後備指揮部雇二等電子資料作業員「一般測驗」題庫

1. 網際網路專用之「防護型隨身碟」機身以何種顏色標示？
○(1)紅色 ○(2)綠色 ○(3)藍色 ●(4)黃色

2. 未經核准攜帶私人電腦(含週邊設備)及資訊儲存媒體入營，經查屬實者，軍(士)官及聘雇人員處以？
○(1)警告 ●(2)申誡 ○(3)記過 ○(4)記大過

3. 下列何者不是災變預防作為？
●(1)資料刪除 ○(2)熟知緊急措施及程序 ○(3)緊急事件處理人員訓練 ○(4)系統備份

4. 個人電腦於攜出前應由何部門實施稽查？
○(1)保防 ○(2)政戰 ●(3)通資 ○(4)值日官

5. 單位肇生資安事件應向何者回報？
○(1)MSOC ●(2)MCERT ○(3)ACA ○(4)KERBEROS

6. 個人電腦連結網際網路使用上網功能時，需注意哪些資安事項？
○(1)不開啟來路不明之電子郵件 ○(2)不任意造訪不熟悉之網站 ○(3)取消電子郵件預覽窗格功能 ●(4)以上皆是

7. 個人電腦應安裝哪個資安管控軟體，何者為非？
○(1)移動式媒體管控軟體 ○(2)檔案加解密軟體 ○(3)防毒軟體 ●(4)修補軟體

8. 各類型網路（軍、民網路）之使用下列何者為非？
○(1)不得跨接 ○(2)不得混用 ○(3)網路線須以顏色區別 ●(4)可裝置切換開關以節省螢幕購置費用

9. 各單位應建置或以任務編組設置資安官，在何者指導下，負責資安教育訓練、稽核、回報及管控資安事件？
○(1)資訊安全督導官 ●(2)資訊安全長 ○(3)保密軍官 ○(4)單位主官

10. 各單位使用資訊設備及儲存媒體，執行資料輸出（入）作業時，由單位（資訊）管理人員協助於何區執行掃毒作業後載入運用？
○(1)「國軍網路使用區」（軍網使用區）○(2)「網際網路使用區」（民網使用區）●(3)「資料交換檢疫區」（交換檢疫區） ○(4)機敏作業區

11. 連接全球網際網路（Internet）及學術網路之通資設備、電腦嚴禁用於？
○(1)處理單位業務 ○(2)儲存分類保密資料 ○(3)公務資料交換 ●(4)以上皆是

12. 避免病毒傳播，最直接的方式為何？
○(1)每天擦拭電腦 ○(2)勤於更換密碼 ○(3)定期備份 ●(4)每日更新防毒軟體病毒碼

13. 單位肇生資安違規需於多久以內完成通報？
○(1)30 分鐘 ○(2)1 小時 ○(3)12 小時 ●(4)24 小時

14. 關掉不必要網路服務，可避免遭受？
○(1)猜測通行碼攻擊 ●(2)系統弱點攻擊 ○(3)網路竊聽攻擊 ○(4)以上皆非

15. 公務用可攜式電腦如因任務需要使用國軍網路，於簽奉權責長官核准後？

●(1)可使用固定 IP 上網 ○(2)可使用內建無線網卡上網 ○(3)可直接以撥接式網路上網 ○(4)以上皆是

16. 電腦網路稽核項目有？
○(1)固定 IP? ○(2)集控軟體派送 ○(3)網域控管 ●(4)以上皆是

17. 國軍資訊安全保密工作之強化，係植基於？
○(1)嚴格管制措施 ●(2)資訊安全保密教育推廣 ○(3)先進資安設備 ○(4)以上皆非

18. 當收到一封確認帳號的信件時該如何做？
○(1)連到信件內說明的網站去確認 ○(2)打信件內說明的聯絡電話去確認 ●(3)自行查詢聯絡資料去確認 ○(4)回信確認

19. 伺服器主機帳號之密碼設定須符合複雜度要求並不得少於幾個字元？
●(1)12 ○(2)10 ○(3)8 ○(4)6

20. 公務資料攜出營區外，使用私人或家中電腦，以致一般公務機密（含）以上資訊外洩者，軍(士)官及聘雇人員應處以？
○(1)警告 ○(2)申誡 ○(3)記過 ●(4)記大過

21. 單位可將業務資料、檔案、文件、圖像運用何種軟體實施加密？
○(1)OFFICESCAN ○(2)防毒軟體 ●(3)國軍檔案加解密軟體 ○(4)KERBEROS

22. 「資訊安全政策」策略包含？
○(1)建立資安風險管控機制 ○(2)各單位依據 CNS27001 國家標準，建立資訊安全管理制度 ○(3)各單位須依據 PDCA 循環模式，以管控資安風險 ●(4)以上皆是

23. 防堵垃圾郵件作為有哪些？
○(1)不回覆、不轉寄垃圾（串接）郵件 ○(2)轉寄信件應刪除原寄件人資料 ○(3)不將郵件帳號公開於部落格、網路論壇、留言板等 ●(4)以上皆是

