

# 國防部全民防衛動員署後備指揮部

## 網路管理作業規定

### 一、依據

國防部 109 年 4 月 21 日國通資安字第 1090084375 號令修頒網路管理作業規定暨本部任務實需辦理。

### 二、目的

為有效規範國軍網路管理程序，落實網段與網路管理作為，特訂定本規定，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。

### 三、名詞定義

- (一) 國軍網路：泛指國軍資訊通信系統(MICS)內使用 TCP/IP 網路通信協定標準之網路總稱。
- (二) 專屬網路：係指國軍網路內，所有自主運作且相互實體隔離之網路，如捷訊網路、戰情網路及迅安網路等。
- (三) 國軍資訊網路(MINET，簡稱軍網)：指國軍網路內提供國軍人員行政作業之網路環境。
- (四) 網路位址(簡稱網址或 IP)：係指節點設備於國軍網路上之 IPv4 位址，任一網址均具唯一性，由四碼組成(例如 10.20.55.33)。
- (五) 網段：指各級註冊中心合法註冊使用 IPv4 位址範圍。
- (六) 網域名稱解析系統(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)。
- (七) 國軍網段管理系統(簡稱 MWHOIS 系統)：為提供國軍網路內網段註冊、管制、查詢等功能之系統。
- (八) 軍租軍網網路：委託民間固網公司籌建之國軍專用資訊網路。
- (九) 國軍網路註冊中心：國軍網路最頂層註冊單位，負責國軍網路網段、網址規劃、註冊與管理。
- (十) 第一級註冊中心：負責專屬網路(含軍網)規劃、註

冊與管理，並向國軍網路註冊中心申請網段。

- (十一) 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。
- (十二) 網址需求單位：依需求向第二級註冊中心申請網段，並負責授權網段規劃、註冊與管理。
- (十三) 國軍骨幹網路：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。
- (十四) 網卡號碼(Media Access Control，簡稱MAC)：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。
- (十五) 網路拓譜：網路連結示意圖。
- (十六) 國軍BNS(簡稱BNS)：指國軍用以管理(控)營區內網路動態之資訊系統。
- (十七) 行政民網(單一閘口民網)：指國軍連結政府網際服務網(簡稱GSN)用以行政作業之民網環境。
- (十八) 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。
- (十九) 動態主機組態協定(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。

#### **四、適用範圍**

國軍資訊通信系統(MICS)內使用TCP/IP IPv4網路通信協定標準，以有線方式連結國軍網路之通資軟硬體設備、武器裝備、單位及人員，均為納管範圍。

#### **五、權責劃分**

- (一) 本部動管處(以下簡稱管理機關)：
  - 1. 依任務特性擔任專屬網路第一級註冊單位，負責核配專屬網段管理。
  - 2. 依第二級註冊中心權責，負責專屬網路(含軍網)所屬網段管理。
  - 3. 負責所屬單位軍租軍網申請資格初審。

4. 綜整所屬單位軍租軍網申請資料向通次室提出複審申請。
  5. 負責管理、稽核所屬單位軍租軍網設備及資訊安全。
  6. 負責所屬營區網路管理制度頒訂、督導及考核。
  7. 負責業管及所屬單位BNS部署、管理與稽核。
  8. 負責業管及所屬單位網段、網路設備、網路存取規則規劃、稽核與技術支援。
  9. 負責業管及所屬單位網路違規通報案件查察、稽核、回復及管制。
- (二) 各地區指揮部(以下簡稱管制單位)：
1. 協助本部管理所屬網路(含軍網)所屬網段管理。
  2. 協助綜整呈報所屬單位軍租軍網申請作業。
  3. 負責管理、稽核所屬單位軍租軍網設備及資訊安全。
  4. 負責所屬營區網路管理制度頒訂、督導及考核。
  5. 負責業管及所屬單位BNS部署、管理與稽核。
  6. 負責業管及所屬單位網段、網路設備、網路存取規則規劃、稽核與技術支援。
  7. 負責業管及所屬單位網路違規通報案件查察、稽核、回復及管制。
- (三) 本部軍網及軍租軍網使用單位(以下簡稱各使用單位)
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. 負責軍租軍網連網設備保管與繳回。
  4. 負責軍租軍網申請、異動、註銷呈報。
  5. 負責所屬BNS維管與稽核。
  6. 負責所屬網路實體環境、網路存取規則管理及維護。
  7. 負責所屬網路違規案件查察及回復。

## 六、國軍網路註冊架構

國軍網路註冊架構，劃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

一)，相關作業權責說明如下：

(一) 國軍網路註冊中心

1. 受理第一級註冊中心網段申請，並依需求配發網段。
2. 建置 MWHOIS 系統，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，並依需求配發或指派網段。
2. 依所配發或指派之網段，專屬網路須完成網段使用單位分配表，軍網須於 MWHOIS 系統完成登錄及管制。
3. 可視實際作業需求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(本部)

1. 受理網址需求單位網段申請，並依需求配發或指派網段。
2. 依所配發或指派之網段，專屬網路須完成網段使用單位分配表，軍網須於 WHOIS 系統完成登錄及管制。

(四) 網址需求單位(地區、縣市)

1. 所配發之網址須使用動態主機組態協定(以下簡稱 DHCP)服務，並以軟、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，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)必須強制限定 IP 與 MAC，以防制使用者私自竄改 IP。

## 七、軍(專)網網路管理

(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(如單位改隸或南遷北調)，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. 軍網內嚴禁使用網址轉換(Network Address Translation, NAT)方式作業，若因任務必須採用 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，各軍種仍循前五目原則由已分配網段內自行配發，不足部分向本部申辦另行檢討分配。

## (二) 網段(址)配發原則

1. 軍網網址規劃，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，兼顧目前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、駐地與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. 非屬軍網第二級註冊中心配發者，一律向軍網第一級註冊中心申請配發。

