資訊與系統安全知識認證
Information and System Security Knowledge Certification

(線上題庫出題率約 60%)

認證檢定說明:

每次考測檢定會有
15 題是非題, 10 題選擇題,

答對每題 4分。

總積分滿分 100 分,達 60 分以上者及格。

考試時間 40 分鐘。

資訊與系統安全知識 是非題

1. 防火牆可用來阻擋所有駭客攻擊。
   ✘ 非｜防火牆僅是防禦工具之一，無法阻擋所有攻擊。

2. 使用複雜密碼能降低帳號被破解的風險。
   ✔ 是｜長且包含大小寫、數字與符號的密碼更難被破解。

3. **HTTPS** 比 **HTTP** 更安全。
   ✔ 是｜**HTTPS** 加密資料傳輸，可防止竊聽與竄改。

4. 電子郵件中的附件一定安全。
   ✘ 非｜附件可能含惡意程式，應小心檢查來源。

5. 社交工程是指利用人性弱點進行攻擊。
   ✔ 是｜例如假冒客服、詐騙連結等。

6. 系統更新可修補已知的安全漏洞。
   ✔ 是｜更新能修復軟體弱點，避免被攻擊利用。

7. 資料備份是資安中不重要的部分。
   ✘ 非｜備份是災難發生後恢復系統的關鍵措施。

8. 只要安裝防毒軟體，就不會中毒。
   ✘ 非｜防毒軟體降低風險，但無法保證百分之百防護。

9. 公共 **Wi-Fi** 使用風險較高。
   ✔ 是｜易被中間人攻擊或攔截資料。

10. 勒索軟體會加密使用者的檔案並要求贖金。
    ✔ 是｜此類攻擊日益猖獗，常見於企業與個人電腦。

11. 多因素驗證比單一密碼登入更安全。
    ✔ 是｜需輸入第二道驗證，例如簡訊或**APP**認證。

12. 資安事件不會影響企業營運。
    ✘ 非｜資安事件可能導致資料外洩、營運中斷甚至商譽受損。

13. 使用弱密碼是企業內部常見的資安風險。
✔ 是｜如**123456**、**password** 等易遭猜測。

14. 資料加密可保護機密資訊即使落入他人手中。
✔ 是｜加密後的資料無密鑰即無法解讀。

15. 每位使用者應有專屬帳號與權限。
✔ 是｜利於管理與追蹤異常操作。

16. 開啟來源不明的電子郵件是一項高風險行為。
✔ 是｜可能導致中毒或個資外洩。

17. 資安風險僅來自外部攻擊者。
✘ 非｜內部員工的疏忽或惡意行為也是重大風險來源。

18. 關閉不必要的系統服務可降低攻擊面。
✔ 是｜減少可利用漏洞，強化防禦。

19. 駭客入侵常藉由系統漏洞與人為疏失。
✔ 是｜技術與社交工程並用是常見手法。

20. 所有網頁伺服器預設設定皆為安全狀態。
✘ 非｜預設設定可能留下安全漏洞，需檢查調整。

21. 定期更換密碼是一種良好資安習慣。
✔ 是｜可防止長期密碼遭破解或外洩。

22. 資安政策應包含使用者行為規範與稽核機制。
✔ 是｜防範內部威脅並能事後追蹤。

23. 僅需備份資料一次即可確保安全。
✘ 非｜應定期備份，並測試可還原性。

24. 釣魚網站外觀常與真實網站極為相似。
✔ 是｜誘使使用者輸入帳密或個資。

25. 使用公開雲端服務不需再考慮資安問題。
✘ 非｜雲端仍需用戶做好存取控制與加密。

26. 資訊安全只屬於 **IT** 部門責任。
✘ 非｜所有使用者都應具備資安意識。

27. 拒絕服務攻擊（**DoS**）會造成系統無法回應。
✔ 是｜使服務癱瘓，無法正常提供服務。

28. 備份資料不需要加密。
✘ 非｜備份資料亦可能外洩，應加密保存。

29. 只要系統未連網，就不會遭資安威脅。
✘ 非｜離線設備仍可能因**USB**或內部人員受害。

30. 安裝非法破解軟體會增加資安風險。
✔ 是｜常含後門程式或惡意代碼。

31. 企業應定期進行資安演練與滲透測試。
✔ 是｜可提前發現系統弱點，提升應變能力。

32. 使用公用電腦登入個人帳號是安全的。
✘ 非｜資料可能被記錄或惡意軟體竊取。

33. 安裝來路不明的手機**APP**可能造成資安風險。
✔ 是｜可能內建木馬、蒐集個資。

34. **IoT**裝置（物聯網）也可能成為資安攻擊目標。
✔ 是｜多數裝置資安防護較弱，易受攻擊。

35. 只要網站有**SSL**憑證就完全安全。
✘ 非｜**SSL**僅保障傳輸安全，不代表網站無惡意。

36. 密碼管理器能提升密碼安全與使用效率。
✔ 是｜可產生複雜密碼並安全儲存。

37. 刪除檔案後就無法復原。
✘ 非｜未經覆寫的檔案可用工具恢復。

38. 個資法（個人資料保護法）要求保護個人資訊。
✔ 是｜防止個資濫用與外洩。

39. 企業資安事故有時需依法通報主管機關。
