.資料庫應設定較嚴謹之網路連線機制，透過嚴謹白名單（如僅開放應用系統伺服器及管理者連線）及開放特定連線埠，以有效管控網路連線行為。

3.帳號應區分權限使用，嚴禁帳號交予他人使用或與他人共用帳號。

（五）網頁管理：

1.網站（頁）所使用文字、圖檔、影音、元件及程式等不得違反智慧財產權及著作權法等相關法令規範。

2.表單輸入須具有防止 HTML 標記（Tag）輸入機制，並加入資料隱碼（SQL injection）、緩衝區溢位（Buffer Overflow）及跨網站指令碼攻擊（Cross-Site Script）等防範程式，以防範網頁入侵行為。

3.網頁圖檔設計大小應以不影響網站瀏覽傳輸速度為考量。

4.討論區或留言板首頁應明顯標示資安、嚴守行政中立及保密等警語、宣導禁止談論非主題相關內容及不當言論。

（六）雲端服務政策管理：

1.盤點應遵循之法規，設定管理基準，契約與服務水準協議應包含雲端服務內容與保證、雲端服務中雙方之權利與義務等項，以確保符合單位雲端服務資安政策。

2.雲端服務提供者及協力廠商須繕造人員名冊，不得有陸籍人士參與，並經保防部門安全查核合格後，得執行作業。

3.雲端服務提供者應確保租（運）用之資通訊產品（含軟體、硬體及服務）無陸製廠牌，並禁止資料存取、備份及備援之實體所在地位於大陸地區、香港或澳門，且不得跨該等境內傳輸相關資料（需提供證明文件及資產清冊）。

4.雲端服務提供者及協力廠商應依資通安全責任等級分級辦法及國防部所認定之資通系統安全等級，採行適當安全控制措施，以確保資通系統達到應具備之安全防護水準。

5.除考量資源配置時間、可用性及故障排除和業務回應時間外，並重視資安與個資保護、資料備份與復原、服務復原時間及服務中斷補償。

七、網站設置作業流程：

（一）軍網網站：由網站需求單位提出申請、通電資業務單位完成需求初審(含資安架構審查、網域名稱及網址分配等項)，經管理機關核定同意建置及通過資安檢測後，副知通次室及資通電軍，始正式上線(如附件二、三)。

（二）民網網站：由網站需求單位提出申請，訂定管理要點，由通電資業務單位完成需求初審及管理機關完成複審，經政辦室核定同意建置及通過資安檢測後，副知通次室及資通電軍，始正式上線(如附件四、五)。