### (三) 網段(址)管控流程

#### 1. 申請作業

- (1) 需求單位辦理軍網網段(址)申請作業，應檢附網路位址需求規劃書(如附件三)，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(如附件四)，並經本部審查後函送通次室審查及核定。
- (3) 註冊中心負責將申請單位相關資料建置於 MWHOIS 系統內。
- (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，並加副知資電部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 系統管理人員一員，人員職務異動時，須即刻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) 各單位因故必須變更或撤銷現用網段或網址者，應行文上層註冊中心並辦理 MWHOIS 系統異動。
- (2) 各單位如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。

## 八、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. 使用單位申辦軍租軍網新增、異動及註銷作業，統一呈報各管理機關初審後，轉通次室複審，不得逕向固網公司臨櫃申請。
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. 若遇特殊情況(如：原有電路無法升速或頻寬已達飽和等)，申請單位得不受上述原則限制，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. 各單位新申請或升速之電路，原則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，以專機專用網路設備設置於固網公司機房獨立機櫃內，依專網專用原則以專用設備電路與國軍專、民網實體隔離，且連接之資訊設備均不得跨網系混接。
2. 軍租軍網連網設備(如數據機、路由器等)須黏貼識別標籤(如附件五)，各使用單位上鎖(或管制區保管)，並納所屬 BNS 管控；電路註銷時，設備歸還固網公司，如有遺失，由使用單位賠償。

## (三) 對固網公司督導原則

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，資料保存一年備查。
3. 固網公司指派專人管理網管系統及網路設備，依國防部資訊安全規定，定期更換帳號及密碼，部署防火牆、媒體管控軟體、防毒軟體、漏洞修補程式等，強化資訊作業安全。
4. 通次室定期(每半年)對固網公司機房實施稽核一次。

(稽核表如附件六)

(四) 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(如附件七)，每半年校正資料一次，於六月三十日及十二月三十一日前，以國軍電子郵件送通次室備查。
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。

(五) 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(如附件八)函送通次室審查。
2. 不論申請期程長短，均應於任務完成後，辦理註銷作業；申請、異動及註銷作業均填具申請表(如附件八)辦理。
3. 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(申請流程圖如附件九)。
4. 各使用單位申請提升頻寬或增加網段時，應檢附網路拓樸圖，呈報各管理機關辦理初審後，函送通次室審核。

(六) 異動作業

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，辦理移機及網段重新核配事宜。
2. 申請表(如附件八)內填註計畫異動後之資料，異動區分欄填註代碼為U。

(七) 註銷作業

1. 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，轉通次室辦理異動或註銷。



2. 申請表(如附件八)內異動區分欄填註代碼為D，備考欄註明附掛電話保留做市話或一併註銷。

#### (八) 故障處理

1. 使用單位遇故障時，逕向固網公司報修，報修時提供附掛電話號碼或電路編號、故障情形、報修人員姓名及聯絡電話以利故障查修，另通報本部資安值日官(軍線：261681)協請登報於國軍電腦緊急應變中心(MCERT)上，以利本部通報通次室，逐級管制修復進度。
2. 軍租軍網故障原因涉及國軍網路設備時，由通次室協調資電部、固網公司共同查修，管制故障處理進度。

### 九、營區網路管理

#### (一) 網路分級管理原則

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，摘述如下：

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、機敏、系統管理不同等級網段，分級概念及存取規則說明如后(概念圖及規則表如附件十)：
  - (1)公務電腦網段：為作業人員使用之公務電腦及週邊設備網路區段，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機敏資訊網段，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它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)，允許存取機敏伺服器資訊服務，及有條件存取一般伺服器資訊服務。

c. 系統管理設備網段：收容網路管理、系統效能監控管理等專屬網路、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、具第三層功能之網路設備等)設定正向表列方式政策，明確定義資訊服務存取對象。

## (二) 網路實體架構原則

1. 軍網(區分行政網及專網)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

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(含)以下為原則。

3. 營區網路建置採取乙太網路(Ethernet)架構，網路主幹與中繼採取 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
5. 管理協定(SNMP)、終端機管理協定(Telnet、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。
6. 連結軍網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)，命名原則參考附件十一。
7. 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)，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. 單位所屬目錄(Active Directory, AD)伺服器、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. 資訊設備(如伺服器、個人電腦、網路印表機、網路監視器等)連結軍網，須先期於 BNS 完成 IP、MAC 及相關資料(如使用單位、使用者、連結之交換器及埠口等)註冊；未經註冊之設備連結軍網，系統將自動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. 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失，續由肇失單位依指揮體制逐級向上回報、管辦。
6. 各級單位請落實定期監控機制，對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(如附件十二)。
7. 偏遠獨立單位營區及軍租軍網專線單位 BNS 納管原則，應依一級督導一級權責，或協調鄰近單位收容，餘管理原則同上所述。

#### (四) 營區網路管理執行作法

##### 1. 網段權限指派：

- (1)由國防部分配本部(含所屬)使用網段，完成路由設定，並於 MWHOIS 賦予網段管理權限。
- (2)本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，俾確維資料正確。

##### 2. 資訊設備申請連結軍網

- (1)長期性連結軍網資訊設備，由資訊業管部門至 BNS 完成 IP、MAC 註冊及交換器埠口設定。
- (2)臨時或短期性連結軍網資訊設備，申請單位填寫連接軍網設備 IP 申請單(如附件十三)，由中校(含)以上權責主官(管)核准，由資訊業管部門至 BNS 完成 IP、MAC 註冊及交換器埠口設定，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。
- (4)無法自動取得 IP 之資訊設備，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。