✔ 是｜如涉及大量個資外洩，依法需通報。

40. 無線網路建議使用 **WPA2** 或更新版本的加密技術。

✔ 是｜**WEP** 已不安全，應使用 **WPA2** 或 **WPA3**。

41. 系統管理員應避免共用管理帳號。
✔ 是｜應各自使用專屬帳號，便於審計與追責。

42. 蠕蟲病毒會自動複製並擴散。
✔ 是｜與電腦病毒類似，但無需附著檔案即可散播。

43. 電子簽章可驗證檔案是否被竄改。
✔ 是｜確保文件真實性與完整性。

44. 每日登入記錄可協助偵測異常活動。
✔ 是｜分析異常登入時間與**IP**有助於早期發現入侵。

45. 僅管理階層需接受資安教育訓練。
✘ 非｜全體員工皆應培養資安意識與基本知識。

46. 掃描**QR Code**不會構成資安風險。
✘ 非｜**QR Code** 可能導向惡意網站或下載檔案。

47. 企業網站應設有安全性憑證與弱點掃描機制。
✔ 是｜確保網站安全性並防止入侵。

48. 用戶無法查覺自己電腦被植入惡意軟體。
✔ 是｜多數惡意程式潛伏執行，難以察覺。

49. 系統異常當機通常與資安無關。
✘ 非｜亦可能為攻擊或惡意程式所致。

50. 資安風險管理應納入企業整體風險控管政策。
✔ 是｜資安風險屬營運風險一環，需高層重視與納管。

51. 電子郵件驗證 **SPF**、**DKIM** 與 **DMARC** 可減少詐騙信風險。
✔ 是｜三種技術協助驗證寄件者身分，防止假冒郵件。

52. 資料在雲端儲存就不需要自行備份。
✘ 非｜雲端亦可能故障或資料刪除，應有第二備份。

53. 企業應對所有資安事件進行通報與事件紀錄。
✔ 是｜即使小規模事件，也應留痕、分析並改進。

54. 資訊安全僅關注技術問題，不涉及人員與制度管理。
✘ 非｜資訊安全三要素包含技術、人員與制度。

55. 零信任（**Zero Trust**）架構假設任何人或設備都不可信。
✔ 是｜強調持續驗證，降低內部攻擊風險。

56. 使用同一密碼登入多個網站風險較低。
✘ 非｜一旦洩漏，駭客可「撞庫」登入其他帳號。

57. 兩階段驗證（**2FA**）比單一密碼安全許多。
✔ 是｜第二道驗證提供額外防護層。

58. 個資法所稱之「個人資料」僅限身分證字號與姓名。
✘ 非｜還包括地址、手機、電子郵件等可識別個人之資料。

59. 定期對資安政策進行檢討與修訂是必要程序。
✔ 是｜制度應隨技術、法規與風險環境更新。

60. 偽造的**SSL**憑證也可能騙過使用者。
✔ 是｜駭客可仿冒網址與憑證，使用者應檢查細節。

61. 滲透測試主要目的是找出系統弱點。
✔ 是｜模擬攻擊，提早發現漏洞。

62. 同一網域內不同使用者帳號可共用密碼。
✘ 非｜共用帳密不利追蹤與安全稽核。

63. 即使是內部使用的測試系統，也應具備基本防護措施。
✔ 是｜測試環境若被駭入，亦可能成為跳板。

64. 資訊資產不含紙本文件。
✘ 非｜所有可辨識、具價值之資訊皆屬資產，包括紙本。

65. 企業網站若未設置權限控管，易發生橫向存取漏洞。
✔ 是｜可導致未授權用戶存取他人資料。

66. 無法查出攻擊來源時，可不列為資安事件。
✘ 非｜是否為事件應依是否有異常行為，而非是否能追查。

67. 使用群組帳號可提高使用效率並保護安全性。
✘ 非｜共用帳號降低可追溯性，應避免使用。

68. 資訊系統開發過程中應納入安全設計與測試。
✔ 是｜安全開發生命週期（**SDLC**）包含設計階段防護。

69. 智慧型裝置如攝影機或門鎖，不需要定期更新韌體。
✘ 非｜**IoT**裝置更新可修補漏洞，確保安全。

70. 資安訓練應僅針對資訊部門施行。
✘ 非｜所有員工都應接受資安訓練，防範社交工程與誤操作。

71. 資訊安全的三大目標為機密性、完整性與可用性。
✔ 是｜**CIA**三要素為資訊安全基本核心。

72. 資安事件回應流程中第一步是調查原因。
✘ 非｜應先隔離受影響系統、停止擴散，然後才是調查。

73. 端點偵測與回應（**EDR**）可用於偵測內部異常行為。
✔ 是｜能即時監控終端設備行為、回應異常。

74. 每次登入都用不同**IP**位置，代表系統更安全。
✘ 非｜異常**IP**或地點登入可能代表帳號被盜用。

75. 通過 **ISO/IEC 27001** 認證代表企業有資訊安全管理制度。
✔ 是｜該標準是國際資安管理系統規範。

76. 無風險設備無須安裝資安防護軟體。
✘ 非｜所有設備皆可能成為攻擊對象。

77. 密碼過期政策可促進使用者定期變更密碼，提升安全。
