

# 一般問題

## 1. 何謂資訊保安?

資訊保安指的是保護各方面資訊和資訊系統，免於未經授權的接達、使用、揭露、中斷、修改或毀壞，以求達到保密性、完整性和可用性。

- 1) 保密性: 僅允許經授權的人員知道或獲得接達到資訊系統所儲存或處理的資訊。
- 2) 完整性: 僅允許經授權的人員修改資訊系統所儲存或處理的資訊。
- 3) 可用性: 用戶可在特定時間內使用資訊系統。

## 2. 何謂資訊科技保安?

資訊科技保安一詞並沒有確切的定義，但通常指的是攸關保密性、完整性和可用性之資訊科技基本建設、資訊系統及相關資源的保護。

## 3. 我們如何能確保資訊科技保安?

對資訊科技保安使用系統性的方法，常常是一個好的建議。

- 首先，機構必須訂立清楚明確的保安要求。
- 第二，應發展和強化保安政策和程序。
- 第三，應執行定期保安風險評估和審計，還有對系統持續監控，以確保適當地推行有效力及有效率的保安政策和程序。

## 4. 我如何能確認我機構的保安要求?

為決定適當的保安標準，機構擁有者應考慮資訊系統和其他資訊科技資產對機構中商業的價值，也應考慮保安事故對機構聲譽和適當地持續業務的影響。通常使用稱為風險分析的工具來確定哪些資產要保護，它們對適當營運/機構交易的相對重要性，以及優先順序安排保安保護的排名/水平。其分析結果將會清楚地制定入機構的保安標準清單內。

## 5. 何謂保安政策? 它與保安標準、指引及程序的關係是什麼呢?

保安政策設定保安規格的標準，並說明了哪一方面是機構最重要的。因此，可視保安政策為必要的基本原則，機構內應處處遵行之，且應符合你的保安要求和機構營業目的與目標。

保安標準、指引及程序是推行和強化保安政策的工具，應詳加說明管理、營運和技術上的議題。這些文件提供詳細步驟和建議，以協助用戶和系統管理員遵守保安政策的要求。標準、指引和程序也許會要求比保安政策更頻繁的覆檢。

## 6. 當擬定保安政策時，應該考慮什麼呢？

保安政策對機構應是有用及可行的，應考慮以下幾點：

- 保護資產的敏感性和價值
- 法律要求、規則和政府法律
- 機構目標和商業目的
- 推行、分佈和執行的實用性

## 7. 當制訂保安政策時，應包含什麼呢？

制訂保安政策需要積極的支援，和來自不同階級與不同功能之各部門的持續參與，可形成工作團隊或專門小組來制訂該政策。一般而言，該團隊也許包含資深管理層之授權代表、技術人員、操作人員和商業用戶。資深管理層以機構目標和目的為出發點，能提供全面指引、評估和決策訂定，而技術人員能提供技術支援和不同保安技術機制的可行性。商業用戶代表的是可能受政策直接影響的相關系統用戶。第三方顧問有時也會涉入，以覆檢保安政策草稿。

## 8. 如何能在我的機構中制訂保安政策？

首先，確定制訂保安政策所需人員。其次，製作所有必要活動、所需資源及流程表的計畫。第三，決定保安要求和根據該要求，制訂機構的保安政策。之後，覆檢起草的保安政策，並經不同利益關係者同意。在制訂保安政策之前，該程序會重複數次。

因科技、商業環境和保安標準會隨時間而改變，應定期覆檢保安政策(例如兩年一次)，以跟上變化。

## 9. 保安政策中應包含什麼呢？

資訊科技保安政策必須說明能被改變的程序和行為，體認每項保安原則皆有例外也是很重要的。盡可能保持政策的彈性，以讓政策長期皆可實行。

資訊科技保安政策主要可包含以下內容：

- 什麼是政策目的和範圍？
- 什麼資訊資源需要受保護？
- 誰會受該政策影響？
- 誰確切有權利和特權？

- 誰能允許權力和特權?
- 什麼是保護資訊資源的最低限度措施?
- 報告保安違規和犯罪的期待和程序
- 有效保安的特定管理和用戶責任
- 政策有效日期以及修訂日期或修檢時間