24. 未依規定安裝「KERBEROS 偵測軟體」或「國軍檔案加解密軟體」者，軍(士)官及聘雇人員應處以？
○(1)警告 ●(2)申誡 ○(3)記過 ○(4)記大過

25. 凡連接國軍網路（民網）之電腦須採下列何種措施管理？
○(1)實體隔離 ○(2)安全密碼 ○(3)加入網域控管 ●(4)以上皆是

26. 資料不得被未經授權之個人、實體或程序所取得或揭露之特性為？
○(1)機密性 ○(2)完整性 ○(3)可用性 ●(4)不可否認性

27. 民網交換資料至軍網流程，以下何者有誤？
●(1)民網下載媒體資料，直接上傳至軍網掃毒，避免電腦病毒感染 ○(2)經「交換檢疫區」由專人進行病毒及後門程式篩檢，確保資料安全 ○(3)檢疫後方可於「軍網使用區」將公用媒體內資料轉存於軍網電腦上 ○(4)申請民網專用儲存媒體存放下載之資料

28. 保護資訊和處理方法的準確性和完整性之特性為？
○(1)機密性 ●(2)完整性 ○(3)可用性 ○(4)不可否認性

29. 關於個人民用通信資訊器材(手機)下列何者正確？

●(1)不可連接營內電腦充電 ○(2)申請核可後，即可攜入禁制區 ○(3)可於個人民用手機編輯、處理及儲存公務資料或密級以上資訊 ○(4)可攜入禁制區，只要不使用即可

30. 風險評鑑流程包含？
○(1)資產確認與評價 ○(2)確認威脅與脆弱性 ○(3)選擇風險處理方法 ●(4)以上皆是

31. 可攜式電腦使用管制，何者敘述為非？
○(1)營區內私人可攜式電腦嚴禁以各種方式連接國軍網路或民網 ○(2)公務用之可攜式電腦須將內建無線傳輸功能關閉停用，並嚴禁利用各種方式連接民網 ○(3)公務用可攜式電腦應區分管理者與使用者權限，一般人員僅能以使用者權限登入? ●(4)公務用筆記型電腦暫存之所有公務資料始用國軍檔案加解密軟體加密儲存，歸還無須刪除資料

32. 各單位於辦理資訊資產採購、租賃及維（修）護作業時，應確遵部頒何項規定辦理?
○(1)國軍網路管理作業規定 ●(2)國軍辦理涉及大陸地區財物或勞務採購注意事項 ○(3)國軍網頁式電子郵件系統管理作業規定 ○(4)政府機關密碼統合辦法

33. 公務用電腦應拆除其內裝之軟碟機及燒錄器，並將摘除零附件繳交何部門管制?
○(1)使用部門 ●(2)通資部門 ○(3)主計部門 ○(4)政戰部門

34. 保密督導官對於「隨身碟」管制，何者有誤？
○(1)每日下班前應實施清點 ○(2)逐一檢查移動式資訊儲存媒體內有無留存檔案資料（包含隱藏惡意程式） ○(3)資訊儲存媒體使用完畢後，保密督導官應要求使用者，嚴格執行刪除媒體內所有檔案並完成格式化作業，再提供次日使用 ●(4)可交由使用者自行保管

35. 保密督導官定期稽查資訊儲存媒體項目有哪些？
○(1)數量 ○(2)儲存內容 ○(3)使用記錄 ●(4)以上皆是

36. 「防護型隨身碟」的功能有？
○(1)電腦辨識碼認證 ○(2)檔案生命週期機制 ○(3)檔案加解密機制 ●(4)以上皆是

37. 有關威脅的區分，何者為非？
○(1)不可抗具因素(如地震) ○(2)人為錯誤(如資料輸入錯誤) ○(3)惡意行動(如駭客入侵) ●(4)資產特性(如裝備可攜帶性)

38. 「密級」（含）以上或「重要公務」資料，應如何加密儲存？
○(1)WINRAR ●(2)國軍電腦檔案加解密軟體（V2.0 以上版本） ○(3)EFS ○(4)WINZIP

39. 風險評鑑方法特性以下何者為非？
○(1)可比較性 ○(2)可量化 ○(3)可再產生性 ●(4)以上皆是

40. 網路對外連接點加設何種軟體以防制自外部的病毒入侵？
●(1)病毒掃描機制 ○(2)入侵偵測機制 ○(3)弱點掃描機制 ○(4)防火牆

41. 作業場所保密裝備(密體)，多久清點一次？
●(1)每日 ○(2)每週 ○(3)每月 ○(4)每半年

42. 經軟體廠商合法授權,經認證為真品,廠商會發行證明與支援的軟體叫做？
●(1)合法軟體 ○(2)作業系統 ○(3)智慧財產權 ○(4)資源分享

43. 移動式儲存媒體視同械彈管制，由單位保密督導官負責集中保管，依任務需要申請使用，並於幾日內歸還？
○(1)1 日 ○(2)2 日 ○(3)3 日 ●(4)當日