✔ 是｜但也需平衡使用者體驗與強度設定。

78. 系統應定期執行弱點掃描並追蹤改善。
✔ 是｜掃描是風險管理的第一步。

79. 過期的帳號與不再使用的系統應主動關閉。
✔ 是｜閒置資源若未控管，可能被利用。

80. **USB** 裝置為常見惡意程式傳播管道。
✔ 是｜插入不明 **USB** 可能植入木馬程式。

81. 兩個系統若資料同步，僅需一邊管理存取權限即可。
✘ 非｜應雙方管理與稽核，避免遺漏。

82. **DNS** 攻擊可導致網站無法解析與導向錯誤站台。
✔ 是｜例如 **DNS Cache Poisoning**。

83. 駭客常使用暴力破解工具猜解密碼。
✔ 是｜透過字典或暴力工具進行大量嘗試。

84. 高權限帳號應避免日常操作使用。
✔ 是｜避免誤操作或中毒影響整體系統。

85. 即時監控系統可協助發現未經授權存取行為。
✔ 是｜能提早識別風險並通報。

86. 使用者若離職，應立即停用其帳號與存取權限。
✔ 是｜避免人員變動後仍可存取機密資料。

87. 資訊安全等級分類應依資料敏感性決定存取權限。
✔ 是｜如公開、內部、機密等等級。

88. **VPN** 可提供遠端連線時的加密通訊保障。
✔ 是｜避免傳輸中被攔截或側錄。

89. 日誌（**Log**）管理在資訊安全中不具實質意義。
✘ 非｜日誌是事件追蹤、鑑識調查的重要依據。

90. 為了便利，可用手機記錄所有帳號密碼。
✘ 非｜未加密記錄可能導致帳密外洩。

91. **WPA3** 是目前無線加密中最安全的標準之一。
✔ 是｜比 **WPA2** 更安全，建議升級使用。

92. 雲端資料儲存仍需用戶端自行負責加密與權限設定。
✔ 是｜雲服務供應商不負完全責任。

93. **IoT** 裝置密碼預設為公開帳密是常見的資安漏洞。

✔ 是｜應立即更改預設密碼。

94. 資安教育應涵蓋釣魚信辨識技巧。
✔ 是｜提高用戶對偽造信件的辨識力。

95. 帳號管理可忽略系統中未曾使用過的帳戶。
✘ 非｜閒置帳戶易成為攻擊切入口。

96. 企業若無明確資安規範，員工行為將難以控管。
✔ 是｜須制定與宣導資訊安全政策。

97. 使用雲端系統時無須擔心法律合規問題。
✘ 非｜仍須依個資法、**GDPR**等法律規範。

98. 災難復原計畫（**DRP**）是企業資訊安全的必要部分。
✔ 是｜協助災後迅速恢復系統運作。

99. 持續監控（**SOC**）中心有助於即時偵測與回應資安威脅。
✔ 是｜可提供全天候資安監控與告警機制。

100. 資安無法完全杜絕風險，但可降低與管理風險。
✔ 是｜風險無法為零，但可透過措施控制於可接受範圍。

資訊與系統安全知識選擇題

1. 下列哪一項不是資訊安全的三大核心目標（**CIA**）之一？
A. 機密性（**Confidentiality**）
B. 完整性（**Integrity**）
C. 可用性（**Availability**）
D. 成本效益（**Cost Efficiency**）
✅ 答案：**D**｜解析：**CIA** 為資訊安全三要素，成本效益非核心目標。

2. 下列哪一種攻擊是透過大量請求癱瘓目標服務？
A. SQL Injection
B. Social Engineering
C. DoS 攻擊
D. XSS 攻擊
✅ 答案：**C**｜解析：**DoS** 是拒絕服務攻擊。

3. 哪一項可有效驗證網站真偽與傳輸加密？
A. DNS
B. CAPTCHA
C. HTTPS
D. FTP
✅ 答案：**C**｜解析：**HTTPS** 使用 **SSL/TLS** 加密。

4. 使用者收到偽裝成銀行的詐騙信件，這是哪種攻擊方式？
A. 鍵盤記錄器
B. 釣魚攻擊（**Phishing**）
C. 木馬程式
D. 逆向工程
✅ 答案：**B**｜解析：釣魚攻擊仿冒合法單位以騙取資料。

5. 下列何者屬於預防性資訊安全控制措施？
A. 入侵偵測系統（**IDS**）
B. 資安事後報告
C. 系統漏洞通報
D. 多因素驗證（**MFA**）
✅ 答案：**D**｜解析：**MFA** 可降低帳號被盜風險。

6. 關於密碼安全，下列何者為最佳做法？
A. 使用出生年月做密碼
B. 所有帳號使用相同密碼
C. 使用強密碼並定期更換
D. 記在紙條上貼螢幕旁
✅ 答案：**C**｜解析：強密碼與定期更換可增加安全性。

7. 何者為內部資安威脅的例子？
A. 駭客攻擊主機
B. 員工蓄意竊取資料
C. 釣魚網站攻擊
D. 網路爬蟲探測漏洞
✅ 答案：**B**｜解析：員工違規或惡意行為屬內部威脅。