## 10. 發展保安政策的好處是什麼?

有了保安政策，所有員工可清楚地了解保護機構內資訊資產及資源時，可被允許及不被允許的行為，這有助提升所有員工保安意識的水平。此外，保安政策提供發展詳細指引和程序的基礎，有助支持對嚴重保安違規事件作出告發的任何決定。

## 11. 當推行保安政策時，我應考慮什麼呢?

即使保安政策已獲得核准，放置保安政策在適當的地方則是另一回事，其需要一系列的步驟：

### 保安意識和訓練

保安意識對確定所有相關人員了解風險且接受、採用優質保安作業實務是很重要的。培訓和教育可提供用戶、發展者、系統管理員、保安管理員及任何相關團體推行適當保安措施所需的技巧和知識。

### 承諾與溝通

除非所有用戶和相關團體承諾將會完全遵守任何一項政策，否則無法全面推行。要確保與用戶和相關人員建立良好的溝通：

- 當他們新加入機構時，透過簡報或是新進人員培訓來介紹政策
- 邀請他們參與發展政策提案
- 培訓他們遵守政策所需的技巧
- 令他們感覺到保安措施是為他們的好處而建立的
- 定期提醒他們並教導新的議題
- 確定他們已經簽署確認通知協議書
- 提供他們推行政策的指引

### 強制執行與矯正

這指的是政策推行時的強制執行權力工作，以及違反該權力時的矯正行動。機構應該設定程序，提供即時支援以調查保安違規。

### 所有團體的持續參與

一項有效力的保安政策也須依賴用戶和企業單位之間持續的資訊交換、諮詢、協調及合作，注入各方面的知識如標準、方法、作業實務守則和其他外部機構來的保安專家，也有助保持最新及恰當的保安政策。

## 12. 保安評估指的是什麼?

保安評估是評價資訊科技環境的保安狀態，包括網絡和資訊系統。保安管理員或第三方保安顧問通常會使用專門設計來搜尋保安風險和內部主機及工作站漏洞的軟件(稱為漏洞掃描器)。此外，作業程序的適當性也在保安評估中核定。

總而言之，在系統發展計畫的初期或何時會有重大資訊資產及環境變化，都應執行保安風險評估，以確定需要哪種保安措施。因為保安漏洞隨著時間浮現，所以應定時執行保安風險評估，如每兩年一次。

## 13. 什麼是保安審計?

以資訊科技保安政策或標準為基礎來決定現存保護的整體狀態，並證實是否適當地執行現存保護，此過程便稱為**保安審計**，其著重於決定是否依照資訊科技保安政策來安全地保護現有環境。

在執行保安評估或審計之前，機構應定義保安審計的範圍、可用的預算及評估/審計的期間。

## 14. 多久應執行一次保安審計?

保安審計只提供特定時間顯現系統漏洞的簡要印象。因科技與商業環境日新月異，所以不可避免地需要定期和持續覆檢。隨著企業的重要性不同，保安審計也許需要每年或每兩年執行一次。

## 15. 誰應執行保安審計?

因保安審計是一項複雜的難題，且需要有技巧和有經驗的人員，所以必須小心計畫。建議獨立且可信賴的第三者來執行審計。視乎內部員工的技巧和被審計的資訊之重要性/敏感性，該第三者可以是企業內另一組別的員工或外部審計團隊。

