

法規名稱：

國軍網路管理作業規定 (民國 114 年 09 月 16 日修正)

1

一、為有效規範國軍網路管理程序，落實網段與網路管理作為，律定管理權責及作業流程，確保國軍網路服務品質，提升網路安全防護強度，特訂定本規定。

2 ④

二、本規定用詞，定義如下：

- (一) 國軍網路：指使用 TCP/IP 網路通信協定標準建構於國軍骨幹網路上之網路總稱（示意圖如附件一）。
- (二) 網際網路：指使用 TCP/IP 網路通信協定標準建構於固網業者骨幹網路上之網路總稱（示意圖同附件一）。
- (三) 行動網路：以行動設備（如智慧型手機或平板電腦）透過通訊基地臺訊號連接到網際網路的無線網路。
- (四) 無線區域網路：不使用任何導線或傳輸電纜連接區域網路，符合 IEEE802.11 標準均屬之。
- (五) 網路註冊中心：國軍最頂層網路註冊單位，負責國軍網路之網段、網址規劃、註冊與管理。
- (六) 軍網行政網 (MINET)：指國軍網路內，提供國軍人員密級行政作業之網路環境。
- (七) 軍網專屬網路（以下簡稱專網）：指國軍骨幹網路內所有自主運作之專用網路，如指管網、戰情網及捷訊網等，網系機密等級由各管理單位定之。
- (八) 第一級註冊中心：負責軍（專）網規劃、註冊與管理，並向國軍網路註冊中心申請網段。
- (九) 網路位址（以下簡稱網址或 IP）：指節點設備於國軍網路上之位址，任一網址均具唯一性。
- (十) 軍租軍網：委民間固網公司籌建之專用資訊網路。
- (十一) 國軍營區網路管理系統（以下簡稱 BNS）：指國軍用以管理（控）營區內網路動態之資訊系統。
- (十二) 國軍網段管理系統（以下簡稱 MWHOIS）：國軍用以管理軍（專）網網段資源之資訊系統。
- (十三) 民網行政網（單一閘口）：指國軍連結政府網際服務網（以下簡稱 GSN）用以行政作業之民網環境。
- (十四) 專線民網（非單一閘口民網）：指因特殊目的連結網際網路服務未納入 GSN 管控之民網環境。
- (十五) 網段：指各級註冊中心合法註冊使用網路位址範圍。
- (十六) 第二級註冊中心：依需求向第一級註冊中心申請網段，並負責授權網段規劃、註冊與管理。
- (十七) 國軍骨幹網路：指國軍自建之地面骨幹通信系統，為國軍各專案網路運作的通資基礎平臺。
- (十八) 動態主機組態協定（以下簡稱 DHCP）：指將所屬網段資源，依註冊之合法使用者配發可使用之 IP。
- (十九) 網卡號碼（以下簡稱 MAC）：指由十二個十六位元編碼組成，作為網路封包傳輸之實體位址。
- (二十) 網路拓撲：指網路連結示意圖。
- (二十一) 軍事院校學術網路（以下簡稱學網）：指軍事院校使用教育部

及國內大學共同建立可連結網際網路之校園網路，以為教學研究用途。

- (二十二) 國軍醫院醫療網路：指國軍醫院向固網公司申租專用電路，建置可連結網際網路之醫療網路。
- (二十三) 網域名稱解析系統（以下簡稱 DNS）：指提供網域名稱解析為網路位址（IP）之資訊系統（服務）。
- (二十四) 臺灣戰術網路（以下簡稱 TTN）：指建構於網際網路雲端環境，屬密級之高存活度戰術網路。
- (二十五) 內容重組淨化（CDR）：檢查資料是否有惡意程式（內容），並實施內容重組及淨化清理程序。
- (二十六) 資料防洩漏（DLP）：執行檔案資料格式檢查及敏感字眼偵測機制，避免機敏資料外洩。

3

三、適用範圍：

- (一) 國軍使用網路通信協定標準（TCP/IP），以有線方式連結國軍網路之通資軟硬體設備、武器裝備、單位。
- (二) 國軍使用行動通訊電路，以行動網路連接國軍網路或獨立網路之通資軟硬體設備、武器裝備、單位。
- (三) 國軍使用無線區域網路（Wi-Fi，符合通信協定標準（IEEE802.11 a/b/g/n/ac/ax/be或以上），以無線區域網路方式執行國軍任務之通資軟硬體設備、武器裝備、單位。

4

四、權責區分：

- (一) 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. 負責國軍網路、無線區域網路及相關軟、硬體設備管理政策與制度之規劃、修訂、督導及考核。
 - 2. 兼任國軍網路註冊中心，負責國軍網路（軍、專、民網）申用審查與網路資源核配。
 - 3. 軍網第一級註冊中心，負責軍網發展規劃、資源分配及資安管理。
 - 4. 負責國防部幕僚單位網址規劃、指派與管制。
 - 5. 負責軍租軍網審核、申租與督管。
 - 6. 負責 BNS 及 MWHOIS 發展、部署與管理。
 - 7. 負責國防部民網行政網維運與管理。
 - 8. 負責全軍專線民網、行動網路及無線區域網路申請審查及國防部幕僚單位申請審核。
 - 9. 負責國防部博愛、衡山營區及各網路交換中心軍、民網資訊（安）設備部署與管理。
- (二) 各司令部、國防部直屬機關（構）、軍事學校及參謀本部直屬機構、部隊（以下簡稱各管理機關）：
 - 1. 依任務特性擔任專網第一級註冊單位，負責專屬網段管理。
 - 2. 依第二級註冊中心權責，負責軍（專）網所屬網段管理。
 - 3. 負責所屬單位軍租軍網、無線區域網路及行動網路申請、管理與稽核。
 - 4. 負責所屬營區網路管理制度訂頒及業管系統維運，並協助所屬單位系統維運、管理與稽核。
 - 5. 負責業管及所屬網路資源規劃、分派、稽核與技術支援。
 - 6. 負責所屬民網行政網維運與管理。

7. 負責所屬單位專線民網申請審查與轉呈。
8. 協助所屬單位資訊（安）網路設備建置、籌獲、部署、維運、管理與教育訓練。

（三）使用單位

1. 依網址需求單位權責，負責核配之網段管理。
2. 負責所屬資訊設備之登錄、IP 申請、異動管理作業。
3. 負責軍租軍網電路申租（註銷）及設備管理（繳回）。
4. 負責所屬 BNS 及無線區域網路維管與稽核。
5. 所屬網路實體環境、存取規則及資訊（安）設備管理及維運。

（四）國防部資通電軍指揮部（以下簡稱資通電軍）

1. 負責國軍骨幹網路管理與維護。
2. 負責軍網廣域路由維管及網路系統資料校對。
3. 配合網路攻防演練，協助驗證各單位執行成效。
4. 負責用戶端國軍網路連結可行性評估。
5. 監控各網路交換中心與軍租軍網設備連接介面，並提供故障排除技術支援。
6. 技術協助各單位將資訊（安）系統（設備）事件紀錄導向國軍資安防護中心，並納入監控與分析。
7. 負責執行軍網行政網營區網路管理系統阻斷驗測作業。