8. 下列哪一種是物理安全措施？
A. 使用 **HTTPS**
B. 鎖住伺服器機櫃
C. 建立資安政策
D. 實施社交工程演練

✅ 答案：**B**｜解析：物理安全屬實體防護範疇。

9. 哪個機構負責發布資安漏洞標準代碼（**CVE**）？
A. Microsoft
B. ISO
C. MITRE
D. IEEE
✅ 答案：**C**｜解析：**MITRE** 負責維護 **CVE** 資料庫。

10. 社交工程攻擊的特點為？
A. 利用技術工具滲透系統
B. 鎖定設備硬體漏洞
C. 操縱人性弱點達成目的
D. 破解網路加密演算法
✅ 答案：**C**｜解析：社交工程透過說服或詐騙方式欺騙人類。

11. 下列哪一種行為最容易導致個資外洩？
A. 使用 **HTTPS** 網站
B. 在公司內部信箱傳送測試信
C. 點擊來源不明的附件或連結
D. 將資料上傳至企業雲端硬碟
✅ 答案：**C**｜解析：附件與連結可能包含惡意程式。

12. 備份資料最重要的目的為？
A. 增加資料存取速度
B. 降低網路使用量
C. 提高資料共享
D. 系統故障時快速回復
✅ 答案：**D**｜解析：備份是災難復原的基本手段。

13. 下列哪一個不是資安攻擊類型？
A. SQL Injection
B. Firewall
C. Ransomware
D. Man-in-the-Middle
✅ 答案：**B**｜解析：**Firewall** 是防護工具，不是攻擊手法。

14. 若企業伺服器長期未更新，最可能的風險為？
A. 執行效率過高
B. 系統無法登入

C. 遭利用已知漏洞攻擊
D. 操作介面過舊
✅ 答案：**C**｜解析：未更新會保留可被利用的漏洞。

15. 在資安領域，**VPN** 的主要作用為？
A. 防止電腦病毒感染
B. 節省儲存空間
C. 建立安全加密的遠端連線
D. 加速系統效能
✅ 答案：**C**｜解析：**VPN** 可保護通訊內容不被截取。

16. 零信任（**Zero Trust**）模型的核心原則為？
A. 信任內部網路即可
B. 不需多因素驗證
C. 所有用戶與設備皆需驗證
D. 所有資料都公開
✅ 答案：**C**｜解析：零信任架構不預設信任任何來源。

17. 若系統被植入勒索軟體，最適當的第一步應為？
A. 繳交贖金
B. 將系統重新啟動
C. 立即斷開網路連線
D. 刪除所有檔案
✅ 答案：**C**｜解析：先阻止勒索程式擴散或與外部連線。

18. 下列哪一項非資安人員的基本職責？
A. 系統設計
B. 威脅偵測
C. 漏洞通報
D. 防護政策制定
✅ 答案：**A**｜解析：系統設計屬 **IT** 開發，非資安核心職責。

19. 以下哪一項技術可驗證檔案未遭篡改？
A. 雜湊函數（**Hash Function**）
B. USB 加密
C. VPN 連線
D. 雲端儲存
✅ 答案：**A**｜解析：雜湊可檢查資料完整性。

20. 哪一項措施可防止駭客暴力破解帳號密碼？

A. 弱密碼容忍策略
B. 鎖定帳號與驗證碼機制
C. 增加網頁圖片設計
D. 使用公開留言板
✅ 答案：**B**｜解析：帳號連續錯誤次數限制與 **CAPTCHA** 可減少暴力破解。

21. 資訊安全政策的目的是？
A. 增加作業流程效率
B. 降低成本
C. 建立一致性的安全規範
D. 鼓勵使用者創新
✅ 答案：**C**｜解析：資安政策提供標準與行為準則。

22. 在資安事件管理流程中，第一步應為？
A. 列印報表
B. 撰寫報告
C. 偵測與通報事件
D. 寫電子郵件通知
✅ 答案：**C**｜解析：偵測與通報為事件管理的起點。

23. 若公司採購新伺服器，哪一項為資安基本措施？
A. 掛上公司**Logo**
B. 安裝最新遊戲
C. 關閉不必要的服務與開放埠口
D. 增加螢幕亮度
✅ 答案：**C**｜解析：減少攻擊面是基本安全作法。

24. 使用 **EDR**（端點偵測與回應）系統的主要目的為？
A. 加快網頁開啟速度
B. 減少辦公室人力
C. 偵測終端設備異常與即時防禦
D. 擴充硬碟容量
✅ 答案：**C**｜解析：**EDR** 主要用於端點安全防護。

25. 下列哪一項非勒索軟體（**Ransomware**）的行為？
A. 加密使用者檔案
B. 要求支付贖金
C. 提供免費掃毒服務
D. 阻止存取檔案
✅ 答案：**C**｜解析：勒索軟體會勒索金錢，不會提供幫助。

26. 如何避免使用公開**Wi-Fi**時個資外洩？
A. 不上網
B. 關閉藍牙
C. 開啟 **VPN** 並避免登入敏感帳號
D. 把手機放進口袋
✅ 答案：**C**｜解析：**VPN** 可加密資料並避免中間人攻擊。