## 16. 什麼是資訊科技保安事故?

資訊科技保安事故是指資訊系統或網絡的不利事件，且引致電腦或網絡保安於可行性、完整性和保密性方面受到威脅。此事故會能導致數據損壞或披露資料。

然而，例如自然災害、硬件/軟件故障，數據線失效或停電等等不利事件通常是排除在外的。

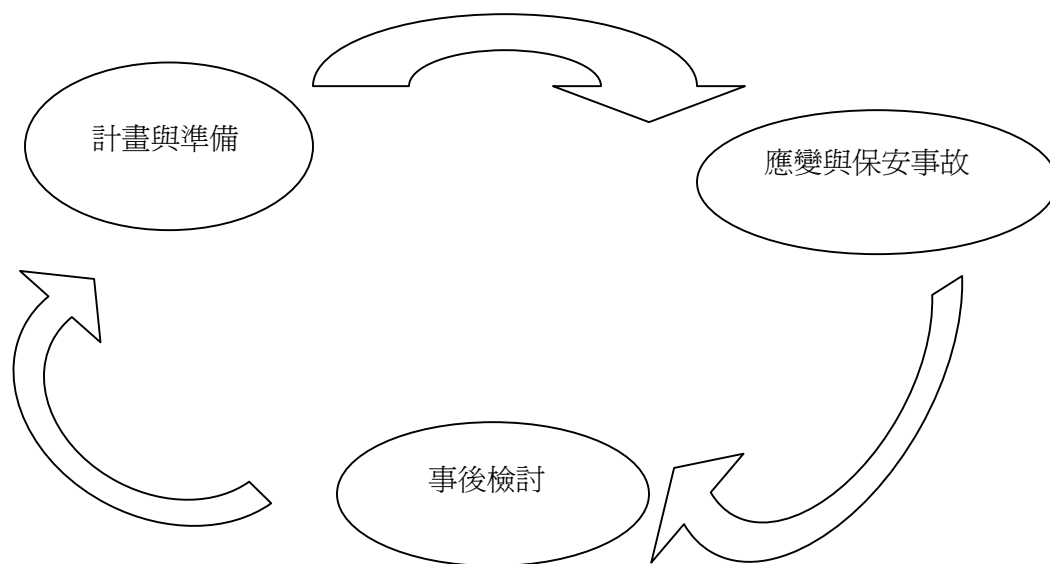
## 17. 我能如何處理保安事故?

**處理保安事故**是指一系列的持續過程，監控在保安事故發生之前、發生當時和發生之後的活動。

處理保安事故開始於計畫和準備適當的資源，然後發展正確程序，以供遵守，例如升級(escalation)和保安事故應變程序。

當發現保安事故時，負責人員遵守事前規定的程序來處理保安事故應變，保安事故應變代表著處理保安事故的活動或行動，並使系統回復正常運作，通常會發展特定事故應變團隊以處理保安事故應變。

在事故過後，採取跟進行動來評估該事故，且加強保安保護，以避免歷史重演。計畫和準備工作將相應地檢討及修改，以確保有足夠資源(包括人力、設備和技術知識)，並妥當地定義程序，以便在未來處理類似事故。



## 18. 什麼是入侵? 什麼是入侵偵測?

入侵指的是試圖損害資訊系統的可行性、保密性和完整性的一連串活動。

入侵偵測是發現入侵的方法論，包含外部入侵者侵入系統的偵測與內部用戶濫用系統資源。

## 19. 假如我的網絡已經有防火牆，為什麼我需要入侵偵測系統(IDS)/入侵防禦系統(IPS)?

防火牆只是整體整合保安系統的一部分，它們有其限制。防火牆無法對所有入侵提出警告，也不能阻止所有保安違規。除非你不斷監控入侵，不然你無法知道你的防火牆能否阻擋所有入侵，但可在策略位置安裝及使用 IDS / IPS，每天每分每秒持續收集和檢查可疑活動的資訊。IPS 也提供積極的應變系統，以便阻止攻擊來源或減低攻擊所帶來的影響。

## 20. 什麼是入侵偵測系統的限制?

入侵偵測系統不能幫助你解決或修理所有保安事故，也不能告訴你究竟是誰攻擊系統或攻擊是如何發生的，以及攻擊者的意圖。它只能提供攻擊來源的資料和產生攻擊的 IP 位址。為了確定真正的攻擊者，你必需分析所有相關紀錄。