44. 嚴禁於何種時機未經核准使用民用通信資訊器材？
○(1)部隊演訓操課 ○(2)執行戰情、衛哨勤務期間 ○(3)機敏會議 ●(4)以上皆是

45. 公務電腦機殼接縫處，應黏貼何種標籤？
●(1)易碎標籤 ○(2)統一識別管制標誌 ○(3)網際網路管制標籤 ○(4)無需任何標示

46. 公務用可攜式電腦等資訊資產攜出營區期間由何人負安全責任？
○(1)資訊官 ○(2)保管人 ○(3)單位主官 ●(4)借用人

47. 密碼作業(保管、操作)人員及其職務代理人，安全調查時機為何？
○(1)每月 ●(2)每季 ○(3)每半年 ○(4)每年

48. 關於保密裝備下列何者有誤？
○(1)須通過國安局鑑測 ○(2)保密裝備作業場所需每日實施清點 ○(3)業管人員須完成安全調查 ●(4)為利方便可將未清點之保密裝備以托運方式運送

49. 召開機敏會議時，與會人員民用通信資訊器材管制作為為何？
○(1)不管制 ●(2)統一放置於會場外置物櫃內 ○(3)非智慧型手機即可攜入 ○(4)得以攜入但需關機或靜音

50. 核准防護型隨身碟使用之管制冊及申請表等資料應詳實記錄及保存多久，併各設備列入各級資訊及保密督檢項目備查？
○(1)一季 ○(2)半年 ○(3)一個月 ●(4)三年

51. 肇生資安事件時蓄意對涉案資訊設備刪除檔案、格式化儲存設備或破壞者，應核予何種處分？
○(1)資安違規講習 ○(2)申誡 ○(3)記過 ●(4)記大過

52. 未經核准安裝、使用資訊設備、儲存媒體，應核予何種處分？
○(1)資安違規講習 ●(2)申誡 ○(3)記過 ○(4)記大過

53. 保密裝備應於哪個系統建立帳籍資料？
●(1)國軍保密裝備管理系統 ○(2)國軍資訊資產管理系統 ○(3)國軍財產管理資訊系統 ○(4)物品管理資訊系統

54. 肇生資安事件未於規定時限內通報者，應核予何種處分？
○(1)資安違規講習 ●(2)申誡 ○(3)記過 ○(4)記大過

55. 個人電腦的那些輸出入埠需要黏貼易碎標籤？
○(1)PS2 埠 ○(2)音源埠 ●(3)RS232 埠 ○(4)D-SUB 埠

56. 國軍電腦緊急應變流程之通報方式何者為是？
○(1)無線電通知 ○(2)實體書信通知 ●(3)電話及 CERT 網頁通報 ○(4)情況不嚴重的話自行處置即可，無需通報

57. 一般個人行政電腦資安管控下列何者為是？
○(1)拆除燒錄器、軟碟機 ○(2)USB 連接埠封閉並貼上易碎標籤 ○(3)RS232 連接埠、

印表機連接埠及機殼接縫處貼上易碎管制標籤 ●(4)以上皆是

58. 以影響.com 及.exe 兩種檔案為主之電腦病毒為何種型態病毒？
○(1)開機型 ●(2)檔案型 ○(3)複合型 ○(4)突變型

59. 建置反情報稽核、防禦、網路系統，對提升反情報作業工作及實體安全防護，著有貢獻者，予以獎勵為何？
●(1)記大功 ○(2)嘉獎 ○(3)口頭嘉勉 ○(4)記功

60. 未採實體隔離作業（網際網路、學術網路與國軍資訊網路、戰情及情傳等網路相互搭接、混用或與國軍各通資系統設備共用主機，或裝置切換設備者），軍(士)官及聘雇人員應予何種處份？
○(1)警告 ○(2)記過 ●(3)記大過 ○(4)資安違規講習

61. 申請私人民用手機進入營區時，應填製何種表格？
●(1)國軍營內民用通信資訊器材申請異動單 ○(2)無線電通信機通信聯絡圖 ○(3)民用無線電通信機採購申請單 ○(4)資訊網路圖

62. 未經核准於禁制區攜帶或使用民用通信資訊器材、各類公(私)務資訊資產籍資訊儲存媒體，懲處為何？
○(1)口頭警告 ○(2)申誡 ○(3)記過 ●(4)記大過

63. 下列何者違反資訊安全規定？
○(1)密級（含以上）資料傳送未加密 ○(2)開放使用「資源分享」功能 ○(3)民網電腦內儲存一般公務資料 ●(4)以上皆是

64. 網路安全面臨的威脅中以何者最為嚴重？
○(1)實體損害 ○(2)自然災害 ●(3)人 ○(4)以上皆非

65. 易碎標籤不應貼於下列何處？
○(1)RS232 埠 ●(2)印表機機身 ○(3)電腦機殼接縫 ○(4)鍵盤接縫處?