- (5)連結軍網之設備，均先行於資訊資產管理系統完成帳籍登載，再行至 BNS 完成註冊，未完成相關設定前，設備不得連接網路線。

### 3. 軍網設備資料異動

- (1)申請異動之資訊設備先行離線，資訊業管人員續依連接軍網設備 IP 申請單，至 BNS 完成 IP、MAC 或交換器異動設定。
- (2)確認異動之資訊設備於系統完成後，始可連結軍網重新取得 IP；無法自動取得 IP 之設備，依新獲配 IP 組態紀錄，以人工手動方式設定，始可連結軍網。
- (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(申請表如附件十四)，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，以落實管理各項網路資源運用。
- (2)私自將未經核定資訊設備連結軍網遭系統偵測、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資通安全獎懲規定檢討相關責失議處，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，一個月內至 MCERT 網站辦理結案。
- (4)合法設備因系統設定錯誤連結軍網遭系統偵測、阻斷，惟紀錄無回傳 MCERT，使用單位檢附佐證資料，由資訊業管部門完成系統修正。

(5)上述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；經查獲藉系統設定(如交換器設定透通模式或停用)刻意規避違規偵測，將依相關規定究責議處。

(6)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。

### 3. 防火牆開通申請

(1)申請單位確認防火牆開通來源端、用戶端、服務埠口及生效、終止日期，填寫防火牆規則變更申請單(如附件十六)，由權責長官核定後，移交資訊業管部門審查。

(2)資訊業管部門依據網路分級存取規則表及國防部頒國軍資訊系統防火牆管理暨規則設定作業指導辦理審查、落實執行。

## 十、民網管理原則如下：

### (一)設置原則

1. 各單位連接民網，以收容至單一閘口機制為主要手段，並以連接政府網際服務網（GSN）為優先考量，藉集中控管確保一致資安防護強度，防止洩（違）密情事發生。

2. 各單位民網節點均應收容至指揮部民網單一閘口；設置原則摘述如后：

(1)指揮部單一閘口統一收容各幕僚單位、直屬單位、地區、縣市指揮部等民網電腦，各地區指揮部不再另設民網單一閘口。

(2)各幕僚單位額外新增連接民網單一閘口網路節點需求者，需填具申請單後，簽奉參謀長（含）以上長官核定後，由動管處規劃連網架構，需求單位負責新增設備及線路費用。

(3)如轄屬單位需新增單一閘口網路節點，需呈文至本

部簽奉參謀長（含）以上長官後始可辦理開通使用。

- (4) 因特殊因素（如任務需求、GSN 線路無法到達等）以單一閘口以外方式連接民網者，需求單位需檢附連網計畫，送動管處審查，簽奉副指揮官（含）以上長官核定後，呈國防部核備。

## (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軍網(含專網)混(搭)接，且不得使用無線網路或處理機敏公務。
2. 民網電腦使用單位應建立民網使用管制登記簿，並簡述瀏覽路徑位址(如 google.com 等)，並定期上呈權責長官批示。
3. 民網電腦移作其他用途或其他用途電腦移為民網電腦時，均須執行電腦格式化。
4. 連線設備使用合法版權軟體(辦公室套裝軟體應安裝國發會 NDC 開放文件格式 ODF 應用工具)，除管理人員外，其他人員嚴禁更動系統設定。
5. 民網電腦不得設定分享並使用後應即登出，長時間不使用應關機。
6. 主機名稱(Hostname)規則同軍網電腦，並納入網域(frccei.mnd.gov.tw)管控，未經核定，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。
7. 應啟用帳密登入，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。

8. 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。
9. 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。
10. 各單位須於每季季末(3、6、9及12月)呈報次季民網IP管制清冊，內容須述明單位、電腦名稱、IP、MAC、使用者、儲位及用途等。
11. 嚴禁於民網(戶役政)電腦私自安裝各類型即時通訊軟體(如Line)、具遠端或資料傳輸(如Teamviewer)或陸港澳地區發行之高風險程式。
12. 如民網電腦因非公務需求不當使用或安裝非奉核軟體而肇生資安防護系統告警或資安事件，除依「國軍資通安全獎懲作業規定」議處外，並註銷該電腦IP使用權限並要求單位撤除電腦。

#### 十一、單一開口外民網管理

- (一)各縣市指揮部戶役政系統主機及資料查詢電腦，設置於資訊室機房內，由資訊官負責管制，使用VPN電路連線，除每週固定時段下載戶役政資料及資料查詢外，不得執行其他作業或瀏覽與戶役政業務無關之網站。
- (二)單一開口外電腦對外應設置防火牆設備，採全面阻擋，例外開放之規則設定且須指定特定服務開通，除業務所需使用及漏洞修補及病毒碼更新白名單外，餘不得隨意開放，並需不定期至電腦緊急應變中心(MCERT)首頁查看行政院技服中心黑名單並納入防火牆黑名單阻擋。
- (三)各單位除每週固定使用時段開啟單一開口外資訊設備外，餘時段須將資訊設備全數關機，避免遭受惡意攻



擊，另作業系統需安裝 Windows Server 2012 以上版本，避免肇生資安罅隙。

(四)防毒軟體應使用集中式端點安全防護產品賽門鐵克防毒軟體，並嚴禁於單一閘口內(外)民網環境使用未經奉准開放使用之移動式儲存媒體(如 USB、讀卡機等)。

(五)如戶役政電腦因非公務需求不當使用或安裝非奉核軟體生資安防護系統告警或資安事件，除依「國軍資通安全獎懲作業規定」議處外，並由本部辦理該電路註銷作業。

## 十二、防火牆管理原則如下：

### (一)組態設定原則

1. 採透通模式(Transparent Mode)、橋接模式(Bridge Mode)或路由模式(Routed Mode)建構(如附件十五)，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，軍網防火牆須設定指向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. 各單位提供之資訊服務，如有不同服務對象(如全軍性服務、軍種內部服務及單位內部服務)，須以服務對象及不同 IP 區段設置不同存取規則。
4. 防火牆須建置事件紀錄及檢核機制，其中被防火牆阻擋的行為，包含來源、目的 IP 位址、目的連接埠、時間等資訊均須完整記錄，相關紀錄至少須保存 1 年；另建置「事件收容模組(EAM)」伺服器單位，須配合資電部將防火牆事件紀錄導向該伺服器；民網戶役防火牆須將防火牆事件紀錄導向本部建置之事件分析器，