5 ④

五、國軍網路網段管理：

國軍網路註冊架構分為國軍網路註冊中心、第一級註冊中心、第二級註冊中心及網址需求單位四類（如附件二），作業權責如下：

（一）國軍網路註冊中心

1. 受理第一級註冊中心網段申請，並依需求、區域、軍種、系統機敏性原則配發網段。
2. 建置 MWHOIS，並依所配發之網段，完成登錄及管制。

（二）第一級註冊中心

1. 受理第二級註冊中心、網址需求單位網段申請，並依需求、區域、軍種配發或指派網段。
2. 依所配發或指派之網段，專網須完成網段使用單位分配表，國軍網路須於 MWHOIS 完成登錄及管制。
3. 依實需將網段管理下授第二級註冊中心配合執行。

（三）第二級註冊中心

1. 受理網址需求單位網段申請，並依需求、區域配發或指派網段。
2. 依所配發或指派之網段，專網須完成網段使用單位分配表，國軍網路須於 MWHOIS 完成登錄及管制。

（四）網址需求單位

1. 依服務性質或需求目的配發網址，配發方式須使用動態主機組態協定（以下簡稱 DHCP）服務或以軟、硬體管控限制使用者自行設定 IP，同時建立網址與使用人員（席位）對應及查察機制。
2. 採用之網路設備須具有網管功能以可納入營區網路管理系統管控為原則，並可設定交換埠使用限制，連網終端設備（如個人電腦及印表機）必須強制定 IP 與 MAC，以防制使用者私自竄改 IP。
3. 建立網路 IP、MAC 監控系統，須可主動偵知未經授權 IP 及 MAC 連線，並達到自動告警、阻斷機制。

六、國軍網路管理

（一）一般原則

1. 各單位區域性網路所需網址，應就整體連網作業所需範圍規劃後，向上級註冊單位申請。
2. 伺服器與用戶端設備須各自配發網段，俾利運用防火牆規則進行有效防護。
3. 單位因組織重整或營區位置調整，原配發網址應繳回原配發單位，後續依所在駐地位置，重新向國防部或各司令部申請配發新網段。
4. 機動部隊與艦艇等單位所需使用動態網址，應檢附單位網址規劃需求及網路架構報部審查及申請配發。
5. 國軍網路內嚴禁使用網址轉換（Network Address Translation，以下簡稱 NAT）方式作業，因任務須採 NAT 方式連網時，應檢附網路架構及網址管控、查核機制報部核定。
6. 各項演訓任務臨時性網址，各軍種仍依前五點之規定，依分配之戰演訓網段自行配發，不足部分另向國防部申辦。
7. 重要伺服器（目錄服務、檔案、對外服務網站等）及開通可連接移動式儲存媒體之電腦（含資料交換電腦），須安裝國軍駭侵主動防禦系統端點防護軟體，管理原則同民（學）網。

（二）網段（址）配發原則

1. 網址規劃以路由集聚（Aggregation）為目標，與地理位置、網路節點及管理需求密切結合，兼顧現況及未來成長適當辦理配發。
2. 軍（專）網網址均以 10.x.x.x（Class A）網段訂定，以一組 Class C 網段為基本配發單位。
3. 第二碼係依據作戰區、駐地、國軍光纖站臺與特殊用途為分配基礎，將全國劃分為臺北特區、臺北、桃園、臺中、臺南、高雄、花蓮、專網等八大網段，由第一級註冊中心依第二級註冊中心需求、編制大小及作業所在地，以連續網址寬放為原則，預劃分配未來可用範圍；第三碼由第二級註冊中心考量網址需求單位駐地位置、連網主機數量（如附件三）配發適量網段。
4. 網址規劃分配應運用子網段分割技術，達到網址之有效利用及分隔功能。
5. 非屬第二級註冊中心配發者，一律向第一級註冊中心申請。

（三）網段（址）申請流程

1. 申請作業
 - （1）辦理國軍網路網段（址）申請作業，應檢附網路位址需求規劃書（如附件四）函送上層註冊中心核定後配發。
 - （2）辦理專網網段（址）申請作業，須擬訂管理要點（如附件五），國防部幕僚單位函送通次室審查後，簽奉副總長以上長官核定；非國防部幕僚單位函送通次室審查後，由管理機關自行核定，並副知通次室備查。
 - （3）註冊中心負責將申請單位相關資料建置於 MWHOIS。
 - （4）各級註冊中心網段不足時，應向上層註冊中心申請調增，上層註冊中心完成審核後，配發新增網段。
 - （5）需求單位申請網段，各註冊中心依權責核復時，應副知資通電軍辦理廣域網路路由調整；資通電軍每月五日傳報上月路由異

動資料予通次室管制。

- (6) 各級註冊中心須律定 MWHOIS 管理人員一員，人員職務異動時，應即通報國防部系統管理員，俾利權限設定及管控。

2. 異動與撤銷作業

- (1) 各單位因故須異動或撤銷現用網段或網址者，應行文上層註冊中心並辦理 MWHOIS 異動。
- (2) 各單位有過多零散不連續網址，可向上層註冊中心申請轉換為一組連續網址，並繳回舊網址。

七、軍租軍網管理

(一) 申裝原則

1. 為落實資源有效運用，各單位申請連接軍網，以國軍網路為優先考量，單一營區不得同時申用軍租軍網及國軍網路。
2. 共駐營區單位申請軍租軍網以核配一路為原則，由共駐營區主管單位或網路節點較多單位，構建網路次節點收容，資訊安全設定與管理由使用單位負責。
3. 單位辦理軍租軍網新增、異動及註銷作業，統一呈報各管理機關初審後，轉通次室審核，不得逕向固網公司臨櫃申辦。
4. 各使用單位因任務需要申辦短期（演訓）軍租軍網使用，由各管理機關自籌經費並彙整電路需求，於三週前逕向通次室提出申請，俾利網路架設施工遂行。
5. 遇原有電路無法升速或頻寬已達飽和等特殊狀況，申請單位得不受申裝原則限制，惟須檢附網路拓樸及網段規劃等相關文件，函送通次室核配。
6. 各單位申辦之電路，不得附掛語音電路，並由單位自行編列預算支付。

(二) 設備管理原則

1. 軍租軍網為國軍租用專屬環境，中繼骨幹電路與設備建置於固網公司資訊機房，與網際網路實體隔離，固網公司負責硬體設備保管。
2. 軍租軍網介接軍網之區域骨幹網路設備，係與固網公司租用，建置於資通電軍北、中、南部網路交換中心，由資通電軍各網路交換中心負責硬體設備代管，依專網專用原則以專用設備及電路與國軍專、民網隔離，且其連接之資訊設備均不得跨網系混接。
3. 數據機、路由器等軍租軍網終端連網硬體設備須黏貼識別標籤（如附件六），由各租用單位（或管制區）上鎖保管，長期或短期（演訓）租用均須納入 BNS 管控；電路註銷時，設備歸還固網公司，租用期間設備遺失，由租用單位賠償。
4. 通次室建置軍租軍網設備遠端連線認證管理平臺，限定系統登入之 IP、帳號及權限，平日維持停用狀態，租用單位報修期間，視固網公司查修需求啟動。

(三) 組態管理原則

1. 系統組態、遠端（VTY）及本地端（Console）帳密設定，統由通次室提供構型設定。
2. 固網公司負責中繼骨幹電路設備之電路路由設定，資通電軍負責區域路由設備介接軍網之廣域路由設定，通次室負責終端路由設備之軍網路由設定。