27. 使用密碼管理器的好處是？
A. 減少記憶負擔並提高密碼安全性
B. 自動安裝軟體
C. 幫忙購物
D. 讓帳號公開
✅ 答案：**A**｜解析：可建立與儲存複雜密碼，避免重複使用。

28. 哪一項技術可確保傳輸資料不被中途竄改？
A. 虛擬記憶體
B. SSL/TLS 加密
C. 預設帳號
D. DOS 模式
✅ 答案：**B**｜解析：**SSL/TLS** 可保障傳輸中的資料安全。

29. 多因素驗證通常包含下列哪兩種？
A. 生日與手機型號
B. 密碼與帳號名稱
C. 密碼與實體憑證（如簡訊、**App**）
D. IP與時間
✅ 答案：**C**｜解析：**2FA** 結合知識因子與擁有因子。

30. 資訊系統日誌的主要功能是？
A. 儲存圖片
B. 分析天氣
C. 留下操作記錄供追蹤與稽核
D. 處理稅務申報
✅ 答案：**C**｜解析：**Log** 是重要的事後調查與風險管理依據。

31. 哪一種方式最適合處理敏感個資？
A. 直接上傳至公開雲端
B. 未經加密儲存

C. 加密存放並限制存取權限
D. 傳給全部人員
✅ 答案：**C**｜解析：敏感資料須加密與存取控管。

32. 偵測內部員工違規存取機密資訊，應採用？
A. 監控郵件內容
B. 加強網速
C. 員工座位改變
D. 新增裝潢
✅ 答案：**A**｜解析：日誌與監控可發現異常操作與風險行為。

33. 哪一項不是資安防護常見層級？
A. 應用層
B. 網路層
C. 傳輸層
D. 價格層
✅ 答案：**D**｜解析：價格與資安無直接關聯。

34. 資安事件報告應包含下列哪項？
A. 傷害人數
B. 事件發生時間與影響範圍
C. 使用者密碼
D. 員工年資
✅ 答案：**B**｜解析：時間與範圍是評估與改善依據。

35. 下列哪一項是資訊安全制度的基礎？
A. 開放分享資料
B. 僅管理階層負責資安
C. 制定並遵守資訊安全政策
D. 讓所有人有最高權限
✅ 答案：**C**｜解析：制度是資訊安全治理的根本。

36. 若某企業實施「最低權限原則（**Least Privilege**）」，其目的為？
A. 提高工作效率
B. 限制使用者只能存取其職務所需資源
C. 降低系統效能消耗
D. 授權所有人最高權限以方便作業
✅ 答案：**B**｜解析：最低權限原則是資訊安全重要原則，避免權限過大造成風險。

37. 下列哪一種攻擊會導致網站執行惡意腳本？
A. SQL Injection
B. DoS
C. Cross-Site Scripting（XSS）
D. Spoofing
✅ 答案：**C**｜解析：**XSS** 可在用戶瀏覽時執行惡意程式。

38. 公司為避免勒索病毒攻擊應優先實施？
A. 提高上班時間
B. 定期資料備份與員工資安訓練
C. 增設網頁廣告
D. 降低密碼複雜度
✅ 答案：**B**｜解析：備份與教育是預防勒索攻擊的有效手段。

39. 哪一項為企業常見的雲端資安風險？
A. 雲端資料永久保存
B. 客戶資料無需保密
C. 存取控制不當與資料未加密
D. 雲端供應商不允許更新
✅ 答案：**C**｜解析：雲端環境常見問題為錯誤設定與加密不足。

40. 若一公司遭駭客攻擊，資訊主管應優先？
A. 關閉所有主機
B. 啟用防火牆
C. 啟動資安事件通報與應變機制
D. 恢復備份資料
✅ 答案：**C**｜解析：依資安事件處理程序執行，是危機處理基本流程。

41. 防範 **SQL Injection** 攻擊時，下列哪項作法較有效？
A. 關閉網站留言板
B. 使用參數化查詢（**Parameterized Query**）
C. 避免使用資料庫
D. 增加使用者密碼長度
✅ 答案：**B**｜解析：可防止輸入值直接被當成程式碼執行。

42. 關於 **ISO/IEC 27001**，下列敘述何者正確？
A. 為資料備份格式標準

B. 為資訊安全管理系統（**ISMS**）國際標準
C. 限用於金融業
D. 僅涵蓋硬體安全
✅ 答案：**B**｜解析：**ISO 27001** 是資訊安全治理的國際框架標準。

43. 零日攻擊（**Zero-Day Attack**）的最大特徵為？
A. 沒有實際傷害
B. 系統可自動防禦
C. 利用尚未公開的系統漏洞
D. 只能透過人工操作
✅ 答案：**C**｜解析：未被廠商修補前的漏洞稱為零日。

44. 企業若欲確認資安防護效能，可定期進行？
A. 品牌知名度調查
B. 滲透測試與弱點掃描
C. 客戶滿意度調查
D. 伺服器停機演練
✅ 答案：**B**｜解析：是評估資訊系統安全狀況的關鍵技術。

45. 雜湊演算法（**Hash**）具備什麼特性？
A. 加密與解密皆快速
B. 可逆運算
C. 單向運算，且不同輸入產生不同值
D. 用於視覺辨識
✅ 答案：**C**｜解析：雜湊為單向不可逆，常用於驗證完整性。