並於防火牆設定規則允許事件紀錄回傳本部以利分析。

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，不得共用帳號。
3. 管理員帳號須每季更新密碼，密碼長度並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、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)，限制防火牆系統本身及內部網路電腦主機執行網域名稱查詢，僅得指向內部 DNS。
- (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。

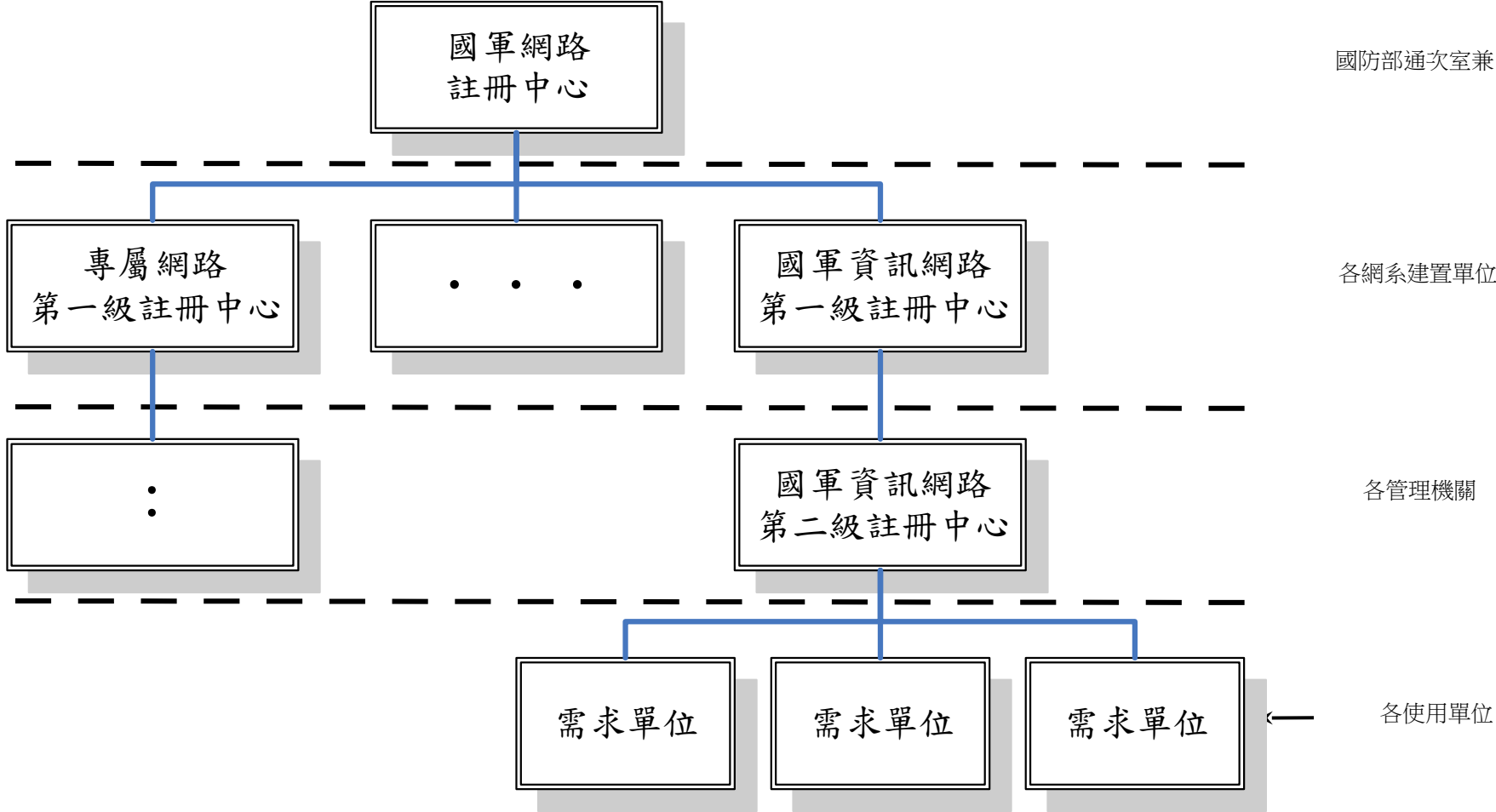
## 3. 申請作業

- (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(如附件十六)，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)因民網環境暴露網路攻擊風險下，需常態保持監控並於遭受攻擊時立即納入防火牆阻擋，攻擊數據統計表併同防火牆臨時變更申請單於每周五上呈幕僚長以上長官批示。
- (3)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。
- (4)規則變更申請須奉單位通資主管(含)以上長官核定；特殊演訓活動依其相關指導計畫所律定權責辦理。
- (5)核定執行之申請單應留存一年，俾後續稽核及查考。

### 十三、其他

- (一) 本部配合年度資訊安全督考時機，驗證各單位執行成效，並提列工作檢討會檢討。
- (二) 本部及各地區定期辦理網路管理教育訓練，提升各單位對網路管理能量，並蒐整改進建議，持續強化網路安全管理作業。
- (三) 凡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訊安全相關規定懲處。
- (四) 網系間資料交換須經跨網系資料交換系統，並經由相關保防部門及權責長官奉准後始可實施資料交換，資料交換均需以核可使用之移動式儲存媒體執行作業。
- (五) 本規定未臻詳盡部份，應遵行部頒「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」、「跨網系資料交換部署計畫」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。

附件一 國軍網路註冊架構



## 附件二 網段配發原則表

連網設備總數量(含虛擬設備)	核發網段數量(Suffix)
200 臺以下	Class C(/24) × 1
201 ~ 500 臺	Class C(/23) × 2
501 ~ 700 臺	Class C × 3
701 ~ 1000 臺	Class C(/22) × 4
1001 ~ 1250 臺	Class C × 5
1251 ~ 1500 臺	Class C × 6
1501 ~ 1700 臺	Class C × 7
1701 ~ 2000 臺	Class C(/21) × 8