3. 固網公司針對國防部租用之網路設備（區域路由設備、終端路由設備）僅具組態瀏覽權限，路由、組態及帳密設定異動作業，統由通次室提供。

（四）軍租軍網租用單位及固網公司稽核原則

1. 固網公司參與軍租軍網管理人員，須經國防部安全查核合格後，方得執行管理作業。
2. 固網公司須管制機房人員進出紀錄，並指派專人定期檢查稽核紀錄及系統運作情形，資料保存一年備查。
3. 通次室定期對軍租軍網租用單位及固網公司機房實施現地稽核。（稽核表如附件七）

（五）資料管理原則

1. 各管理機關建立所屬軍租軍網使用單位電路總表（如附件八），每半年校正資料一次，清校結果於六月三十日及十二月三十一日前不備文通次室備查。
2. 通次室綜整各管理機關申辦紀錄與固網公司核校電路實際使用動態。

（六）申請作業

1. 申請作業依任務需求區分為長期及短期（演訓）電路申請，均於三週前由各管理機關彙整連網需求後，檢附申請表（如附件九）函送通次室審查。
2. 通次室審核通過後，通知固網公司協助使用單位辦理裝設作業（申請流程圖如附件十）。
3. 申請電路不論長、短期程，均應於任務完成後，辦理註銷作業；申請、異動及註銷作業應填具申請表（同附件九）辦理。
4. 各使用單位申請提升頻寬或增加網段時，應檢附網路拓模圖，呈報各管理機關辦理初審後，函送通次室審核。

（七）異動與註銷作業

1. 使用單位執行營區搬遷、基地演訓或組織調整時，呈報各管理機關轉通次室，辦理移機、網段重新核配及組態調整等事宜；申請表（同附件九）內異動區分欄填註代碼為 U。
2. 使用單位組織調整（單位合併、裁撤等因素）時，造成軍租軍網與國軍網路並存情形，依實際環境、線路品質擇優使用，呈報各管理機關，轉通次室辦理註銷；申請表（如附件九）內異動區分欄填註代碼為 D。

（八）故障處理

1. 使用單位遇網路阻通時，逕向固網公司報修，報修時提供電路編號、阻通概況、報修人員姓名及聯絡電話（民線或手機），以利固網公司聯繫相關行政事宜；另逐級回報，並由管理機關副知通次室（業管軍線：635942），俾逐級管制修復進度。
2. 固網公司查修作業須登入網路設備調整組態時，由通次室啟動管理平臺供遠端連線，並提供平臺及網路設備登入帳密。
3. 除障作業完成後，由報修單位偕檢修人員完成連線及速率檢測，將測試結果回覆通次室，由通次室檢查組態設定，並修正密碼後，始同意固網公司報請竣工。

國軍網路依據資訊服務資源與存取行為，劃分網路分級管理原則如下：

1. 網路 IP 網段，依資源服務分為公務電腦網段與資訊伺服器網段兩類，再依作業性質，區分為一般、限制、系統管理不同等級網段，分級概念及存取規則說明如下（概念圖及規則表如附件十一）：

- (1) 公務電腦網段：作業人員使用之公務電腦及週邊設備網段，公務電腦對資訊伺服器存取授權資訊服務，依據作業性質細分一般及限定資訊網段，執行分級管控，區分如下：
 - a. 一般公務電腦網段：收容一般行政公務電腦、印表機等設備，僅允許存取一般伺服器資訊服務。
 - b. 限制用途電腦網段：收容機敏辦公處所或重要戰備場所公務電腦、印表機等設備，允許存取機敏伺服器資訊服務，及有條件存取一般伺服器資訊服務。
- (2) 資訊伺服器網段為提供資訊服務之網路區段，依據資產與任務重要性，建立不同安全等級伺服器區域，接受合法公務電腦網段與其他伺服器區之存取服務要求；資訊服務安全等級愈高，存取條件愈嚴格，依其作業性質區分如下：
 - a. 一般性服務網段：收容機敏等級較低之通用性資訊服務（如入口網站、網域名稱伺服器、網頁式郵件系統等），採簡易身份、密碼認證，提供一般伺服器資訊服務。
 - b. 限制性服務網段：收容機敏、戰備資訊服務（如戰演訓系統、資料庫管理系統等），允許存取限定伺服器資訊服務，及有條件存取一般伺服器資訊服務。
 - c. 系統管理網段：收容網路管理、系統效能監控管理等專網、伺服器設備或具特殊性用途，不開放外部存取之專屬性服務（如網管系統、機房環控系統、機房伺服器監控系統、高級主官在營燈系統、無線區域網路防護系統等），允許對各網段執行條件式存取。
2. 營區網路依分級原則建立安全存取等級，管理單位建立網路存取控制（Access Control）機制，同時部署存取端（Access）至骨幹端（Core）存取過濾機制。
3. 網路存取規則應依網路分級存取規則表，於具資訊安全防護功能設備（如防火牆、具第三層功能以上之網路設備等）以正向表列方式定義資訊服務存取對象。

（二）網路實體架構原則

1. 國軍網路專用設備及電路須依「專網專用」原則相互隔離，網系內資訊資產（含機櫃、主機、線路、網路設備及儲存設備等）均不得跨網系混接，並依實況建立網路邏輯及實體架構圖，適時修訂。
2. 營區網路由多個交換器（Switch）以階層式拓樸部署，底層採效能及背板頻寬較次等之網路設備，收容終端節點，再由效能較佳之交換器收容至較高速之上層網路，架構以三層以下為原則。
3. 營區網路建置採取乙太網路（Ethernet）架構，主幹與中繼採取 1000/100Mbps 以上速率、用戶收容以 100Mbps 以上為主。
4. 網路交換器應支援簡單網路管理協定（SNMP）、終端機管理協定（SSH），現存不具網管功能之交換器（或集線器）應排定時程

檢討汰換，網路交換器須以可納入 BNS 管控為原則。

5. 連結國軍網路資訊設備應設定主機名稱 (Hostname)，合法提供連網服務之應用伺服器，應申請完全領域名稱 (Full Quality Domain Name, FQDN)，命名原則參考附件十二。
6. 網路線材以顏色為識別 (顏色區別參照國防部頒國軍資訊資產管理作業規定，既有線路頭尾端以張貼不同色系區別網系)，每一線路均依編碼原則標示線路起訖端，以利識別管理。