46. 下列何者非社交工程的典型範例？
A. 偽造客服來電
B. 鼓勵弱密碼設定
C. 寄送釣魚信
D. 透過技術弱點入侵系統
✅ 答案：**D**｜解析：**D** 為技術攻擊，非人性操弄類型。

47. 以下哪一個是實體資安管理常見措施？
A. 安裝入侵防禦系統
B. 鎖定**IP**位址
C. 機房門禁管制與監視系統
D. 使用雲端儲存
✅ 答案：**C**｜解析：門禁、攝影機屬實體環境防護。

48. 以下哪一項可提高帳戶登入安全性？
A. 簡短密碼
B. 停用防火牆
C. 使用兩步驟驗證（**2FA**）
D. 使用生日作為密碼
✅ 答案：**C**｜解析：**MFA** 是防止帳號遭竊的重要手段。

49. 資安事件中所謂的「內鬼攻擊」指的是？
A. 外部駭客入侵系統
B. 使用公共**Wi-Fi**傳輸資料
C. 內部人員未授權操作或蓄意破壞
D. 資料備份失敗
✅ 答案：**C**｜解析：內部威脅是企業資安的一大挑戰。

50. 下列何者是備份策略「**3-2-1** 原則」的正確敘述？
A. 三份備份、兩種媒體、一份異地保存
B. 三個人負責備份
C. 每週三備份兩次
D. 一台主機備份三份資料
✅ 答案：**A**｜解析：常用於企業備份標準策略。

51. 當資安人員需即時監控並應對攻擊行為，建議使用？
A. ERP 系統
B. SOC（**Security Operation Center**）
C. 客服中心
D. DNS Server
✅ 答案：**B**｜解析：**SOC** 是資安營運監控中心。

52. 哪一項屬於資安治理層面的指標？
A. 上網速度
B. 資料備份頻率
C. 重大資安事件通報時間與處理效率
D. 主機記憶體大小
✅ 答案：**C**｜解析：治理強調制度與績效指標。

53. 關於 **GDPR**（一般資料保護規則），以下敘述何者正確？
A. 僅適用美國地區
B. 允許企業永久保留顧客資料
C. 為歐盟個資保護規範，具有域外效力
D. 僅約束個人用戶

✅ 答案：**C**｜解析：**GDPR** 為全球最嚴格資料保護法之一。

54. 雲端服務中的「共用責任模型」指的是？
A. 由客戶與供應商共同負責資安
B. 只由供應商負責全部資安
C. 使用者完全免責
D. 管理權交由第三方
✅ 答案：**A**｜解析：雲端資安需雙方合作分工。

55. 使用者傳送加密檔案時，若欲確保檔案真偽，應使用？
A. ZIP 壓縮
B. MD5 驗證值
C. PDF 轉檔
D. Proxy 設定
✅ 答案：**B**｜解析：可驗證是否被竄改。

56. 下列哪一項資安工具可偵測內網可疑行為？
A. DHCP Server
B. IDS（入侵偵測系統）
C. 電子白板
D. 監控攝影機
✅ 答案：**B**｜解析：**IDS** 可主動告警異常網路行為。

57. 下列哪種攻擊方式會改變網頁內容？
A. DoS 攻擊
B. 網頁篡改（**Website Defacement**）
C. 密碼重設
D. 動態**IP**設定
✅ 答案：**B**｜解析：攻擊者透過漏洞竄改頁面內容。

58. 針對公司外部網站安全檢測，最常用的方法為？
A. DNS解析測試
B. 弱點掃描與滲透測試
C. 員工滿意度調查
D. Excel分析
✅ 答案：**B**｜解析：是企業網站最常用的資安檢測流程。

59. 若公司使用免費公用雲端硬碟存放敏感資料，潛在風險為？
A. 讀取速度太快
B. 資料加密無法進行

C. 雲端供應商未提供保密保障
D. 傳輸資料無網路流量限制
✅ 答案：**C**｜解析：免費平台不保證商業等級資安。

60. 在資訊安全架構中，資產分類與分級的目的為？
A. 計算儲存容量
B. 建立預算依據
C. 區分資料敏感性與保護層級
D. 快速刪除檔案
✅ 答案：**C**｜解析：分級後可依敏感度設定防護措施。

61. 駭客使用社群網站搜尋目標員工資訊以發動攻擊，此屬於？
A. 網站植入
B. 資料封包攻擊
C. OSINT（開放資源情報）+ 社交工程
D. 鍵盤記錄器攻擊
✅ 答案：**C**｜解析：結合公開情報與心理誘騙。

62. 資訊安全風險管理流程第一步通常為？
A. 風險報告撰寫
B. 識別資產與潛在威脅
C. 安裝**EDR**
D. 加密資料
✅ 答案：**B**｜解析：先找出保護對象與可能威脅。

63. 企業內部為何應禁止安裝未經授權軟體？
A. 增加人事成本
B. 影響營運成本
C. 提高資訊管理效率
D. 降低惡意程式潛入與授權風險
✅ 答案：**D**｜解析：非授權軟體可能為惡意軟體來源。

64. 在 **BYOD**（自帶設備）政策中，資訊安全最大挑戰為？
A. 硬體價格
B. 員工效率過高
C. 裝置控管與資料分離困難
D. 加班費問題
✅ 答案：**C**｜解析：裝置多樣性與無控管是管理難點。