（三）網站需求單位應每月完成網站伺服器自我檢查（如附件六、

七），管理機關應每年針對所屬單位軍、民網網站實施資安檢測及要求完成修正、複檢作業。

（四）網站（系統）如屬國防部或軍種統一規劃建置與配發，由規劃建置單位負責網站設置申請事宜。

八、考核與獎懲事項：

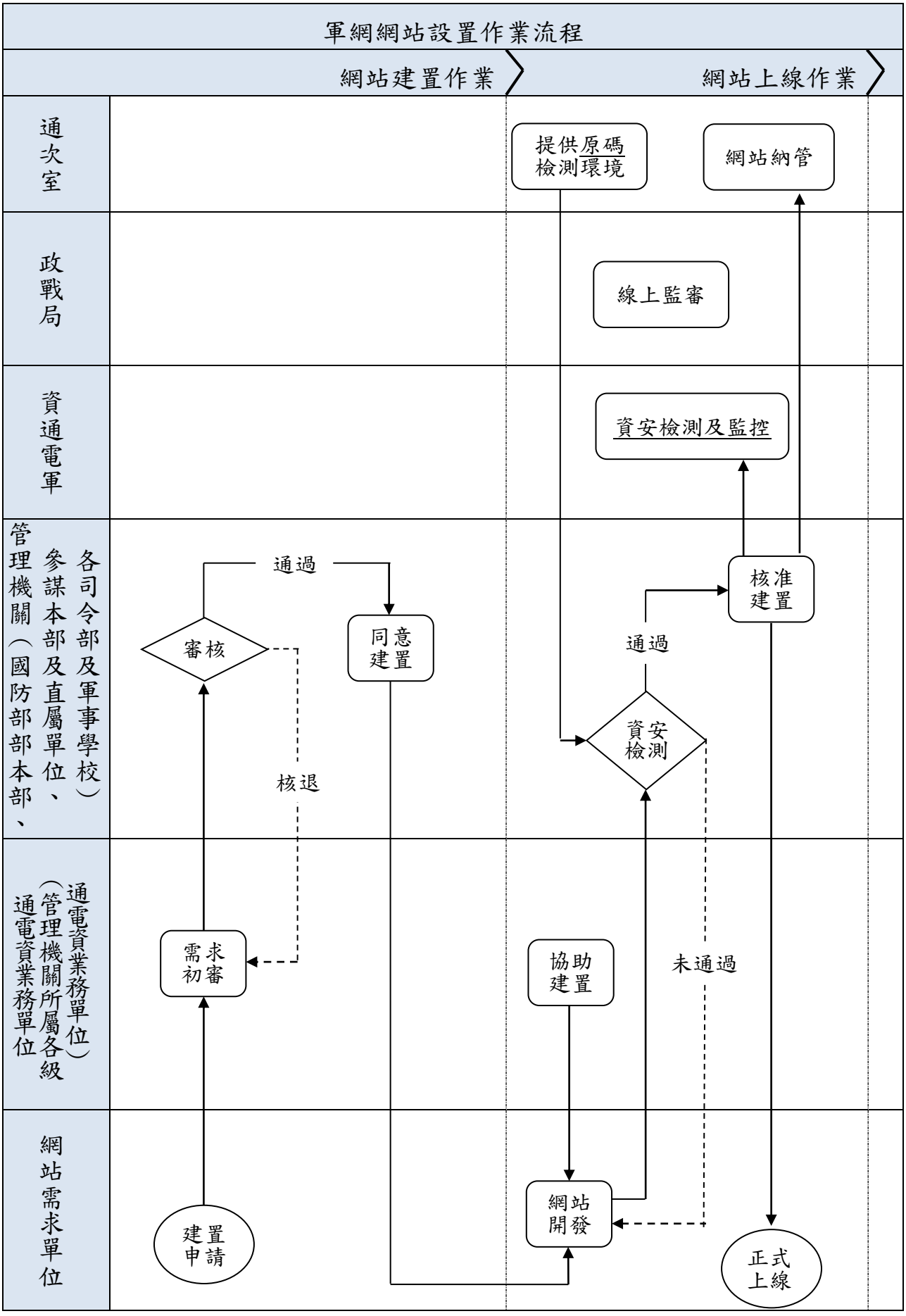
（一）管理機關應秉一級督（輔）導一級精神，對於所屬單位因作業管制不當，致肇生洩密或資安事件者，應主動派員查核，並要求檢討改善與追究違失人員責任；國防部將配合年度資通安全督（輔）訪時機考核。

（二）各單位因網站內容造成洩密事件者，視情節輕重，依陸海空軍懲罰法及國軍資通安全獎懲規定相關規定辦理懲處。

附件一：

(單位全銜)網站清冊(範例)										
網站編號	業管單位	網址	IP位置(網系)	網站名稱	維管人員	電話手機	憑證發行者	到期日	自我檢測結果	原碼檢測及弱點掃描
範例(新增)	司令部人軍處	lqsys.caf.mil.tw/login.aspx	10.28.X.X(軍網)	空軍休請假系統	王○○	234567	國軍憑證管理中心-G3	2025年1月6日	合格	1.原碼檢測112.2.11執行，無風險 2.弱點掃描113.6.1執行，低風險1，修正中
範例(撤站)	司令部	fpsceid.hq.caf.mil.tw	10.28.X.X(軍網)	文案宣導系統	姚○○	789456	國軍憑證管理中心-G3	2025年10月7日	不合格	1.原碼檢測112.10.11執行，無風險 2.弱點掃描113.10.1執行，低風險10，徹站
範例(既有)	政辦室	www.mnd.gov.tw	172.X.X.X(民網)	國防部全球資訊網	黃○○	632123	政府伺服器數位憑證管理中心-G1	2025年4月22日	合格	1.原碼檢測112.2.11執行，無風險 2.弱點掃描113.6.1執行，低風險1，修正中