(三) BNS 管理原則

1. 單位 DHCP 伺服器、具網管功能路由器、交換器均應納入 BNS 管控，並完成相關設定。
2. 單位所屬目錄 (Active Directory, AD) 伺服器應整合 BNSAD GPO 程式，以利掌握使用者及 IP 使用軌跡。
3. 單位應檢討伺服器 (主機) 建置網路位址偵測 (Address Resolution Protocol, ARP) 輔助工具，並管控所屬網段。
4. 伺服器、個人電腦、網路印表機、網路監視器等資訊設備連結軍網行政網，須於資訊資產管理系統完成帳籍登載後，再至 BNS 完成 IP、MAC、使用單位、使用者、連結之交換器及埠口等相關資料註冊；未經註冊之設備連結軍網行政網，系統將自動阻斷違規設備 IP 及關閉該交換器連結埠，並通報國軍電腦緊急應變中心 (以下簡稱 MCERT)。
5. 各單位應落實軍網行政網交換器及網段納管，每月自行實施網路節點阻斷驗測，由資通電軍排定受測單位，赴現地實施阻斷驗測，並於每月將驗測結果提供通次室，驗測失敗單位應於次月成功復測，復測失敗則納入定期會議檢討。
6. 主網路管理系統提供虛擬帳籍建置功能，主要為提供虛擬區域網路 (Virtual Local Area Network, VLAN)、伺服器第二張以上網卡及其他無法納入資訊資產系統管理之特殊情況使用，應納入資產系統管理設備，採臨時帳籍建立時，以不超過九十天為原則，逾期使用予以自動註銷及阻斷；另各管制單位應每半年清校虛擬帳籍清冊，提供通次室備查。
7. 共駐營區系統部署於最高指揮單位為原則，並為初級管制單位，共駐單位肇生違規事件，由初級管制單位至 MCERT 網站實施初報以釐清責任，續由肇事單位依指揮系統逐級向上回報、管辦。
8. 各級單位應落實系統監控機制，對網路違規、交換器或網路位址偵測輔助工具離線等情事，應依程序主動查察、回報、記錄並恢復系統功能 (流程圖如附件十三)。
9. 偏遠獨立單位營區及軍租軍網單位 BNS 納管原則，應依一級督導一級權責或協調鄰近單位收容。

(四) 營區網路管理執行作法

1. 網段權限指派
 - (1) 本部規劃各司令部及其所屬單位使用網段，完成路由設定，並於 MWHOIS 賦予網段管理權限。
 - (2) 各司令部依據國防部配發之網段，於 MWHOIS 指派所屬單位使用網段，並指定其所屬 BNS 設定權限。
 - (3) MWHOIS 資訊應依據現況適時更新，確保資料正確。
 - (4) 資通電軍定時檢視、維護管理廣域路由表 (含無效路由刪除)，並協助路由資料回饋資訊系統管控；本部將利用年度各項督

檢時機稽核執行成效，俾確維網路傳輸安全。

2. 資訊設備申請連結軍網行政網

- (1) 常態連結軍網行政網設備，於資訊資產管理系統完成帳籍登載後，可逕至 BNS 完成註冊（不需填寫申請單），未完成相關設定前，設備不得連接網路線。
- (2) 臨時連結軍網行政網之設備，於資訊資產管理系統完成帳籍登載後，申請單位應填寫連接軍網行政網設備 IP 申請單（如附件十四），由中校以上權責主官（管）核准，經資訊業管部門於 BNS 完成 IP、MAC 註冊及設備種類等設定，申請單統由資訊業管部門存管，紙本保存一年後銷毀。
- (3) 確認申請之資訊設備已完成系統設定，設備始可自動取得 IP 連結軍網行政網。
- (4) 無法自動取得 IP 資訊設備，依配賦之 IP 組態紀錄，以人工手動方式設定，設備始可連結軍網行政網。

3. 軍網行政網設備資料異動

- (1) 申請異動之資訊設備先行離線，資訊業管人員於 BNS 完成 IP、MAC 或交換器異動設定。
- (2) 確認異動之設備於系統完成設定後，始可連結軍網行政網重新自動取得 IP；無法自動取得 IP 之設備，得以人工手動方式設定連結軍網行政網。
- (3) 資訊設備 IP、MAC 及使用位置不變，惟使用者因職務異動，資訊業管人員僅須至 BNS 完成使用（保管）人異動變更。

4. BNS 帳號管理與事件處置

- (1) 系統管理帳號（申請表如附件十五）應登錄授權管理之網段、網路設備、網路位址輔助偵測器及申請之 IP 位址，以落實各項網路資源管理。
- (2) 私自將未經核定資訊設備連結軍網行政網遭系統偵測、阻斷，且違規紀錄回傳 MCERT，資訊業管部門應依國軍資安事件通報應變指導要點完成稽查，及依國軍資通安全獎懲規定檢討相關責任議處，並於一個月內辦理結案。
- (3) 合法設備因系統設定錯誤連結軍網行政網遭系統偵測、阻斷，且紀錄回傳 MCERT，使用單位檢附佐證資料，由資訊業管部門完成系統修正，一個月內辦理結案。
- (4) 合法設備因系統設定錯誤連結軍網行政網遭系統偵測、阻斷，無紀錄回傳 MCERT 者，由單位資訊業管部門自行管制完成系統修正。
- (5) 單位應定期執行系統阻斷功能驗測（交換器、ARP），有系統異常應儘速修復。
- (6) 各項異常事件均由資訊業管部門記錄備查，以為後續稽核、追蹤之依據。
- (7) 非經奉核調整系統設定（如交換器設定透通模式或停用），致系統偵掃、阻斷功能異常，將依相關規定究責議處。

九、民網管理

（一）設置原則

1. 各級單位建置民網設備須與國軍網路實體隔離，並優先考量收容至國防部或業管軍種司令部（指揮部）單一閘口管控，收容原則

如下：

- (1) 國防部單一閘口統一收容各幕僚單位及直屬機關、單位（業務機關）民網設備。
 - (2) 軍種司令部、國防部本部及參謀本部各直屬機關（構）、部隊設置單一閘口收容所屬單位民網設備，並研擬管理要點（含資安管控）呈報國防部核定。
 - (3) 設置場所以開放場所、集中收容為原則，並指定專人管理；國防部副處長級以上長官及司、局、次長以上長官秘書（隨員）室，得設置連網節點，由單位保密督導官管制稽核，餘均不得於個人辦公處所設置民網設備；各司令部長官辦公室與秘書（隨員）室，由各司令部自行管制。
 - (4) 戰演訓輪值或專案辦公室等機敏處所需設置民網電腦，須由任務需求單位或場域管用單位擬訂相關資安管控作為，國防部幕僚單位函送通次室簽奉副總長以上長官核可後設置；非國防部幕僚單位簽奉業管理機關核定後設置，並副知通次室備查。
 - (5) 新增民網單一閘口網路節點，國防部幕僚單位須填具連接民網設備 IP 申請單（如附件十四），由編階少將以上主官（管）初審同意後，函送通次室審復辦理，設備新增、線路佈設及相關費用，由需求單位負責；非國防部幕僚單位須向各單一閘口業管軍種司令部（指揮部）提出申請，並於核定後設置。
2. 因特殊因素（如任務需求、GSN 線路無法到達等）需以單一閘口以外方式連接民網（專線民網、TANET 學術網路及醫療網路等），須擬訂管理要點，國防部幕僚單位函送通次室審查後，簽奉副總長以上長官核可；非國防部幕僚單位函送通次室審查後，由管理機關自行核可，並副知通次室備查。