## 附件三 網路位址需求規劃書(範例)

### 網路位址需求規劃書

#### 一、前言

#### 二、網路架構簡介(含網路架構圖)

#### 三、網路位址需求及編配規則

##### (一)網路位址需求

案內規劃建議配發 IP 總需求數為○○，建議撥發○個 Class C 網段，安裝之設備及網路位址需求數量如下列所示：

陣地名稱	裝備名稱	裝備數量	IP 數量
○○營區	個人電腦	○	○
	伺服器	○	○
	路由器	○	○
	交換器	○	○
	印表機	○	○
	IP 需求數量	○	
	建議配發 IP 數量	○個 Class C	

##### (二)網路位址編配規則規劃

IP 位址的分配規劃如下：

- 個人電腦：10. x. y. a ~b，共○個 IP 位址。
- 伺服器：10. x. y. c~d，共○個 IP 位址。
- 路由器：10. x. y. e~f，共○個 IP 位址。
- 交換器：10. x. y. g~h，共○個 IP 位址。
- 印表機：10. x. y. i ~j，共○個 IP 位址。

## 附件四 專屬網路/專線民網管理要點(範例)

# ○○○專屬網路/專線民網管理要點

壹、依據

貳、目的(說明本網申用之必要性)

參、權責劃分

肆、連線架構(含網路架構圖，民網須說明申租之固網公司)

伍、適用範圍(含設備列表)

須含所有連結本專網所列管之設備(交換機、網路設備、電腦設備、保密器、環控設備、電話話機及攝影機等)。

陣地名稱	裝備名稱	裝備數量	IP 數量
00 營區	個人電腦	○	○
	伺服器	○	○
	路由器	○	○
	交換器	○	○
	印表機	○	○
	IP 需求數量	○	
	建議配發 IP 數量	○個 class C	

陸、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(含各項連結本專網之實體設備)

四、網路連線管理(含資安防護系統等)

五、作業系統管理(含權限及網域政策等)

六、作業機制管理(含資料交換、儲存等)

七、維運管理(含系統維護、備援及督導稽核等)

柒、其他

一、獎懲做法。

二、聯絡資訊。



## 附件五 軍租軍網識別標籤

軍租軍網網路設備	
使用單位	
保管人	
附掛電話 (電路編號)	
備註：軍租軍網租用設備， 請妥慎保管，於電路註銷時 繳回固網公司	

## 附件六 固網公司機房資安稽核表

### 國軍軍租軍網固網公司(○○公司)機房 ○○年度資安稽核表

稽核日期： 年 月 日

檢查項目	合乎要求	所見事實	備考
<b>一、實體安全部份：</b>			
(一)資訊機房門禁是否使用密碼鎖(數位電子鎖)？			
(二)人員進出機房是否填寫管制簿管制，並保留近一年紀錄？			
(三)軍租軍網網路設備是否設置為獨立機櫃？機櫃前後門是否上鎖，鑰匙是否由專人保管？			
(四)各設備未使用之連接埠是否關閉並加蓋負責人章及加註時間之貼紙黏貼？			
(五)軍租軍網組態設定是否統一由台北機房網管主機管理？			
(六)台北機房網管主機是否依本部資訊安全要求辦理？是否安裝移動式媒體管控軟體、輸出入埠是否有管制？			
(七)維管人員進行軍租軍網連網相關設定或異動時，是否紀錄於工作日誌以供查閱？			

國軍軍租軍網固網公司(○○公司)機房

○○年度資安稽核表

稽核日期： 年 月 日

檢查項目	合乎要求	所見事實	備考
<u>二、人員安全部份：</u>			
(一)中華電信維管人員是否經過公司實施安全審查作業？			
(二)人員安全審查要件是否符合國軍人員安全調查標準？			
<u>三、網路安全部份：</u>			
(一)軍租軍網資訊網路是否與其它網路串連？			
(二)是否保存近一年之防火牆紀錄(台北機房網管主機)？			
(三)資訊網路設備帳號、密碼是否定期變更並紀錄備查？密碼設定是否符合安全性原則(複雜度、使用歷程十二次以上、最長使用期限九十天)？			
(四)檢查本地路由器路由資訊及各區域路由資訊是否符合網段分配規則？			

## 附件七 軍租軍網電路總表

[illegible]