## 21. 什麼是網絡防火牆?防火牆可以保護我的系統避免什麼?

防火牆是在兩個網絡之間，強制執行接達控制政策的系統。一般而言，防火牆可以阻擋從網絡外面到裡面的通訊，並准許從裡面的資訊交換到外面的世界，以進行溝通。防火牆也可以提供紀錄和審計功能，以紀錄所有通過的通訊；換言之，防火牆可通過定義接達控制政策來允許或拒絕通訊，以保護內部網絡避免外來的攻擊。然而，防火牆無法保護那些不通過它的攻擊，且不能避免那些包含在網絡通訊裡面的攻擊，如病毒或數據導引式攻擊，因防火牆准許這類通訊(例如網上通訊)。適當的防火牆配置對確保有效的保安保護扮演著非常重要的角色。

## 22. 保護網絡的一般考量是什麼?

以下列出一些可提供幫助的網絡保護指引：

- 保持簡單網絡(即在安全網絡和不安全網絡之間保持最少數量的網絡介面點)
- 只允許經授權的通訊進入安全的網絡
- 設定適當的控制，以限制連結到外部/不安全的網絡
- 使用多重機制來認證用戶(如: 密碼系統加上事前註冊的IP/IPX網絡，還有事前註冊的MAC 位址/終端機號碼)
- 使用網絡管理系統來控制網絡
- 在透過網絡傳輸前，使用經證明過的加密演算法來加密資料

## 23. 什麼是實體保安?

實體保安指的是保護硬件、電腦設備和其他資訊科技資產免受外來實體的威脅，例如未經授權的接達、偷竊或遺失在運送到外面場地時的備份媒體。

## 24. 什麼是應用系統保安?

應用系統保安指的是建立在應用系統裡面的保安措施，以提供安全的電腦環境。一般應用系統的保安措施包括應用系統認證、不同階級用戶的接達矩陣、輸入確認以避免可能產生的應用系統缺點，例如緩衝區滿溢(buffer overflow)，以及應用系統紀錄特色 (application logging features)等等。在應用系統設計階段時，應用系統擁有者應與發展團隊根據應用系統的重要性，還有處理的數據敏感性，共同決定應用系統的保安要求。

## 25. 互聯網保安應考慮什麼?

互聯網是網絡中的萬維網絡，使用 TCP/IP 協定作為溝通工具。互聯網的連接在增加資訊的接達方面帶來無數的好處；然而互聯網深受重大且普遍的保安問題所苦。

其根本的問題在於互聯網並沒有安全地被設計，許多 TCP/IP 服務對於保安威脅是無力抵抗的，例如竊聽和仿冒，只要使用便利可行的軟件，人們便可以監控和捕捉電子郵件、密碼和檔案傳輸。

互聯網服務需要強大的認證機制和密碼使用機制，而這些機制必須在不同機種之間可以互相通用。查詢互聯網資料或處理交易均需要用戶認證，認證的資料也需要審計和備份，且應妥善加密敏感和個人的數據。

總之，互聯網保安涵蓋廣泛的議題，如識別和認證、電腦病毒保護、軟件執照、遠端接達、撥接接達、實體保安、防火牆推行和其他有關互聯網使用方面的議題。

## 26. 如何保護我的網上私隱?

當你在網上填寫表格或使用即時通訊工具與不明人士聊天時，切勿在網上分享你的個人資料，包括你的名字、家裡住址、電子郵件地址、身份証號碼、電話號碼等等，除非你有特別理由希望他們知道。當你輸入你的個人資料時，應設置適當的保安措施如 SSL。

在網上送出你的個人資料時，請特別三思，因你個人的資料可能會被使用於其他你未打算過的用途。在傳送和儲存電子郵件之前使用數碼簽署並加密訊息，以保護你的電子郵件。妥善保管你的個人電腦，因其有可能遭受實體攻擊或是遭竊。定期更改密碼並將其保密，且不要使用容易猜到的密碼，如字典上的字。

## 27. 如何確定用戶密碼是安全的?

用戶應該選擇難以猜到的密碼，並盡可能將其保密。在重設密碼之後或收到新密碼時，應立刻更改密碼。管理員應確定每一個新用戶都拿到一個好的初始密碼，而不是使用機構內所有員工都知道的預設密碼。應設定程序來確定只有真正要求密碼的那個人可以得到密