（二）管理原則

1. 民網專用設備及電路須依專網專用原則隔離建置，機櫃、主機、線路、網路設備及儲存設備等資訊資產均不得以任何型式與國軍網路（混（搭）接，且不得處理機敏公務。
2. 主機名稱（Hostname）規則同軍網行政網電腦，並納入網域管控，未經國防部核定，.mil 網域嚴禁私自部署伺服器主機或提供資訊系統服務；非閘口或專線民網因考量未建置網域管理者，應建立電腦管制清冊。
3. 網域名稱解析優先（Primary）導向本部 DNS（163.29.148.[10、12]），次要（Secondary）導向單位內部 DNS。
4. 應啟用帳號登入，帳號區分管理者及一般使用者權限，管理者帳號僅供資訊管理員使用，一般使用者帳號僅供瀏覽民網資料使用，以一人核配一帳號為原則，不得共用帳號；因專案任務需求，得向單位主官及資安長申用專案帳號，僅供一般使用者權限，且專人核配專用帳號；另均應設定開機保密警語。
5. 使用合法授權之作業軟體，並安裝資安防護系統，並定期更新作業系統及修補程式（含病毒碼）；國軍發展之公務軟體，未經國防部業管單位核定，嚴禁於民網電腦安裝使用。
6. 限制連線服務（如下載軟體、不良網站、垃圾郵件等），並嚴禁瀏覽色情、暴力、違反善良風俗等不當網站；瀏覽器歷程記錄，保留天數應設定一百八十天以上。
7. 各單位定期清校行政民網及專線民網使用情形，完成民網電路（

如附件十六)調查統計,當年度十二月三十一日前提供通次室備查。

8.配合部署國軍駭侵主動防禦系統網路流量及端點等二套防護暨鑑識系統,說明如下:

(1)部署範圍:

- a.網路流量:建置民(學)網閘口,並將上述區域伺服器及使用者區域所有流量導入。
- b.端點:重要目標伺服器(目錄服務、檔案、對外服務網站等)及電腦。

(2)資通電軍負責監控與分析各單位網路流量與端點防護暨鑑識系統執行狀況,每日執行相關分析與端點防護軟體安裝管制情形記錄備查,發現異常行為立即執行分析,並依國軍資安事件通報應變指導要點執行通報、管制與查處作業。

(3)各單位負責監控與分析單位內網路流量與端點防護暨鑑識系統,並管制端點防護軟體安裝狀況,每日執行相關分析與端點防護軟體安裝管制情形記錄備查,發現異常行為立即執行分析,並依國軍資安事件通報應變指導要點執行通報、管制與查處作業。

(4)資通電軍負責編列監控範圍所需端點防護軟體作業維持費及後續擴大部署建置費用。

(5)國防部由資通電軍負責監控與分析。

(6)各案件均統由資安鑑識實驗室追蹤與管制。

10

十、行動網路管理

(一)設置原則

- 1.因任務特性,臨時指揮所、部隊進駐機動戰術位置、專案實驗室等外點臨時場域,得申請行動通訊電路,連接所需網路。
- 2.固定營區原則不開放申請行動通訊電路,維持固接有線網路連接國軍網路。

(二)安全防護原則

1.以行動網路連接軍網行政網或專屬網路

(1)行動裝置端:須以專用行動裝置透由專屬行動數據虛擬私有網路(Mobile Data Virtual Private Network,簡稱 MDVPN)構連電信業者基地臺。

(2)行動載臺端:須以專用行動路由器透由專屬 MDVPN 構連電信業者基地臺,相關連網裝置採有線方式與行動路由器連接。

(3)營區端:連接軍網行政網或專屬網路電路,須採與網際網路實體隔離之虛擬私有網路(Virtual Private Network,以下簡稱 VPN)專屬電路。

(4)行動裝置及營區間,須以國安局認證保密器,完成加密連線後始可使用。

(5)營區端須搭配應用層防火牆進行流量管控。

2.以行動網路建構獨立網路

(1)行動裝置端:須以專用行動裝置透由專屬 MDVPN 構連電信業者基地臺。

(2)行動載臺端:須以專用行動路由器透由專屬 MDVPN 構連電信業者基地臺,相關連網裝置採有線方式與行動路由器連接。

- (3) 營區端：若涉及機敏，須採與網際網路實體隔離之 VPN 專屬電路。
- (4) 若涉及機敏資訊傳遞，則行動裝置、載臺及營區間，須以國安局認證保密器，完成加密連線後始可使用。
- (7) 未涉及機敏資訊傳遞，則行動裝置及營區間，則行動裝置、載臺及營區間，採一般 VPN 專屬電路，得以商用加密機制（符合 FIPS140-2 等級 3 以上，其加解密方式為金鑰長度 256 位元以上之 AES 演算法）執行傳輸作業。
- (5) 服務端及營區端須搭配應用層防火牆進行流量管控。

(三) 管理作法

- 1. 申用行動網路須擬訂管理要點（如附件五），由管理機關呈報國防部審核後始可申請，未奉核定嚴禁私自申裝。
- 2. SIM 卡、行動裝置及行動路由器須由專人保管，每日辦理網路連線通聯測試、SIM 卡與設備清點，並記錄備查。
- 3. 使用單位須建置裝置管控及使用者認證機制，以驗證設備與使用者身分有無遭偽冒，並每月定期重新檢視設備及使用者清單是否有未經授權使用狀況。
- 4. 行動裝置端須安裝行動裝置管控軟體，並以集控方式管控 SIM 卡之存取端點名稱、全球定位系統（Global Positioning System，以下簡稱 GPS）、相機、藍芽、熱點分享及無線區域網路，GPS 及相機得因任務需求經單位資安長同意後啟用，其餘功能不得使用。

十一、無線區域網路管理

(一) 設置原則

- 1. 臨時場域（如臨時指揮所、部隊進駐機動戰術位置、專案實驗室等外點場域）因任務特性，得因實需申請設置無線區域網路。
- 2. 固定營區因專案任務（如醫療需求、學術教學等）得申請使用無線區域網路，餘維持固接有線網路連接國軍網路。
- 3. 申請建置無線區域網路，以具備資安官及保防官（或政戰官）編階上校以上主官之單位，得提出設置申請；申用單位須擬訂管理要點（如附件五），並檢附自我檢查表（如附件十七），審核後始可建置使用，未奉核定嚴禁私自架裝，審核權責如後：
- (1) 與國軍網路連接：統由管理機關呈報國防部審核。
- (2) 未與國軍網路連接：統由管理機關檢送通次室審復後自行核定。
- 4. 使用學術網路之軍事院校開放無線區域網路，適用範圍以無線訊號涵蓋區域未設置軍、專網節點之教室、實驗室、圖書館、展覽間、休息室與開放空間為主，仍應訂定管理要點，簽奉管理機關資安長以上長官核可。
- 5. 軍事上應特重保密之機敏處所（機敏專案辦公室或處理密級以上之專案辦公場）或其他法規所限制之禁制區域，嚴禁納入無線區域網路訊號涵蓋範圍。
- 6. 單位已奉核准使用之無線區域網路設備應確依原申請項目運用，後續如在用途、設備型式及資安防護機制等有所變更時，應

報請國防部審查核可後，方可變更使用。

7. 臺灣戰術網路 (TTN) 相關裝置，均可運用無線區域網路結合衛星、實體線路、寬頻無線電或微波等方式，與 TTN 雲端環境或地端伺服器建立民網網路連線，惟該無線區域網路僅限運用於 TTN 授權裝置，不得逕行變更用途。