附件八 國軍軍租軍網申請、異動、註銷表

國軍軍租軍網申請、異動、註銷表

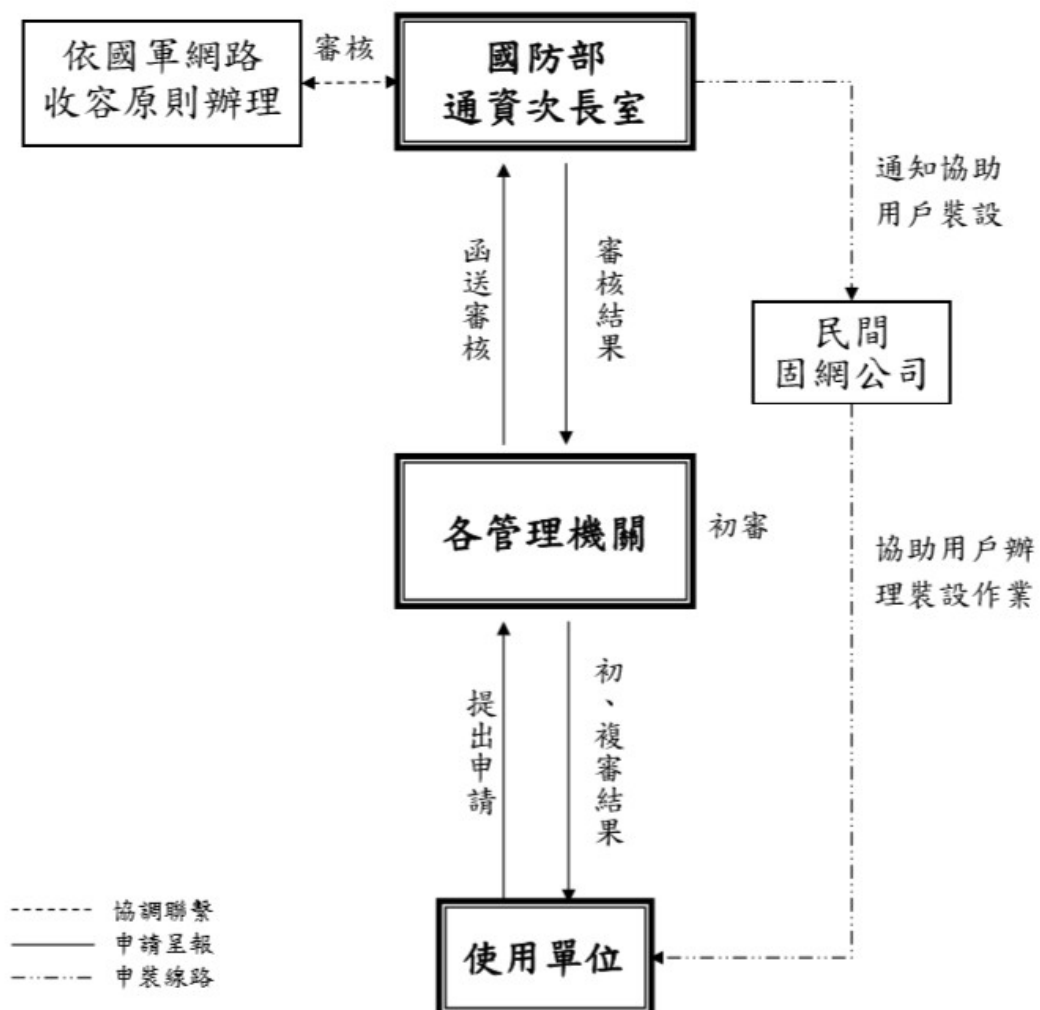
項次	網段	電路編號	使用單位 (營區名稱)	裝機地址	聯絡人		事由	異動區分	備考
					姓名	聯絡電話			

填表說明

- 標題請區分申請、異動或註銷表。
- 「網段」：屬新申請者，統一由通次室填註，請保持空白；屬異動或註銷者請填註原分配之軍租軍網網段。
- 「附掛電話(電路編號)」：請填註連網外線電話號碼(含長途碼)或電路編號；電路註銷時請於備考欄註明「附掛電話」確認保留做市話使用。
- 「使用單位」：請填寫單位全銜並於最後加上(○○營區)，避免單位番號或代碼等機敏資訊外流。
- 「裝機地址」：請填註民間地址，如查無民間地址，請註明某路段或地標附近，俾利派工人員前往施工。
- 「連絡人」及「連絡電話」：請依實況填註軍線、外線電話(如有分機號碼請一併填註)或行動電話，俾利派工時間協調與確認。
- 「事由」：請概略說明使用單位申請、異動、註銷主要原因。
- 「異動區分」：A 申請、U 異動、D 註銷。
- 「備考」：未盡事宜請於備考欄補述(如：1、異動時請於備考欄註明異動項目(如原裝機地址異動為…)。2、短期(演訓)電路由各使用單位自籌經費支應，請於備考欄註明「自費」、帳單地址及使用起迄日期；任務結束後通次室統一辦理註銷)。
- 本表不足部分請自行由本表最後項次延伸，惟延伸時請將「填表說明」置於最後，俾利參考。
- 故障報修電話：080-000-123

## 附件九 國軍軍租軍網申請流程圖

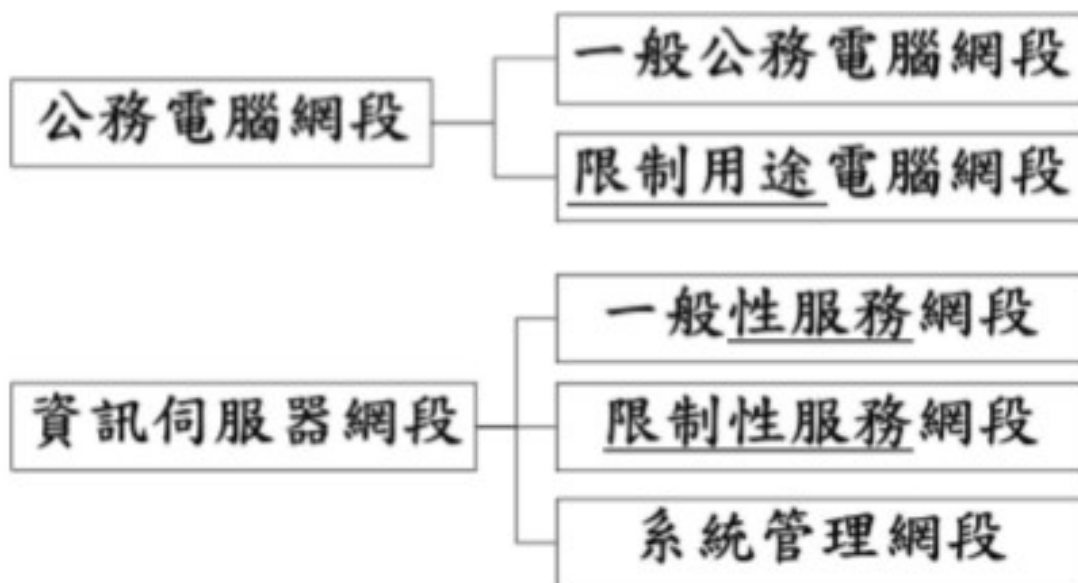
### 軍租軍網申請流程圖



備註：

1. 各管理機關彙整連網需求，於三週前送通次室審查。
2. 網路架設施工期間，任何異動統由各管理單位向通次室提出申請。
3. 任務結束後，通次室統一辦理註銷，租用設備(如數據機)由各管理單位管制於一週內歸還固網公司，如有遺失，由各管理單位負責賠償。