65. 若某公司系統遭中毒癱瘓，最合理的恢復程序為？

A. 立刻重啟系統
B. 拆除主機
C. 啟動災難復原計畫（**DRP**）
D. 啟動備份計畫之主機防火牆
✅ 答案：**C**｜解析：**DRP** 是中長期災害處理流程。

66. 企業導入資安管理制度最主要的原因為？
A. 增加報表產出
B. 建立一致性作業與風險管控
C. 提高銷售額
D. 減少 **IT** 招募
✅ 答案：**B**｜解析：制度化可規範人員行為與事件應變。

67. 電子簽章在資安上的作用是？
A. 降低電費
B. 確認訊息來源與防止文件篡改
C. 加快上網速度
D. 移除惡意程式
✅ 答案：**B**｜解析：可驗證文件真偽與完整性。

68. 某企業每日記錄所有登入失敗紀錄，目的為？
A. 分析使用者行為習慣
B. 強化操作教育訓練
C. 偵測暴力破解與異常登入行為
D. 彈性調薪評估
✅ 答案：**C**｜解析：失敗登入可揭露潛在攻擊企圖。

69. 哪一項屬於資訊安全文化的核心？
A. 對所有人開放最高權限
B. 避免提及資安
C. 組織高層帶頭遵守與推動資安政策
D. 採購昂貴設備
✅ 答案：**C**｜解析：高層推動是形成資安文化的關鍵。

70. 若組織使用 **AI** 進行資安監控，其優勢在於？
A. 過濾垃圾郵件
B. 偵測零日攻擊與行為異常更即時有效
C. 減少密碼管理困難
D. 增強網站搜尋能力
✅ 答案：**B**｜解析：**AI** 可提升偵測準確度與速度。

71. 下列哪項敘述最能反映資安治理的核心目標？
A. 降低人力成本
B. 提高程式碼品質
C. 將資訊安全融入企業營運決策與風險管理
D. 強化品牌識別度
✅ 答案：**C**｜解析：資安治理重點是將資安納入整體經營策略與治理架構中。

72. 若企業欲合法蒐集與處理個人資料，依個資法應採取哪一措施？
A. 公告所有顧客資料
B. 先取得當事人同意並說明目的與範圍
C. 資料收集後通知主管機關
D. 僅由主管保留同意紀錄即可
✅ 答案：**B**｜解析：個資法明定需特定目的、取得明確同意。

73. 若企業因資安事件導致客戶資料外洩，應依何原則處理？
A. 嚴密封鎖消息
B. 儘速公告並啟動應變與通報機制
C. 暫停所有業務
D. 拒絕回應媒體
✅ 答案：**B**｜解析：應依事件回應程序啟動通報、調查與溝通。

74. 社交工程防範的首要方法為？
A. 增設防火牆
B. 禁止進入公司網站
C. 培訓員工提高警覺與辨識能力
D. 強制下班關機
✅ 答案：**C**｜解析：社交工程攻擊目標為人，因此員工教育最關鍵。

75. 資安風險評估中的「影響程度」是指？
A. 預算執行進度
B. 攻擊可能發生的頻率
C. 攻擊成功後對組織的損害大小
D. 備份資料的大小
✅ 答案：**C**｜解析：評估風險必須考量事件對業務影響的嚴重性。

76. 在企業資安政策中，哪一項最能確保使用者行為合規？
A. 推行自願性密碼更新
B. 建立明確可查的存取控管制度與審查流程
C. 憑感覺判斷帳號存取
D. 允許帳號共用以提高效率
✅ 答案：**B**｜解析：制度化存取控管可落實稽核與責任歸屬。

77. 下列哪一項是資訊安全的國際認證標準？
A. ISO 14001
B. ISO 27001
C. ISO 50001
D. ISO 9000
✅ 答案：**B**｜解析：**ISO 27001** 為資訊安全管理系統標準。

78. 資安事故發生後需進行鑑識調查，應優先保全何項證據？
A. 電腦品牌型號
B. 網頁畫面截圖
C. 系統日誌與登入紀錄
D. 員工薪資單
✅ 答案：**C**｜解析：**Log** 是事件重建與責任歸屬的關鍵依據。

79. 關於 **DLP**（資料外洩防護）系統，其主要功能為？
A. 提升硬碟容量
B. 阻止未授權資料外傳或存取
C. 加快網頁載入
D. 建立雲端平台
✅ 答案：**B**｜解析：**DLP** 可防止資料被複製、上傳、寄出等外洩行為。

80. 以下哪一項情境最可能涉及**APT**（高階持續性威脅）攻擊？
A. 收到簡訊抽獎通知
B. 政府機構遭長期滲透並竊取機密
C. 短時間大量掃描網站弱點
D. 一般用戶被植入木馬
✅ 答案：**B**｜解析：**APT** 為有組織、有目的的長期滲透行為。

81. 資訊安全中「不可否認性」主要靠何技術實現？

A. 加密演算法
B. 公開金鑰與數位簽章
C. 硬體升級
D. 網路加速器
✅ 答案：**B**｜解析：簽章可確認資料來源且無法否認。

82. 在資訊系統發展生命週期（**SDLC**）中，哪一階段最適合導入資安設計？
A. 維運階段
B. 開發完成後
C. 規劃與需求分析階段
D. 測試階段
✅ 答案：**C**｜解析：安全性應自系統設計之初納入考量。