(二) 安全防護原則

1. 建置無線區域網路之單位，依國軍資訊安全責任等級分級作業實施計畫劃分之安全責任等級，A 級單位及其他等級單位機敏場所，應規劃建置固定式無線區域網路偵防系統，並視狀況搭配機動式偵防系統，全時間偵測及阻斷營區內非法無線區域網路溢波；B、C、D 級單位，應規劃建置固定式或機動式無線區域網路偵防系統，定期偵測及阻斷營區內非法無線區域網路溢波。
2. 無線網路區域設備須取得具備國家 (際) 等級之安全認證執照 (如美國聯邦資訊處理標準 (Federal Information Processing Standards, 以下簡稱 FIPS) 140-2 等級 3 以上或歐盟共同規範 Common Criteria 等)。
3. 無線區域網路需傳輸機密級以上資料時，須串接保密設備，保密設備須通過國安局鑑定；若無傳輸機密級以上資料時，須串接保密設備，保密設備須通過國家安全局鑑定或取得國家 (際) 等級之安全認證執照 (加密機制應符合 FIPS140-2 等級 3 以上，或經國安局認證通過，其加解密方式為金鑰長度 256 位元以上之 AES 演算法)。
4. 須具備用戶連線認證機制，且端點間跨無線區域網路及廣域網路存取應建立專屬之安全通道 (VPN)。
5. 無線終端用戶電腦須比照現行規定安裝各項防護、防毒及部頒資訊資產管控軟體，並納入國軍資安監控系統監控。
6. 須建置裝置管控系統，集中管控無線終端用戶電腦只允許連接特定無線區域網路名稱 (Service Set Identifier, 以下簡稱 SSID)，不得連接其他有無線區域網路，避免串網。
7. 恪遵網路實體隔離政策，嚴禁透過無線區域網路設備或以點對點 (ad-hoc) 模式連結其他設備跨接異質網系。

(三) 管理作法

1. 無線區域網路正式運作前，須建立網路安全整體架構圖，相關無線區域網路及附屬安全設備均應登錄資訊資產管理系統管制，並律定專人管理，每日清點記錄備查。
2. 短期申用之機動式 (非常駐式) 無線區域網路設備，應由單位通資部門管理及設定，使用人員須完成教育訓練記錄備查後始可申用，任務 (作業) 結束應即歸還。
3. 連接學術網路內無線區域網路之資訊設備，須為教師、學員 (生) 教學籍研究用之專用電腦設備，並應符合國軍營內民用通信資訊器材管理要點及國軍學術網路電子資料管理要點之規範。
4. 無線區域網路之 IP 區段須為專用、獨立網段，以區隔有線網路，利於資安防護、監控系統 (如防火牆及 IPS) 制訂無線區域網路管理政策。
5. 無線區域網路內設備，須採定址管理 (固定 IP、MAC)，以

系統登載使用者、IP、MAC 對應資訊，並針對未經授權連網裝置實施自動封鎖及告警，相關事件紀錄應至少保持一年以上。

6. 申用單位應每二週實施一次營區無線安全稽核，各司令部針對所屬申用單位每半年完整稽核一次，並運用機動式無線偵防設備加強稽核，以發覺營區潛在之無線威脅；相關紀錄均須簽請業管資安長及資訊主管核閱，以掌握情形。
7. 單位如發生無線區域網路相關設備遺失，或肇生資安洩（違）密事件，應立即停用該無線區域網路服務，俟違失（遭駭）查證及責任歸屬後，全面更換資料傳輸加密方式、帳密設定，並完成漏洞（風險）修復，始可重新呈報復用。

十二、國軍各密等網系傳輸架構及行政網資料交換系統管理

（一）軍、民行政網環境整備

1. 依實需建置軍、民網資料交換專用電腦及軍、專網資料交換專用電腦，須安裝專用構型系統、端點防護軟體 Fidelis、防毒軟體、及 ACA，加入軍網行政網 Staff 目錄服務管控，並以防火牆限制僅可連線跨網系資料交換系統（以下簡稱跨網系統）、基礎資訊服務（如 AD、DHCP、BNS、WSUS 及防毒系統等）及檔案伺服器（提供公發裝置影音檔案輸入使用，並依檔案伺服器管控作法執行設置）；另須開通軍網行政網（綠色）防護型隨身碟。
2. 檔案伺服器資安管控作法：檔案伺服器由各司令（指揮）部造冊列管，每季更新一次，統一納入各司令（指揮）部目錄伺服器（AD）管控、派送政府基準組態（GCB）、專用資料夾、資料夾設定權限管制（以個人或群組方式設定，且須供批核長官可讀取）、資料夾每週定期清理、安裝資安管控程式（端點防護軟體 Fidelis、防毒軟體、ACA、檔案加解密等）。
3. 建置單機檢疫電腦，須安裝還原卡（二小時還原一次）、構型系統（須每季更新版本，免更新病毒碼及漏洞修補）及單機版國軍移動式儲存媒體管控軟體，並依實需開通軍網行政網（綠色）、民網（黃色）、專網（紅色）防護型隨身碟及儲存媒體。
4. 管理機關資訊部門協助單位資訊人員完成跨網系統帳號及權限設定前，單位資訊人員須於系統內，先完成所屬批核長官及保密督導官權限、交換電腦、儲存媒體等設定。
5. 本案批核長官及保密督導官由各單位正副主官（管）或保防官擔任，若有職務異動或權限轉授，須簽奉上校級以上主官（管）核可。
6. 民網檔案轉入軍網功能，限於受防火牆保護且具固定連網 IP 位址之民網電腦始可申請使用。

（二）作業機制

1. 不得運用本系統傳輸非公務所需資料。
2. 各單位資料交換作業，以運用本系統為優先，無須填寫紙本資料交換申請單，若因任務急需或系統無法使用，可採取以紙本資料交換申請單及人工檢疫方式實施交換。
3. 民網檔案轉入軍網行政網（示意圖如附件十八）
 - （1）上傳檔案大小不得超過 4 GB，若有加密，須於上傳時一併

提供密碼，且加密方式須與交換系統功能相符，始能獲取核准碼，系統自動以單向光纖傳輸，並執行檔案掃毒及內容淨化，確認檔案安全後，傳送至軍網行政網跨網系統。

- (2) 使用者使用軍網行政網個人電腦登入跨網系統，以核准碼查詢檔案，並完成提送申請單後即可下載檔案運用；批核長官使用軍網行政網個人電腦登入跨網系統稽核檔案。

4. 軍網行政網檔案轉入民網行政網或專網（示意圖如附件十九）

- (1) 使用者使用軍網行政網個人電腦登入跨網系統，並將交換檔案上傳系統後，完成申請單填寫後，提送保密督導官審查。
- (2) 保密督導官使用軍網行政網個人電腦登入跨網系統，審查檔案內容無虞後，轉呈業管長官批核。
- (3) 批核長官使用軍網行政網個人電腦登入跨網系統，確認申請目的及稽核結果後批核申請。
- (4) 使用者申請軍網行政網檔案轉出至民網行政網，須使用軍、民網行政網資料交換專用電腦（以下簡稱軍民網交換電腦）登入跨網系統，下載檔案儲存於軍網行政網（綠色）防護型隨身碟後，至檢疫電腦執行掃毒與交換作業。
- (5) 使用者申請軍網行政網檔案轉出至專網，須使用軍、專網資料交換專用電腦（以下簡稱軍專網交換電腦）登入跨網系統，下載檔案儲存於軍網（綠色）防護型隨身碟後，至檢疫電腦執行掃毒與交換作業。
- (6) 確認檔案安全後，軍網行政網檔案轉入民網以民網（黃色）防護型隨身碟儲存檔案攜至民網行政網電腦下載檔案運用；軍網行政網檔案轉入專網以專網（紅色）防護型隨身碟儲存檔案攜至專網電腦下載檔案運用。