66. 「一級督導一級」輔導方式為何？
○(1)親自教導 ○(2)現地輔導 ○(3)電話（電子郵件）指導 ●(4)以上皆是

67. 下列哪一項是國軍依據資安政策推的管理活動？
○(1)四階文件 ○(2)風險評鑑 ○(3)內部稽核 ●(4)以上皆是

68. 國軍行政網使用之資訊資產應張貼何種顏色識別標籤？
●(1)綠色 ○(2)黃色 ○(3)紅色 ○(4)不須張貼

69. 要將數位相機資料下載應？
○(1)使用自己的電腦下載 ○(2)使用民網專用電腦下載 ●(3)奉權責長官核定後使用檢疫電腦下載 ○(4)由軍網單一輸出入口輸出

70. 演訓專用之移動式資訊儲存媒體須以何種顏色標籤區分？
●(1)紅色 ○(2)黃色 ○(3)藍色 ○(4)綠色

71. 傳送機密資訊未採取加密措施者(如演習期間參演人員使用演訓用電子郵件系統寄送演習情資未加密簽證)，軍(士)官及聘雇人員處以？
○(1)警告 ●(2)記過 ○(3)申誡 ○(4)資安違規講習

72. 國軍規範燒錄器及軟碟機使用作法何者為非？
●(1)摘除燒錄器及軟碟機由保防部門管制 ○(2)公務用電腦應拆除軟碟機及燒錄器 ○(3)外接式燒錄器由保密督導官存管 ○(4)新購電腦不得配置軟碟機及燒錄器

73. 何者屬於移動式儲存媒體？
○(1)外接式硬碟 ○(2)記憶卡 ○(3)數位相機 ●(4)以上皆是

74. 領用公用儲存媒體，繳回時未依規定將資料清除，資料內容如屬密級之一般公務機密資料，軍(士)官及聘雇人員處以？
○(1)記大過 ○(2)申誡 ●(3)記過 ○(4)資安違規講習

75. 國軍人員於下列何種時機，各單位應施予資訊安全教育訓練？
○(1)新進 ○(2)離退 ○(3)因公出國 ●(4)以上皆是?

76. 一般使用者之密碼長度設定至少為幾位元？
○(1)7 ●(2)8 ○(3)9 ○(4)10 個位元，並且符合「複雜性」需求

77. 網路防護的手段何者為非？
○(1)防毒軟、硬體 ○(2)防火牆 ●(3)資源分享 ○(4)漏洞修補程式

78. 隨書或研討會附贈唯讀光碟等儲存媒體，併同書籍（會議資料）如何管制？
○(1)黏貼管制標籤 ●(2)統一造冊管控 ○(3)交由保密軍官保管 ○(4)承辦人保管

79. 具讀取記憶卡功能列表機管制作法為何？
○(1)允許運用列表機之讀卡功能使用記憶卡儲存/讀取資料 ○(2)直接破壞記憶卡插槽 ●(3)禁止運用列表機之讀卡功能使用記憶卡儲存/讀取資料 ○(4)以矽膠封住記憶卡插槽

80. 資料使用移動式儲存媒體交換時機為何？
○(1)基於業務需要，隨時皆可交換資料 ○(2)隨時隨地皆可 ○(3)視個人需求而定 ●(4)基於業務需要，且無法以電子郵件交換資料時

81. 伺服器應如何設定密碼？
○(1)文數字 ○(2)英文字大小寫 ○(3)特殊符號 ●(4)以上混合

82. 嚴禁使用私人通信資訊器材編輯、處理及儲存公務資料或密級（含）以上資訊，不得與公用資訊設備及國軍何種網路搭接進行資料交換、傳輸或充電等行為？
○(1)軍網 ○(2)內網 ○(3)機敏網路 ●(4)以上皆是

83. 公務用電腦應拆除其內裝之燒錄器，外接式燒錄器比照隨身碟由何人存管?
○(1)保防部門保密軍官 ○(2)單位保密軍官 ●(3)保密督導官 ○(4)監察部門保密軍官

84. 伺服器及個人電腦上均應加裝何種軟體並定期更新，以有效防治電腦病毒之攻擊？
○(1)防火牆 ○(2)密碼 ○(3)螢幕保護程式 ●(4)防毒軟體

85. 在收件匣內發現有可疑的郵件時，應該執行什麼動作？
○(1)直接開啟瀏覽 ●(2)直接刪除 ○(3)轉寄給別人 ○(4)以上皆是

86. 資訊媒體（設備）進出放行申請表須由何者簽證或查核？
○(1)保防安全部門 ○(2)通資部門 ○(3)單位主官 ●(4)以上皆是

87. 網路防護的手段何者為非？

○(1)入侵偵測軟體 ○(2)防火牆 ●(3)開啟不明的信件 ○(4)防毒軟、硬體

88. 網路對外連接點加設何種軟體以防制自外部的病毒入侵？
●(1)病毒掃描機制 ○(2)入侵偵測機制 ○(3)弱點掃描機制 ○(4)防火牆

89. 如何預防電腦病毒？
○(1)不使用不明軟體 ○(2)安裝防毒軟體 ○(3)不開啟來源不明的信件 ●(4)以上皆是

90. 如何檢查防毒軟體病毒碼更新版本？
○(1)紀錄於個人隨身 PDA 中，手動輸入但可自動化管理 ○(2)紀錄於個人隨身筆記本中，手動輸入並需人工管理 ●(3)直接開啟防毒軟體，檢視紀錄檔版本日期 ○(4)打電話問系統管理員