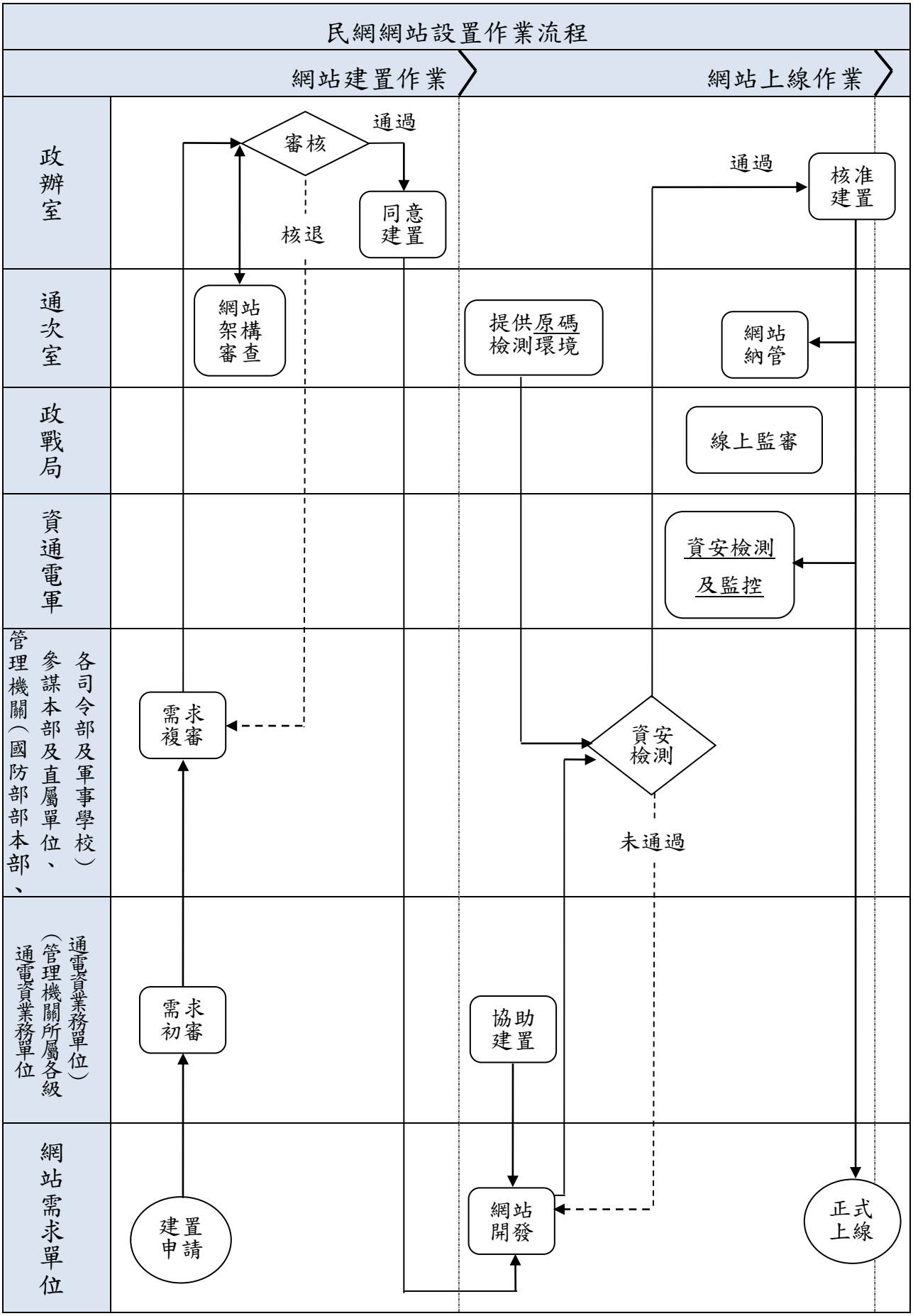
附件二：軍網網站設置作業流程



附件三：軍網網站設置申請表

（全銜）網站設置申請表	
申請單位：	
通電資業務單位承辦人：	聯絡電話：
網站名稱：	網域名稱：
網站防護架構：（請以附圖說明）	網址：
網站建置目的及用途：	
網站作業系統：	網站伺服器：
網頁程式：（如：ASP.NET C#、Java、PHP 等等）	
通電資業務單位審查與簽章：	
申請單位簽章	單位主官批示

附件四：民網網站設置作業流程



附件五：民網網站設置管理要點

（全銜）（網站名稱）設置管理要點

一、目的（說明本網站架設之原因）

二、權責劃分（含單位、協力廠商或雲端提供業者）

三、連線架構（含網站服務架構）

四、資料存放地點（含設備列表及備援）

五、雲端服務種類

六、雲端服務部署模型

七、雲端服務使用期限

八、雲端服務提供者資訊（含聲譽、可靠性、服務資訊透明度、所提供之資安強度、管理、經驗及背景）

九、雲端服務部署資安規劃內容

十、管理要點（視需求增減要項）

（一）通用原則（含限制條件）

（二）實體環境管理（如資訊機房、機櫃等）

（三）實體設備管理（連結專網之各項實體設備）

（四）網路連線管理（含資安防護系統等）

（五）網站管理（是否可支援 CDN 或 IPFS、管理者認證機制是否符合多因子認證並整合零信任架構）

（六）作業系統管理（含權限及網域政策等）

（七）作業機制管理（含資料交換、儲存等）

（八）維運管理（含系統維護、備援及督導稽核權責與週期等）

（九）資安事件處置流程（含事件應變及採證等相關作業）

十一、其他

（一）獎懲作法。

（二）聯絡資訊。

備註：網站如非屬雲端架構，無須填寫第五至九項。

附件六：網站伺服器自我檢查表

（全銜）網站伺服器自我檢查表				
項次	檢查項目	檢查結果		
		是	否	不適用