5. 專網檔案轉入軍網行政網（示意圖如附件二十）

- (1) 使用者使用專網電腦將檔案儲存於專網（紅色）防護型隨身碟後，至檢疫電腦執行掃毒。
- (2) 確認檔案安全後，以軍網（綠色）防護型隨身碟儲存檔案，始可攜至軍專網交換電腦下載檔案，並登入跨網系統，完成申請單填寫後，將交換檔案上傳系統後提送保密督導官審查。
- (3) 保密督導官使用軍網行政網個人電腦登入跨網系統，審查檔案內容無虞後，轉呈業管長官批核。
- (4) 批核長官使用軍網行政網個人電腦登入跨網系統，確認申請目的及稽核結果後批核申請。
- (5) 使用者使用軍網行政網個人電腦登入跨網系統下載檔案運用。

6. 專網檔案轉入民網行政網完成專網檔案轉入軍網程序後，再以軍網檔案轉入民網行政網程序辦理。

7. 儲存媒體檔案轉入軍網行政網（示意圖如附件二十一）

- (1) 使用者將儲存媒體內之檔案下載至檢疫電腦執行掃毒。
- (2) 確認檔案安全後，以軍網行政網（綠色）防護型隨身碟儲存檔案，並攜至軍民網行政網交換電腦下載檔案。
- (3) 使用者使用軍民網行政網交換電腦登入跨網系統，將交換檔案上傳，自動執行檔案掃毒及內容淨化。
- (4) 使用者使用軍網行政網個人電腦登入跨網系統，提送審查申

請後下載檔案運用；批核長官使用軍網行政網個人電腦登入跨網系統稽核檔案。

(5) 公發裝置影音檔案轉入軍網行政網：

- a. 使用者將儲存媒體內之檔案下載至檢疫電腦執行掃毒。
- b. 確認檔案安全後，以軍網行政網（綠色）防護型隨身碟儲存檔案，始可攜至軍民網行政網交換電腦下載檔案。
- c. 使用者使用軍民網行政網交換電腦登入跨網系統，將檔案關鍵資訊（名稱、類型、雜湊值、大小等）上傳，提送審查申請，並同時將檔案傳送至司令部核定之營區內或上級單位檔案伺服器存放，再至個人行政電腦下載運用。
- d. 權責長官使用軍網行政網個人電腦登入跨網系統實施事後稽核。

8. 專網檔案轉入專網

- (1) 使用者使用專網電腦將檔案儲存於專網（紅色）防護型隨身碟後，至檢疫電腦執行掃毒。
- (2) 確認檔案安全後，以專網（紅色）防護型隨身碟儲存檔案攜至專網電腦下載檔案運用。

(三) 系統管理

1. 權限管控：各單位管理者應每月針對單位內批核長官、保密督導官、管理者等權限帳號實施盤點，並將離（退）人員帳號及權限移除。
2. 資訊設定：單位管理者須依單位實況，於系統內登載交換電腦、儲存媒體編號、存置地點等相關資訊，並每月實施盤點與資料校正。
3. 未完成表單管理：各單位管理者應每月針對單位內申請單批核狀況實施追蹤，未完成批核程序之表單，主動請批核長官實施批核，通次室將不定期針對二個月以上未批核表單，並檢討單位未批核表單管制作法。
4. 異常檔案分析作業：經跨網系資料交換系統判定為異常並隔離之檔案，每月移請資安鑑識實驗室納入病毒庫或情資威脅資料庫。
5. 由博愛資料中心負責每日執行系統病毒碼更新作業。
6. 中毒事件：
 - (1) 各單位運用跨網系資料交換系統執行資料交換，並依程序完成申請單核定後，若該檔案經個人電腦防毒軟體判定為病毒者，系統上申請單紀錄可作為病毒事件查察佐證資料，經查察跨網系資料交換系統所登載檔案紀錄與病毒事件檔案相符，屬於正常交換程序，不得因此懲處當事人。
 - (2) 跨網系資料交換系統上實體檔案，若遭防毒軟體判定為風險檔案，得由通次室承辦人將申請單紀錄提供資安區隊辦理事件追查，並由申請單單位實施澄復。
 - (3) 跨網系資料交換系統內防毒軟體若產生風險檔案告警，由資安區隊協助經端點防護或鑑識調查分析，若無風險將持續提供服務。
7. 系統紀錄與檔案：
 - (1) 檔案及記錄保存：各項操作及交換表單紀錄至少保存二年以上，實體檔案超過三個月以上，未達一年者，將實施封存，

得由司令（指揮）部承辦人員，以電子郵件向通次室申請後始可下載，封存達三個月以上檔案，經通次室權責長官核定後使得刪除。

（2）封存檔案申請：由司令（指揮）部承辦人員，以電子郵件向通次室承辦人員申請後始可下載。

（3）操作記錄調閱：配合政戰局保防部門進行操作紀錄與檔案查察。

（四）國軍各密等網系傳輸架構

1. 單向閘道器導入原則（國軍各密等網系傳輸架構規則表如附件二十二）：

（1）國軍網路：軍、民網行政網路間統由本部建置單向傳輸設備、資安防護架構及資料審核系統；專屬網路由需求單位籌獲所需軟硬體資源，完備資安防護架構、過濾（審核）機制及網系機密等級認定並辦理管理要點訂（修）定後，始可建置單向傳輸機制。

（2）網際網路：網際網路傳輸可採防火牆限制資訊流方式逕行取得所需資訊，惟與國軍網路介接傳輸須完備管理要點訂（修）定及單向傳輸所需軟硬體資源籌獲。

2. 具備要件

（1）國軍網路內同機密等級網系間傳輸僅須建置整合式威脅管理與應用層防火牆防護介接，可依需求增設單向閘道器及其它防護機制。

（2）國軍網路與網際網路屬同機密等級網系間傳輸比照高機密等級網系資訊傳輸至低機密等級網系作法。

（3）低機密等級網系資訊傳輸至高機密等級網系：

a. 具時效性資訊：須建置三組單向閘道器、二組不同品牌作業系統多合一防毒（第一組八套以上、第二組二套以上防毒品牌）及內容重組淨化系統搭配整合式威脅管理與應用層防火牆（封包過濾）。

b. 其他類型資訊：傳輸資訊應建置審核系統並具備保密督導官及批核長官審核機制，須建置三組單向閘道器、二組不同品牌作業系統多合一防毒（第一組八套以上、第二組二套以上防毒品牌）及內容重組淨化系統搭配整合式威脅管理與應用層防火牆（封包過濾）。