91. 國軍行政網(Minet)專用之「防護型隨身碟」機身以何種顏色標示？
○(1)紅色 ●(2)綠色 ○(3)藍色 ○(4)黃色

92. 如何防範網路釣魚？
○(1)取消預覽功能 ○(2)主動聯繫確認郵件來源 ○(3)可疑檔案切勿點擊 ●(4)以上皆是

93. 電腦緊急應變通報通資安全事件等級共分為？
○(1)一類 ○(2)二類 ○(3)三類 ●(4)四類

94. 如果想把電子郵件寄送給許多人，卻又不想讓收件者彼此之間知道你寄給哪些人，可以哪項功能做到？
○(1)副本 ○(2)收件人 ●(3)密件副本 ○(4)加密

95. 專案（機敏）系統用電腦及移動式儲存媒體，黏貼何色「管制標籤」？
●(1)紅色 ○(2)綠色 ○(3)藍色 ○(4)黃色

96. 「個人電腦輸出(入)裝置使用管制規定」內規定管制之項目不包含？
○(1)USB 埠 ●(2)音源埠 ○(3)RS-232 埠 ○(4)燒錄機

97. 數位相機照片交換需？
○(1)透過民網交換 ●(2)透過檢疫區交換 ○(3)透過駭客交換 ○(4)直接插入軍網電腦使用

98. 上網時出現「需要下載安裝軟體才能檢視此網頁」，這是什麼情形？
○(1)網頁內含有動畫顯示 ○(2)網頁內含有即時更新畫面 ○(3)網頁內含有後門程式 ●(4)以上皆是

99. 為有效反制來自內部及外部的入侵行為，資訊系統應加設？
○(1)防火牆 ○(2)入侵偵測機制 ○(3)內部網路安全掃描程式 ●(4)以上皆是

100. 何者不是電腦使用者離開座位時，應對所使用之電腦所作之防護動作？
○(1)隨手關閉使用中之應用程式 ○(2)登出系統 ●(3)直接離開座位，不做任何動作 ○(4)啟動螢幕保護機制並加設密碼

101. 國軍移動式儲存媒體管制作為，何者為非?
●(1)相機內之照片因業務需求可暫存幾天 ○(2)依規定每日清點，由資安官負保管之責 ○(3)民網用隨身碟不可存放機敏資料 ○(4)借用限當日歸還

102. 電腦等配賦管制品項，須呈報何單位審核後，始可以集中辦購方式辦理採購？
●(1)管理機關 ○(2)司令部 ○(3)軍團、防衛部 ○(4)各單位主官

103. 印表機等電腦周邊設備，須呈報何單位審核後，始可由申購單位辦理採購？
○(1)國防部 ○(2)司令部 ●(3)管理機關 ○(4)各單位主官

104. 針對違反實體隔離規定之人員嚴予懲處，其罰則為何？
○(1)記大過 ○(2)調離現職 ○(3)洩密者依法偵辦 ●(4)以上皆是

105. 下載至資訊儲存媒體資料，應先於單機隔離電腦─即所謂？
●(1)交換檢疫區 ○(2)軍網使用區 ○(3)民網使用區 ○(4)以上皆非，並由專人進行病毒及後門程式篩檢，確保資料安全

106. 何者不是預防電腦病毒的手段？
○(1)安裝防毒軟體 ○(2)不開啟來源不明的信件 ●(3)使用大補帖光碟 ○(4)不隨意下載小遊戲及美女圖

107. 何者不是網路系統被入侵之原因？
○(1)不重視安全性，沒有保護措施 ○(2)系統程式有問題 ○(3)惡意的員工 ●(4)網路線沒插好

108. 下列何種惡意程式會將受害者檔案加密，並由攻擊者向受害者要求繳納贖金？
●(1)勒索病毒 ○(2)後門程式 ○(3)特洛依木馬 ○(4)電腦蠕蟲

109. 何者不屬於網路攻擊的手段？
●(1)感冒病毒 ○(2)變種病毒 ○(3)電腦病毒 ○(4)後門程式

110. 電腦緊急應變處理（CERT）管制範圍？
○(1)國軍網路 ○(2)指管網路 ○(3)學術網路 ●(4)以上皆是

111. 下列何種是防毒軟體病毒碼的更新最佳方案？
○(1)手動每月 1 次 ○(2)手動每週 1 次 ●(3)設定自動更新 ○(4)安裝後即無需更新

112. 何者是國軍電腦緊急應變處理（CERT)管制範圍？
○(1)國軍行政網 ○(2)國軍民網 ○(3)專屬網路 ●(4)以上皆是

113. 何者不是資訊安全防範的範圍？
○(1)駭客入侵 ○(2)電腦病毒 ●(3)天氣變化 ○(4)人為疏失

114. 下列何者違反資訊安全作業規定？
○(1)在網路散播或公開違反善良風俗之暴力、色情、猥褻、詐欺 ○(2)詆毀個人或單位名譽等相關文字、圖片、聲音、影像等 ○(3)不當之違反內部管理或軍紀要求的資訊 ●(4)以上皆是