一	**開機及進入系統：** 1、伺服器作業系統登入時是否設定密碼 2、密碼設定是否符合複雜性需求	□ □	□ □	□ □
二	**桌面及螢幕保護裝置：** 1、桌面是否設置部頒「保密警語畫面」 2、螢幕保護裝置啟動時間是否設定三分鐘以內 3、螢幕保護裝置結束後，是否以密碼保護	□ □ □	□ □ □	□ □ □
三	**防毒軟體及漏洞修補：** 1、是否安裝防毒系統 2、病毒碼是否更新至最新版本 3、是否已完成系統安全漏洞修補及連接至軟體自動更新伺服器（WSUS）	□ □ □	□ □ □	□ □ □
四	**帳號密碼設定** 1、紀錄網站主機所有帳號（配合後續比對有無異常帳號） 2、密碼長度是否設定12字元以上 3、複雜性密碼原則是否設定 4、系統管理者密碼是否設定需1個月更換乙次 5、網頁維護者密碼是否設定需3個月更換乙次 6、輸入錯誤密碼3次後鎖定帳戶	□ □ □ □ □ □	□ □ □ □ □ □	□ □ □ □ □ □
五	**網路及本機安全性設定** 1、網路是否符合實體隔離政策規定 2、是否依開放服務設定存取規則（如Firewall Access Rule） 3、是否已設定本機稽核原則 4、非必要系統服務是否已關閉 5、非必要網路服務是否已關閉 6、是否紀錄自動排程程序(配合後續檢查是否有異常排程) 7、檢查有無異常自訂開機執行程序 8、是否開啟內建防火牆、設定管理連接埠允許來源IP位址及網頁服務頁面限制允許存取來源IP位址	□ □ □ □ □ □ □ □	□ □ □ □ □ □ □ □	□ □ □ □ □ □ □ □
六	**應用程式資訊安全檢查** 1、是否加入檢查HTML標記（Tag）輸入機制 2、是否加入防範資訊隱碼攻擊（SQL injection）程式 3、網站是否採用安全傳輸通訊協定（HTTPS）機制，以SSL/TLS加密傳輸	□ □ □	□ □ □	□ □ □
七	**政策訂定** 訂定網站上線實施計畫，內容應涵蓋：使用者帳號申請管制程序、每日檢查程序、定期備份程序、版本異動程序、定期弱點掃描程序	□	□	□