（4）高機密等級網系資訊傳輸至低機密等級網系：

a. 具時效性資訊：傳輸資訊應完成資料審核降（濾）密作業，符合目標網系機敏等級，須建置二組單向閘道器、二組不同品牌作業系統多合一防毒（第一組八套以上、第二組二套以上防毒品牌）及內容重組淨化系統搭配整合式威脅管理與應用層防火牆（封包過濾）、資料防洩漏系統機制，自動化執行傳輸資訊過濾（過濾條件由各單位自行律定）。

b. 其他類型資訊：傳輸資訊應建置審核系統，由保密督導官審查及批核長官審核並完成資料審核過降（濾）密作業，符合目標網系機敏等級，須建置二組單向閘道器、二組不同品牌作業系統多合一防毒（第一組八套以上、第二組二套以上防毒品牌）及內容重組淨化系統、資料外洩防護系

統機制搭配整合式威脅管理與應用層防火牆（封包過濾），自動化執行傳輸資訊過濾（過濾條件由各單位自行律定）。

- (5) 感測器資訊傳輸至各等級網系：
 - a. 傳輸至相同機密等級網系：僅須建置整合式威脅管理與應用層防火牆防護介接，可依需求增設單向閘道器及其他防護機制。
 - b. 傳輸至低機密等級網系：傳輸資訊應完成資料審核過濾（降密）作業，符合目標網系機敏等級，須建置單向閘道器及整合式威脅管理與應用層防火牆（封包過濾）機制。
- (6) 單向傳輸設備須通過評估保證等級（Evaluation Assurance Level, EAL）4 以上，且不得以遠端連線方式執行管理。
- (7) 傳輸紀錄須保存一年以上備查。
- (8) 須限制傳輸目的及來源設備。
- (9) 須擬訂管理要點（格式如附件二十三），審查及核定批核與作法同專線民網（可納入附件五之專網管理要點訂定）。
- (10) 須經資通電軍指揮部反規測試通過後，始可啟用。
- (11) 單向傳輸設備線路均須張貼標示及設備連接點區黏貼易碎標籤。

十三、防火牆管理

（一）組態設定原則

- 1. 採透過模式（Transparent Mode）、橋接模式（Bridge Mode）或路由模式（Routed Mode）建構（如附件二十四），並設定管理 IP，限定僅可由內部特定電腦（如管理員電腦）連線作業。
- 2. 啟動校時（NTP Client）功能，軍網行政網防火牆須設定指向國軍網路時間同步伺服器（ntp.mil.tw）或其他完成校時之網路時間同步伺服器；民網防火牆須指向經濟部標準檢驗局委託中華電信建置之網路時間同步伺服器（clock.stdtime.gov.tw）；其他網系防火牆亦須建置相關時間校準機制，俾資安事件稽核及查處。
- 3. 依據防護標的或服務對象設置不同防護區域（ZONE，如全軍性服務區、內部服務區及使用者區等），限制各防護區域之網路連線，確保資訊服務存取安全。
- 4. 防火牆部署須配合建置事件紀錄及分析機制，經防火牆規則阻擋之來源、目的 IP 位址、目的連接埠、時間等紀錄，優先導向國軍資安防護中心監控、分析；因故無法導向之系統，須自建紀錄伺服器（Log Server），並保存一年以上紀錄。
- 5. 修補程式或更新版本，應利用深夜或假日等網路流量較小之離峰時間，並定期完成備份作業，備份檔案保存一年以上。

（二）管理原則

- 1. 防火牆須建置具門禁及溫、濕度管控之空間及環境，確保實體安全及系統高可用度。
- 2. 防火牆管理帳號申請（異動）須經單位通資業務主管同意，以最小數建置，並限定專人專用、登入 IP，且不得共用帳號。
- 3. 管理員帳號須每季更新密碼，密碼長度及複雜度須符合部頒國

軍資訊安全政策暨相關資安規範；另帳號登入失敗次數超過三次須發出警訊，並鎖定三十分鐘。

（三）防火牆規則

1. 通用原則

- （1）以全面阻擋，例外開放為原則，開通規則（輸出、輸入）以白名單方式設定，明確律定各區域間資訊流方向。
- （2）輸入規則須律定來源端、目的端 IP 與目的端連接埠，不得以任何或未指定方式（any、all）設定，避免非法連線隱藏於合法資訊流。
- （3）輸出規則僅允許內部合法網段對外部網路連線，內部來源端不得以任何或未指定方式（any、all）設定，以阻擋來自內部之偽冒攻擊。
- （4）檔案傳輸（如 TCP：20、21）、檔案分享（如 TCP：139、445）及遠端連線管理（如 TCP：22、23、3389）等高風險連接埠，須嚴格審查並奉權責長官核定後始得開通。
- （5）國軍電腦緊急應變中心發布黑名單資訊後，即向通資業管主管報備，於防火牆以專屬規則阻擋，並於完成後簽奉核定，以防範網路零時差攻擊。

2. 民網專屬原則

- （1）不允許自外部（網際網路）連線至內部（包含防火牆）進行系統、設備維管作業。
- （2）僅允許內部 DNS 對外部建立網域名稱查詢連線（UDP：53），防火牆系統本身及內部網路電腦主機僅向本部及單位內部 DNS 執行網域名稱查詢。
- （3）選擇一個特定 IP 位址（例如：172.20.20.1），於內部 DNS 將黑名單內所有網域（Domain）位址指向此特定 IP，同時於防火牆規則，設定記錄連至此 IP 的電腦主機，當有後門程式連線行為時，即會觸發規則並列入紀錄。
- （4）相關資訊系統、伺服器、防護系統、網路等設備管理，須於專用網段下以專屬電腦操作，且該電腦不得連接網際網路或移動式儲存媒體。

3. 申請作業

- （1）因任務須辦理防火牆規則開通或變更，應填具防火牆規則變動申請單（如附件二十五），於任務執行前一週完成一般性申請；因緊急任務（如演習、系統緊急測試等）須立即開通或變更防火牆規則，得由需求單位及業務部門協調通資部門（跨軍種應由管理機關通資部門相互協調）優先作業，並於一週內完成正式程序申請。
- （2）內部網段存取外部資訊服務，由通資部門審認後開通；外部網段存取內部資訊服務，如內部系統非通資部門業管，須由業管部門附議業務需求，再經通資部門審認後開通。
- （3）規則變更申請須奉單位通資主管（含）以上長官核定；演訓活動依相關指導計畫所律定權責辦理。
- （4）申請單應留存一年，俾後續稽核及查考。
- （5）開通之規則有效期限最長迄止時間為當年度十二月三十一日止，不得以「永久」方式申請，各單位應定期執行規則清校簽奉權責長官核定，並刪除無效之規則。

十四、其他

- (一) 本部將定期辦理執行現況檢討會，並配合年度通資電戰備督考及網路攻防演練時機實施驗證；各級單位應依一級督導一級權責，定期督考、驗證所屬執行成效。
- (二) 定期對所屬網管人員辦理教育訓練，並鼓勵獲取相關專業證照，以提升各單位網路管理能量。
- (三) 本規定未臻詳盡部份，應遵行國軍資訊安全政策、國軍資訊資產管理作業規定、國軍資通安全責任等級分級作業指導、國軍資安事件通報應變指導要點及國防部所管特定非公務機關資通安全管理作業辦法等規範；未依規定肇致相關違犯事件，除依法究辦外，並依陸海空軍懲罰法及國軍資通安全獎懲規定議處。