115. 攜帶私人資訊儲存媒體應受何處分？
○(1)記大過 ○(2)勒令退伍 ○(3)罰站 ●(4)申誡

116. 下列何者是防範電腦中毒的原則？
○(1)安裝一套盜版的防毒軟體，不需更新病毒碼 ●(2)不使用盜版或來路不明的軟體 ○(3)開啟電子郵件軟體的預覽郵件功能 ○(4)在公共電腦用過的儲存媒體直接與辦公室電腦連接

117. 何者不是國軍電腦作業環境？
●(1)士兵作業區 ○(2)一般作業區 ○(3)機敏作業區 ○(4)民網專區

118. 採購筆記型電腦，應要求供應商於驗收前將何種功能移除？
○(1)鍵盤 ●(2)內建無線網路 ○(3)螢幕 ○(4)觸控板

119. 何者不是防毒軟體設計方式？
○(1)掃描式 ○(2)檢查碼式 ●(3)自由式 ○(4)推測病毒行為模式

120. 電子公文附件應採用何種檔案格式為優先？
○(1)Word ○(2)Excel ●(3)ODF ○(4)RAR

121. 為確保網路安全，應配合使用何種功能設備以有效防止備份資料遭到竊取與竄改？
○(1)加密 ○(2)解密 ●(3)加解密 ○(4)以上皆非

122. 機敏網路專用之「防護型隨身碟」機身以何種顏色標示？
●(1)紅色 ○(2)綠色 ○(3)藍色 ○(4)黃色

123. 何者為「國軍資訊安全政策」之國軍執行資安防護主要目的？
○(1)防止駭客入侵 ○(2)防堵病毒事件 ○(3)防止資料遭竊 ●(4)以上皆是

124. 何者係指未經軟體廠商合法授權，即持有或使用之軟體？
○(1)免費軟體 ○(2)合法軟體 ○(3)共享軟體 ●(4)非法軟體

125. 何者係指具有版權，且使用者不必付費即可使用，還能任意複製的軟體？
●(1)免費軟體 ○(2)合法軟體 ○(3)商用軟體 ○(4)非法軟體

126. 國軍內網可使用何種軟體協助實施資安設定檢查？
●(1)資安小幫手 ○(2)資安大補帖 ○(3)資安破解光碟 ○(4)資安小蝦米

127. 合約廠商（含駐點人員）進入營區須遵守何規定？
○(1)單位門禁管制 ○(2)單位資安管控作為 ○(3)單位資安稽核作業 ●(4)以上皆是

128. 可攜式儲存媒體比較容易被忽視，常見的威脅有？
○(1)病毒 ○(2)資料外洩 ○(3)遺失 ●(4)以上皆是

129. 依「國軍資通安全責任等級分級作業指導」所核定之 A、B 級國軍單位，一般使用者每人每年應接受多少小時以上之資通安全教育訓練？
○(1)一小時 ○(2)二小時 ●(3)三小時 ○(4)不用

130. 公用移動式資訊設備及儲存媒體應如何存管？
●(1)集中、專人、保密櫃 ○(2)使用者自己保管 ○(3)不須保持用完淨空 ○(4)以上皆是

131. 單位肇生 1 至 4 級事件需於多久以內完成通報？
○(1)24 小時 ○(2)3 天 ○(3)48 小時 ●(4)30 分鐘

132. 故意破壞、關閉或移除國軍行動裝置管理系統及設定或以其他技術，致國軍行動裝置管理系統於營內無法發揮應有功能，得核予下列何種懲罰？
○(1)申誡 ●(2)記過 ○(3)言詞申誡 ○(4)記大過

133. 公發可攜式電腦應確實由何者集中管控？
●(1)保密督導官或指定專人 ○(2)電腦保管人 ○(3)電腦帳籍管理人 ○(4)資產管理系統

134. 單位民網管理使用管制與稽核，下列何者為是？
●(1)瀏覽器記錄應保留 180 天以上 ○(2)保密督導官至少每季稽查乙次 ○(3)伺服器連線紀錄應保存一個月 ○(4)以上皆是

135. 民網應該使用何種顏色網路線，以利區隔？
○(1)黑色 ●(2)黃色 ○(3)彩色 ○(4)白色

136. 管制標籤因故損毀或編號模糊不易辨識時，應主動請何部門辦理原標籤註銷及重新申請黏貼？
○(1)後勤 ●(2)通資 ○(3)保防 ○(4)政戰

137. 下列何種情形得核予嘉獎獎勵？
○(1)未安裝上級規定之各類資安防護、管控軟體 ○(2)肇生資安違規或事件，未於規定時限內通報 ●(3)向單位舉發未經核准，攜帶民用通信資訊器材出入營區 ○(4)擅自安裝非統一配發、未獲授權使用之軟體系統