## 附件十 網路分級概念圖及存取規則表



網路分級存取規則表						
目的網段		公務電腦		資訊伺服器		
來源網段		一般	限制	一般	限制	系統管理
公務電腦	一般	×	×	○	×	△
	限制	×	×	△	△	△
資訊伺服器	一般	×	×	○	×	×
	限制	×	×	△	△	×
	系統管理	△	△	△	△	△
○：可以存取      ×：禁止存取      △：條件式存取						

## 附件十一 資訊設備命名原則

### 一、命名原則

- (一) 主機名稱由英文及數字組合而成，一律定為十碼以上，不得採用中文名稱。
- (二) 同一營區單位主機名稱不得重覆。
- (三) 同一網段內收容不同單位設備時，主機名稱由網段管理單位律定。

### 二、資訊主機命名方式

「單位名稱英文縮寫」+「IP 位址編碼」+「用途碼」。  
(以通次室公務電腦為例)

	單位名稱英文代碼	設備 IP 位址編碼	用途碼
碼數	3 碼	6 碼 (10.32.55.120)	1 碼
範例	CEI	203778	W

### 三、資訊伺服器完全領域名稱命名原則

- (一) 資訊伺服器完全領域名稱主記錄(A Record)由前項律定之主機名稱加上單位領域名稱(Domain)組成。
- (二) 資訊伺服器對外公佈之完全領域名稱，應使用別名(Alias)記錄，避免使用原始主記錄，以強化安全管理與記憶。
- (三) 別名記錄申請以 3 組為上限，並應符合伺服器提供之網路服務。

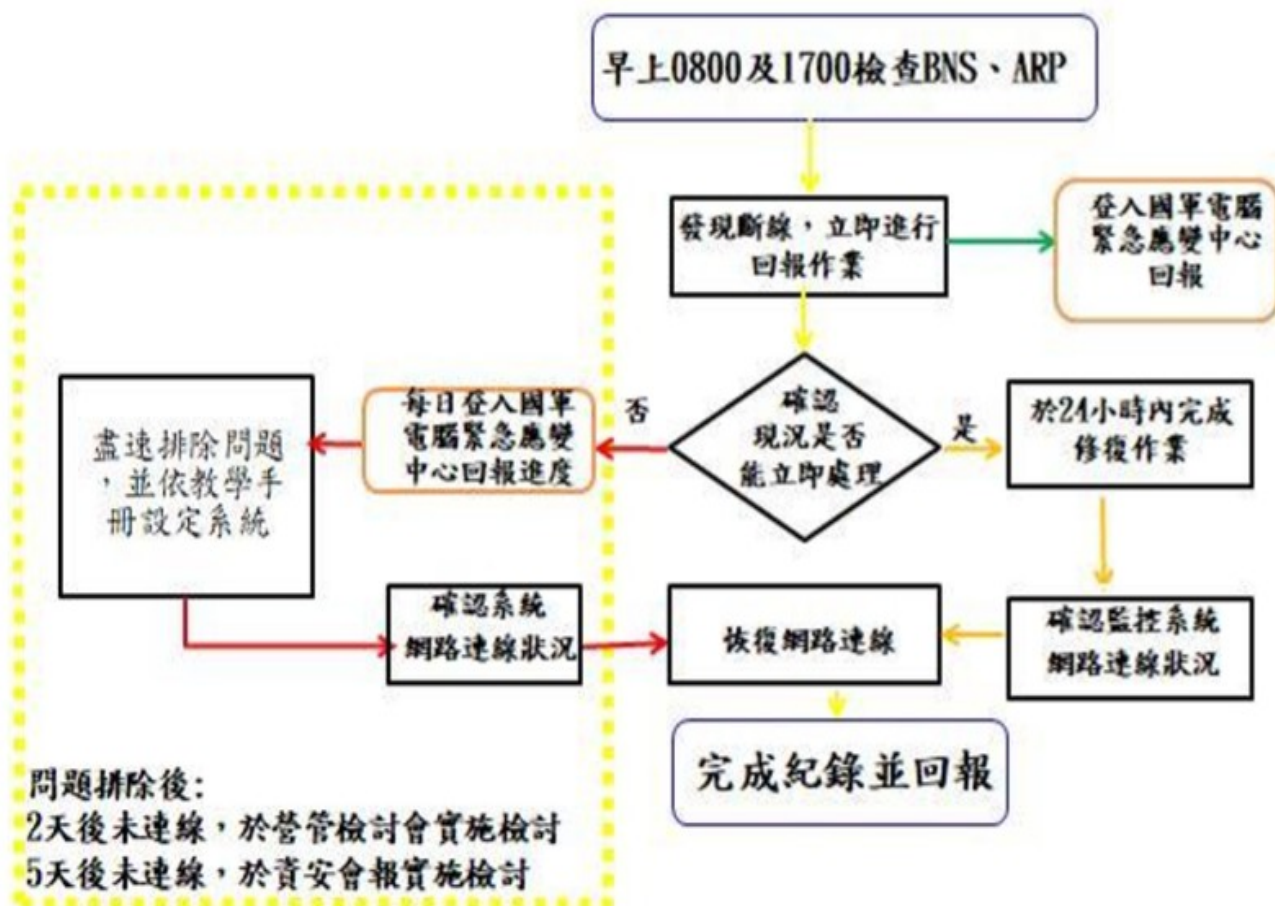
### 四、用途碼

設備用途區別，本欄位由各單位依實際需求擴增，惟不得變更原已賦予之編碼代號。

用途別	編碼
個人電腦 (Personal Computer)	W
資 訊 伺 服 器 ( Application Server)	A
網路印表機 (Network Printer)	P
防火牆 (Firewall)	F
交換器 (Switch)	S
路由器 (Router)	R