碼。在任何時候，密碼都不應該清楚地在螢幕上顯示出來。在儲用戶密碼時，也應使用安全演算法加以加密。

任何時候都應妥善地保護密碼。當儲存密碼於數據庫或伺服器時，應利用如接達控制和加密等保安控制來保護密碼。因密碼是登入系統時重要的憑證，所以當傳送經過不可信或不安全的溝通網絡時，必需把密碼加密。假如密碼加密不可行，應推行其他控制如更頻繁地更改密碼。

## 28. 如何保護我的電腦數據?

你應該考慮以下必做之事：

- 執行抗電腦病毒、抗間諜軟件和最新惡性程式碼定義檔及保安修補程式等軟件的自動更新功能
- 安裝和執行個人防火牆
- 確保密碼保密和定時更改密碼
- 安全保護可攜式儲存設備
- 加密敏感數據
- 備份重要數據
- 定期測試數據復原程序

以下是不可做之事:

- 不要瀏覽可疑網站
- 不要開啓從陌生人寄來的電子郵件或附加檔

此外，當你使用公共無線網絡及/或公共電腦設備時，應要小心注意數據的安全。

## 29. 如何成爲一名聰明的互聯網用戶?

假如你依以下各點來保護你的電腦，你便可以成爲一名聰明的網絡用戶：

- 安裝最新病毒識別碼和惡性程式碼定義檔的抗電腦病毒和惡性程式碼偵測和修補軟件，並定期掃描全部的系統。
- 安裝個人防火牆軟件，保護電腦以避免網絡入侵。
- 使用最新保安修補程式於所有軟件和應用系統中。
- 執行電腦密碼保護且定期更改密碼，以避免電腦被未經授權的使用。
- 執行互聯網下載的軟件是很危險的一件事，要特別注意，除非該軟件來源是已知和可信任的。
- 沒必要時不要揭露你的個人資料。
- 當使用完網絡後，要儘快從互聯網離線。

## 30. 資訊保安管理包含什麼?

資訊保安全管理是一項牽涉預防、偵測、反應程序的綜合體，它是反覆活動和程序的循環，需要無間斷的監控和控制。該循環包括以下活動：

- 評估保安風險: 執行保安風險評估，以確定威脅、漏洞和影響。
- 推行和維護安全的架構: 定義和發展政策、分配責任和應用保衛措施。
- 監控和紀錄: 持續地監控和紀錄，如此，當應付保安事故時，才能採取適當的安排。
- 覆檢和改善: 定期執行覆檢和保安審計，確保適當的保安控制有符合保安要求。

### 31. 我們要如何知道機構內的資訊是否安全?

你應該依據以下各點自行檢查，以找出你機構內的資訊是否安全：

- 我的機構是否有自信，機構內的網絡伺服器正妥善地被訓練完善的人員保護和管理？
- 我的機構是否有清楚的政策列明誰被准許接達何種資訊？
- 我的機構是否已指定人員負責資訊保安全管理？
- 我的機構是否已利用保安工具，例如防火牆和加密工具？
- 我的機構是否已有計劃緊急應變和從災害中復原，且定期覆檢這些計劃，以確定它們符合持續業務運作計劃？

假如以上五項問題都是負面答案，你的機構將可能依然面臨許多保安漏洞的威脅。

### 32. 一般機構的網絡與無線網絡的差別是什麼?

無線局部區域網絡 (WLAN) 是一種使用高頻無線波的局部區域網絡，而非使用電線作為設備之間溝通的橋樑。WLAN是一種彈性的數據溝通系統，用來作為有線LAN的替代品或是延伸。無線資訊的溝通使人們更容易地及自由地互動。隨著科技的進步，無線接達能力已使得越來越多辦公室或公共場所部署該項科技。