138. 為何電腦須使用易碎管制標籤？
○(1)避免使用非法軟體 ●(2)管制輸出入裝置 ○(3)確認為公有資產 ○(4)好看

139. 國軍資訊通信及電子戰機房須設置自動錄影監控系統，且紀錄須至少保留多久？
○(1)半個月 ○(2)一個月 ○(3)二個月 ●(4)三個月

140. 國軍資安政策應有幾階文件？
●(1)4 ○(2)8 ○(3)6 ○(4)以上皆非

141. 國軍資安管控機制包含那些項目？
○(1)安裝檔案加解密軟體 ○(2)安裝防毒軟體 ○(3)收回管理者權限 ●(4)以上皆是

142. 國軍個人電腦應全面拆除何裝置？
○(1)喇叭 ●(2)燒錄機 ○(3)不斷電系統 ○(4)以上皆非

143. 國軍資訊安全政策中人員離退管制，何者為非？
○(1)離職人員應儘速撤換系統通行碼 ●(2)保留離職人員電腦使用者權限 ○(3)收繳儲存媒體 ○(4)以上皆非

144. 國軍人員嚴禁作何事？
○(1)使用民網寄送電子郵件 ●(2)公務家辦 ○(3)攜帶行動電話 ○(4)使用網路交易

145. 國軍官兵違反資安規定應依何者實施檢討？
○(1)軍風紀維護實施規定 ○(2)內部管理規定 ○(3)衛哨勤務執勤規定 ●(4)國軍資訊安全獎懲基準規定

146. 國軍針對個人電腦資訊安全防護作業規定有那些？
○(1)落實實體隔離政策 ○(2)資料需分級處理 ○(3)確實執行個人電腦安全設定檢查 ●(4)以上皆是

147. 將核准攜入營內使用之民用通信資訊器材連接公務電腦充電，軍(士)官及聘雇人員應處以？
○(1)警告 ●(2)申誡 ○(3)記過 ○(4)記大過

148. 對單位內資訊保密安全，負有執行資訊安全教育、法令宣導、紀律檢肅、督導資訊

安全措施執行之責的人是？
○(1)單位主官 ●(2)保密督導官 ○(3)人事官 ○(4)作業人員

149. 電腦網路稽核項目應包含有？
○(1)是否任意開啟資源分享 ○(2)是否有更新病毒 ○(3)是否依規定設定密碼及加密 ●(4)以上皆是

150. 下列何者不是通資安全事件處理階段？
○(1)辨識階段 ●(2)備份階段 ○(3)復原階段 ○(4)追蹤階段

151. 凡連接網際網路（民網）之電腦須採下列何種措施管理？
○(1)實體隔離 ○(2)專人管理 ○(3)資料管制 ●(4)以上皆是

152. 未經核准，攜帶民用通信資訊器材出入非禁制區，當事人懲處為何？
○(1)口頭警告 ●(2)申誡 ○(3)記過 ○(4)記大過

153. 一般作業區管制作法為何？
●(1)拆除燒錄器、軟碟機→安裝 KERBEROS ○(2)拆除燒錄器、軟碟機→安裝雙網卡 ○(3)拆除燒錄器、光碟機→封閉網路埠 ○(4)拆除燒錄器、軟碟機→封閉 CRT 連接埠

154. 各單位燒錄「光碟片」，其均應黏貼各項管制標籤，除納入「資訊媒體（含筆記型電腦）管制清冊」，並統一交由單保密督導官保管「保密櫃」列入管制項目，並於何時實施清點檢查？
○(1)每週 ○(2)每月 ●(3)每日 ○(4)不用請查

155. 電腦機敏檔案存管，須以何種方式實施加密儲存，未依規定完成加密者，依「國軍資訊安全獎懲基準規定」究責？
●(1)國軍檔案加解軟體 ○(2)私人下載之自由軟體 ○(3)僅以 OFFICE 軟體 ○(4)WINRAR 軟體

156. 依國防部「國軍人事資料查核運用作業規定」，凡因「違犯保密規定」，遭記過（含）以上處分者，3 年內不得作何人事運用？
○(1)不得晉任 ○(2)向上派職、送訓 ○(3)因公出國 ●(4)以上皆是

157. 資訊設備張貼何種管制作為，以防範移動式儲存媒體非法連接電腦或機殼內零組件遭置換等情事肇生？
●(1)易碎標籤 ○(2)資訊設備管制標籤 ○(3)保密警語 ○(4)單位財產清點標籤

158. 網際網路電腦設備應？
●(1)張貼黃色管制標籤 ○(2)張貼綠色管制標籤 ○(3)可隨意安裝軟體 ○(4)不須安裝防毒軟體

159. 應使用何種方式執行軍網電腦檔案資料交換作業，並落實相關管制及檢疫作為，確保電腦檔案於安全及受監管之環境下實施交換？
○(1)私自燒錄光碟片 ●(2)專用防護型隨身碟 ○(3)一般隨身碟 ○(4)以上皆可

160. 何者非個人電腦防護項目？
●(1)使用系統預設密碼 ○(2)安裝個人防火牆 ○(3)安裝防毒軟體 ○(4)安裝螢幕保護

程式

161. 哪些東西均不得攜入（出）營區，各單位應強化門禁查察工作，以確保國軍資通安全？
○(1)未經核准之資訊設備 ○(2)未鎖定照相、藍芽等功能之行動電話 ○(3)非公務用途之業餘無線電機 ●(4)以上皆是