檢測人： 檢測日期：

附件七：雲端服務自我檢查表

（全銜）雲端服務自我檢查表					
類別	項次	檢查項目	檢查結果		
			是	否	不適用
基礎設施即服務 IaaS	一	是否確認雲端服務提供者提供相關保護機制（流量清洗、CDN)，以確保其虛擬機器不會受到其他租戶或來自網際網路攻擊？	□	□	□
	二	是否確認雲端服務提供者執行嚴謹之管理者登入控管，以安全存取虛擬系統資源？	□	□	□
	三	是否確認雲端服務提供者有針對虛擬伺服器定期進行資安掃描？	□	□	□
	四	確認雲端服務提供者在遭遇主系統服務中斷時，是否有備援方案，提供客戶於主系統服務中斷時的配套方案？	□	□	□
	五	雲端服務提供者是否有提供用戶技術與服務諮詢管道？	□	□	□
	六	是否確認雲端服務提供者有落實雲端資料安全？ 1、資料備份之一致性。 2、可靠之刪除機制。	□	□	□
平臺即服務 PaaS	一	是否確認雲端服務提供者有定期檢視應用、組件或Web 服務是否存在漏洞，並進行更新修補？	□	□	□
	二	是否確認雲端服務提供者使用標準程式語言與工具？所提供之資通系統基礎建設介面是否通用？	□	□	□
	三	是否有進行組件測試，確認在編譯階段之軟體函式庫與執行階段之呼叫函式皆符合預期，即具有預期之功能與功效？	□	□	□
	四	雲端服務提供者是否有提供用戶技術與服務諮詢管道？	□	□	□
	五	是否有確認 PaaS 應用程式可被設定具有資安功能(如專屬 VLAN 網段、在客戶端與伺服器間溝通時可加密訊息)，並能與機關既有資安框架進行整合 （如識別與認證功能）？	□	□	□
	六	雲端服務提供者是否保存資安事件追查所需之平臺、系統與網路等日誌資訊，並可依單位需求提供參考?	□	□	□
軟體即服務 SaaS	一	是否有訂定使用者管理政策？是否有落實該政策？	□	□	□
	二	是否確認關閉不必要之通訊埠與共用資料夾？	□	□	□
	三	是否確認雲端服務所使用之系統與應用程式，有定期進行資安掃描並修補被掃描出之弱點?	□	□	□
	四	是否有確認雲端服務有相關網路入侵防護、實體入侵防護、監測活動管理或防毒機制?	□	□	□
	五	是否有強化使用者設備與應用程式保護，如Web瀏覽器之安全防護？	□	□	□
	六	是否有建立加密機制，如網際網路資料傳輸加密、資料儲存加密等？	□	□	□
	七	雲端服務提供者是否有提供技術與服務諮詢管道？	□	□	□
	八	是否有要求雲端服務提供者提供可靠之資料備份機制，以利需要或刪除時確實復原所有儲存資料？	□	□	□

檢測人： 檢測日期：