83. 下列哪一種登入方式風險最低？
A. 密碼 **+ OTP**
B. 生日當作密碼
C. 單一密碼用多個平台
D. 手寫密碼貼在螢幕上
✅ 答案：**A**｜解析：結合密碼與一次性密碼（**OTP**）屬多因子驗證。

84. 若使用者遭遇釣魚網站，最常見的目的為何？
A. 增加流量
B. 收集廣告數據
C. 偷取帳號密碼或個人資料
D. 改變主題樣式
✅ 答案：**C**｜解析：釣魚網站旨在誘導用戶主動洩露資料。

85. 在企業中推行資訊分級制度的好處為？
A. 簡化資料分類
B. 所有資料均等保護
C. 根據敏感程度決定保護強度與存取權限
D. 增加行政成本
✅ 答案：**C**｜解析：分級制度有助於風險分擔與資源配置。

86. 下列何者屬於靜態資安防禦機制？
A. 防毒軟體
B. 入侵防禦系統（**IPS**）
C. 系統權限設定
D. 事件通報系統

✅ 答案：**C**｜解析：權限控管為事前配置性防禦措施。

87. 若企業採用雲端儲存服務，哪一項是使用者責任？
A. 機房防火設施
B. 雲端架構升級
C. 設定存取權限與資料加密
D. 主機維修管理
✅ 答案：**C**｜解析：雲端安全為「共責模型」，用戶負責設定與控管。

88. 哪一項為預防資訊洩漏的良好做法？
A. 所有人都用預設密碼
B. 開放匿名登入
C. 使用加密與最小權限原則
D. 頻繁變動主機 **IP**
✅ 答案：**C**｜解析：加密資料並限制存取是防外洩關鍵。

89. 資安風險矩陣評估中，兩軸通常為？
A. 人力與技術
B. 頻率與風險
C. 發生機率與衝擊程度
D. 資產價值與記憶體大小
✅ 答案：**C**｜解析：矩陣可視覺化風險分布與優先順序。

90. 哪一項資料屬於高度敏感資料？
A. 上班打卡時間
B. 員工年齡
C. 銀行帳戶、密碼與身份證字號
D. 公司**LOGO**圖片
✅ 答案：**C**｜解析：這類資料一旦外洩，可能造成財務與身分風險。

91. 哪一項屬於資安意識訓練的關鍵議題？
A. 新人介紹流程
B. 社群行銷技巧
C. 如何辨識釣魚郵件與惡意連結
D. 軟體設計模式
✅ 答案：**C**｜解析：釣魚信識別是資安訓練核心。

92. 資安稽核的主要目的是？
A. 發現資安預算不足

B. 提高公司形象
C. 評估實際作業與資安政策落實程度
D. 檢查業績表現
✅ 答案：**C**｜解析：稽核為制度檢查機制，確保實施成效。

93. 若資安事件發生時無清楚責任歸屬，最常見的制度缺失為？
A. 員工升遷制度
B. 權限控管與帳號紀錄不足
C. 薪資計算系統錯誤
D. 打卡制度錯誤
✅ 答案：**B**｜解析：無法追蹤即無法界定責任。

94. 若企業將資安委外處理，最應注意？
A. 外包成本
B. 資安廠商廣告數量
C. 委外合約中責任與服務範圍界定
D. 廠商有無制服
✅ 答案：**C**｜解析：資安委外需明確定義服務內容與責任歸屬。

95. 哪一類資料不建議直接公開於網站？
A. 年度活動照片
B. 公司歷史沿革
C. 員工手機號碼與身份證號
D. 品牌標誌
✅ 答案：**C**｜解析：個資應受保護，不宜公開。

96. 若資料未加密即透過 **Email** 傳送，潛在風險為？
A. 造成電郵格式異常
B. 傳送速度變慢
C. 資料可被中間攔截或竄改
D. 寄件人無法收信
✅ 答案：**C**｜解析：未加密傳輸容易被監聽或竄改。

97. 哪一項情況應被視為資訊安全事件？
A. 員工離職
B. 定期換電腦螢幕
C. 系統發現不明登入嘗試
D. 加班晚下班
✅ 答案：**C**｜解析：異常存取應即時記錄與通報。

98. 資訊安全風險通常無法完全消除，應採何策略？
A. 完全忽略風險
B. 視為必要成本
C. 透過風險管理將其降至可接受範圍
D. 委外處理後不再管理
✅ 答案：**C**｜解析：資訊安全重點是風險控制與持續改善。

99. 實施資安教育訓練後，應透過何方式驗證效果？
A. 發禮物
B. 攝影紀錄
C. 測驗、演練或社交工程測試
D. 擴大訓練時數
✅ 答案：**C**｜解析：應搭配成效評估手段驗證學習成效。

100. 資訊安全的最終責任者通常應為？
A. 系統工程師
B. 一般使用者
C. 資訊主管或企業高階管理層
D. 客服人員
✅ 答案：**C**｜解析：資安為企業風險管理的一部分，高層應負決策責任。