## 附件十二 「BNS」斷線處置流程



# 附件十三 連接軍網設備 IP 申請單

連接軍網設備 IP 申請單		編號：
以下由設備使用(保管)人自行填寫		主官(管)核示
申請日期	年 月 日	
單位		
級職		
姓名		
連絡電話	(軍) (自)	
設備類別	<input type="checkbox"/> 個人電腦(含筆記型電腦) <input type="checkbox"/> 伺服器 <input type="checkbox"/> 印表機 <input type="checkbox"/> 網路設備 <input type="checkbox"/> 其它 _____	審查意見
MAC 位址	- - - - -	申請單位
申請用途	<input type="checkbox"/> 辦公室作業 <input type="checkbox"/> 系統開發 <input type="checkbox"/> 測試環境 <input type="checkbox"/> 網路管理 <input type="checkbox"/> 伺服器 _____ <input type="checkbox"/> 其它 _____	
起迄時間	起:_____ 迄:_____	
以下由資訊業管部門填寫，並登錄「BNS」		
電腦名稱		
I P 位址		
登錄日期	年 月 日	
注意事項	1. 處理程序：申請人(保管人)填寫申請資料→資訊業管填寫審查意見→呈單位主管批核→資訊業管登錄於「國防部「BNS」」→備查。 2. 申請人(保管人)對申請設備負有全權保管之責，若因保管、使用不當而衍生資安事件，依相關規定辦理懲處。 3. 管理人員應配合人員、節點設備異動，辦理新增、刪除作業，以維護正確、安全作業環境。 4. 電腦設備，請立即安裝國軍集控式防毒系統、移動式媒體管理軟體暨軟體更新用戶端程式，以確保電腦作業安全。 5. 個人端公務電腦均應加入國防部網域目錄服務管控，請確依規定辦理。	

# 附件十四 「BNS」管理帳號申請單

「BNS」帳號申請單		
以下由申請人填寫		主官(管)核示
日期	年      月      日	
單位		
級職		
姓名		
連絡電話	(軍)                      (自)	
Webmail		
申請帳號	_____ <input type="checkbox"/> 網域: _____ —	
申請 IP 位址		系統管理單位
系統角色	<input type="checkbox"/> 一般使用者 <input type="checkbox"/> 系統管理者	
權限	<input type="checkbox"/> 查詢 <input type="checkbox"/> 完整	
管理範圍	<input type="checkbox"/> 領域 <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> 完整	申請人
備註	1. 處理程序：申請人填寫申請資料→呈單位主官(管)批核→函送系統管理單位→新增(異動)帳號→備查。 2. 申請人(保管人)對申請帳號負有全權保管之責，若因保管、使用不當而衍生資安事件，依相關規定辦理懲處。 3. 業管人員異動，請確實函送系統管理單位辦理帳號變更。	

# 附件十五 防火牆連接架構示意圖暨說明

防火牆各種模式架構示意及說明圖		
透通模式(Transparent mode) 橋接模式(Bridge Mode)	路由模式 (Routed mode)	網址轉換模式 (NAT Mode)
<p>特徵說明： 建置防火牆時無須變更網路架構，防火牆如同透明設備一般，且防火牆與路由器對接之介面無IP位址。</p>	<p>特徵說明： 建置防火牆時須變更網路架構，防火牆與路由器對接之介面有IP位址，防火牆須設定路由功能。</p>	<p>特徵說明： 建置防火牆時須變更網路架構，防火牆與路由器對接之介面有IP位址，防火牆須設定路由功能，且有內部IP位址轉換成外部IP位址之對應關係設定。</p>
<p>外部路由器 10.1.1.1/30 防火牆 無IP位址 無IP位址 內部路由器 10.1.1.2/30</p>	<p>外部路由器 10.1.1.1/30 防火牆 10.1.1.2/30 10.1.1.5/30 內部路由器 10.1.1.6/30</p>	<p>外部路由器 10.1.1.1/30 防火牆 10.1.1.2/30 10.1.1.5/30 內部路由器 10.1.1.6/30</p>

## 附件十六 防火牆規則變更申請單

異動	事由	連線來源地(Source)			連線目的地(Destination)			服務埠口(port)	動作	生效日期	中止日期	備考
		區域	單位	IP 或網段	區域	單位	IP 或網段					
<input type="checkbox"/> 新增 <input type="checkbox"/> 修訂 <input type="checkbox"/> 刪除				<input type="checkbox"/> IP: <input type="checkbox"/> 網段: <input type="checkbox"/> 群組:			<input type="checkbox"/> IP: <input type="checkbox"/> 網段: <input type="checkbox"/> 群組:		<input type="checkbox"/> 允許 <input type="checkbox"/> 不允許 <input type="checkbox"/> 紀錄			
<input type="checkbox"/> 新增 <input type="checkbox"/> 修訂 <input type="checkbox"/> 刪除				<input type="checkbox"/> IP: <input type="checkbox"/> 網段: <input type="checkbox"/> 群組:			<input type="checkbox"/> IP: <input type="checkbox"/> 網段: <input type="checkbox"/> 群組:		<input type="checkbox"/> 允許 <input type="checkbox"/> 不允許 <input type="checkbox"/> 紀錄			
<input type="checkbox"/> 新增 <input type="checkbox"/> 修訂 <input type="checkbox"/> 刪除				<input type="checkbox"/> IP: <input type="checkbox"/> 網段: <input type="checkbox"/> 群組:			<input type="checkbox"/> IP: <input type="checkbox"/> 網段: <input type="checkbox"/> 群組:		<input type="checkbox"/> 允許 <input type="checkbox"/> 不允許 <input type="checkbox"/> 紀錄			
申請單位			防火牆政策人員(審查)				防火牆管理人員(執行)					