162. 下列何者為遭受網路服務的攻擊徵候？
●(1)使用者帳號及密碼檔案不正常更動 ○(2)正常網路服務的開啟 ○(3)鍵盤沒有作用 ○(4)滑鼠沒有作用

163. 每季配合哪個部門針對所屬電腦操作人員實施考核作業，避免不適當人員操作電腦，肇生竊（蒐）密情事？
○(1)人事部門 ●(2)保防部門 ○(3)後勤部門 ○(4)作戰部門

164. 各單位使用民網電腦，應確遵部頒「國軍民網管理作業規定」，落實何種規範？
○(1)「專機專用」 ○(2)「與軍網實體隔離」 ○(3)「嚴禁處理機敏公務」 ●(4)以上皆是

165. 於機敏網路平台違反管制規定使用資訊設備及媒體，致造成資安事件者，當事人應予何種處分？
○(1)禁足乙天 ○(2)申誡乙次至兩次 ○(3)記過乙次 ●(4)大過乙次

166. 密級之一般公務機密資訊未採取對應等級以上之加密系統(軟體)或保密裝備實施傳輸者當事人懲處為何？
○(1)口頭警告 ●(2)申誡 ○(3)記過 ○(4)記大過

167. 依連接軍網個人電腦資安管控機制檢查項目（實體安全）以下何者為非？
○(1)電腦張貼資訊設備管制標籤 ●(2)電腦可裝設雙網卡 ○(3)未與民網電腦共用印表機 ○(4)電腦機殼與機身接縫張貼易碎封條

168. 各類型電腦應確實完成各項安全設定，並依更新期程完成何種作業，避免危害國軍資訊安全？
○(1)系統漏洞修補 ○(2)病毒碼更新 ○(3)以上皆非 ●(4)以上皆是

169. 禁止使用軍網電子郵件系統執行何種行為？
○(1)傳遞非公務資料 ○(2)任意開啟或下載軍、民網路中來源不明之郵件及其附檔 ○(3)分享非授權軟體 ●(4)以上皆是

170. 以下何者為非？
●(1)可自行將儲存媒體攜出營區於坊間使用，無須奉權責長官核定 ○(2)將儲存媒體攜出營區於坊間使用，易遭病毒染感 ○(3)移動式儲存媒體用畢後需執行格式化 ○(4)病毒可能經由檢疫交換程序間接滲入軍網，造成資安潛在風險

171. 人員離退時應確實完成交接，軍網電腦內資料應如何存管？
●(1)舊有檔案非必要留存應檢整移除 ○(2)舊有檔案直接全數留用 ○(3)可以安裝私人軟體 ○(4)可將非公務資料留存電腦內

172. 資料使用移動式儲存媒體交換時機為何？

○(1)基於業務需要，隨時接可交換資料 ●(2)基於業務需要，且無法以電子郵件交換資料時 ○(3)隨時隨地皆可 ○(4)視個人需求而定

173. 國軍各級人員不得利用全球資訊網私自架設聊天室、個人網站與部落格(Blog)討論軍中事務，尤其不應論及何種公務，違反者依相關規定論處？
○(1)單位駐地變更 ○(2)人事調整 ○(3)職務異動 ●(4)以上皆是

174. 國軍各級作業人員不得藉公務之便，使用國軍民網電腦或透過民網網站連結何種不當網站？
○(1)情色網站 ○(2)交友網站 ○(3)賭博網站 ●(4)以上皆是

175. 有關單位「燒錄器」管制，下列何者正確?
○(1)可使用複寫式光碟燒錄 ○(2)應使用內接式燒錄器燒錄 ○(3)申請完備後可於個人行政電腦燒錄使用 ●(4)燒錄後之光碟須黏貼資訊媒體管制標籤

176. 「資訊資產攜出入營區三聯單」計分三聯，下列何者正確？
●(1)第一聯衛兵查驗後交保防部門稽查 ○(2)第二聯交軍事安全部門存查 ○(3)第二、三聯併同資訊媒體攜行並送交衛兵司令查驗放行 ○(4)第二聯自行存管

177. 保密裝備作業專用電腦應列為何種電腦？
○(1)專案電腦 ○(2)戰情電腦 ○(3)民網電腦 ●(4)行政電腦

178. 國軍資訊通信及電子戰機房應依作業性質，設置安全防護措施，下列何者為非？
●(1)人臉辨識系統 ○(2)防盜功能門窗 ○(3)電子門禁管制系統 ○(4)監控（錄）系統

179. 保密裝備或技術須通過哪個權責單位完成鑑測作業。
○(1)軍情局 ●(2)國安局 ○(3)國防部通次室 ○(4)國安會

180. 凡個人因學習需要，攜帶私人電腦（桌上型、可攜式等）進入（出）營區者，應？
○(1)比照一般資訊設備開立出入營區三聯單 ●(2)得經權責長官核准申請管制標籤 ○(3)無管制皆可攜入 ○(4)全面禁止