WLAN以IEEE 802.11標準為基礎，之後，例如 802.11a、802.11b 和 802.11g等不同的標準進化來支援不同的頻率範圍和頻寬。有兩個IEEE相關的標準：802.11x 和 802.11i。802.11x是一項連接埠接達控制規約，提供IEEE網絡的保安架構，包含以太網和無線網絡。而 802.11i標準是創造來作為與IEEE 802.11x一起操作的無線規格保安功能。

WLAN應該與足夠的認證和傳送加密措施一起使用，並搭配適當的保安全管理過程和作業實務。

### 33. 當使用公共/城市的無線網絡時，什麼是個別用戶最佳作業實務?

- 時常將城市無線服務視為不可信賴的網絡，假如當SSL的加密通道不可行時，不要送出你的個人/敏感資料。在沒有虛擬私有網絡(VPN)保護或其他類似加密機制確

保通訊保密的前提下，從城市無線服務接達到公司的伺服器並不是一項明智之舉。在使用VPN時，應該停止使用分割通道技術（分割通道允許用戶在連接到互聯網的同時，保持到一個VPN的連接）。

- 當連接到一個公共熱點(hotspot)時，用戶可能被導向到一個捕獲門戶(Captive portal)的網頁。攻擊者可能會設置虛假的捕獲門戶網頁，以獲取敏感資料。因此，通過核實網站的證書，鑒別捕獲門戶網頁的真偽顯得尤為重要。
- 有些作業系統提供為用戶創造一個首選無線網絡清單。一旦這份清單確定後，該系統將不斷尋找清單裡的首選網絡，並嘗試自動連接到首選網絡。通過獵取這種個人設備發送出來的資訊，攻擊者可以設置一個假的無線接駁點來回應受害者設置的首選網絡清單裡的無線網絡連接請求。這樣，用戶會自動連接到入侵者的無線網絡。為防止這種類型的攻擊，首選網絡清單功能要被關閉或移除。
- 應避免電腦與電腦之間的對等無線聯網。隨機操作模式（Ad-hoc Mode）能使個人無線設備與其他電腦直接無線連接，但這種方式對未授權的連接入只提供最低限度的的保安。為防止攻擊者獲取資訊資源，個人無線設備應該關閉這個功能。網絡資源分享功能也應該關閉。
- 在連接到城市無線網絡服務時，為了保護自己的電腦，個人用戶應該運行著帶有最新電腦病毒識別碼的抗電腦病毒/抗間諜軟件，應用最新的系統修補程式，以及開啓個人防火牆。儲存在任何無線設備裡的敏感和機密資料，應以嚴格的加密演算法進行加密。在公共場所連接到互聯網時，常用的安全措施如開機密碼或系統登入認證、和密碼保護的螢幕的保護裝置程式等也應該使用。

#### 34. 當使用即時通訊(IM)時，住家用戶應採取什麼預防措施?

- 在即時通訊上不要設定自動接收檔案傳輸。
- 在開啓透過IM接收的任何檔案之前，你應要查證寄送者確實寄送檔案給你，此外，在開啓該檔案前，確定檔案已被抗電腦病毒軟件掃描過。
- 絕不點擊在IM上不信任/未知的URL連結。
- 絕不透過IM寄出個人或敏感資料，即使有充分理由這樣做，也要確定加密該資料。
- 使用最新修補程式隨時更新IM軟件(和其他系統零件)，開啓個人防火牆，安裝具有最新病毒識別碼和最新惡性程式碼定義的抗電腦病毒軟件，以及安裝偵測和修補引擎。

#### 35. 當使用對等式(P2P)科技時，住家用戶應採取什麼保安措施?

- 電腦要安裝抗電腦病毒程式和個人防火牆，確定定期更新病毒識別碼、惡性程式碼定義，以及偵測修補引擎。
- 使用最新保安修補程式。

- 移除電腦所有不必要的用戶特權。
- 爲了正常運作，對等式(P2P) 應用程式需要在防火牆上開啓許多連接埠，假如不需要分享檔案，應關閉不必要的連接埠區域。
- 假如需要使用對等式下載，建議你在完成下載後，離開對等式應用程式。
- 不要從不信任或可疑來源下載檔案。
- 絕不下載兒童色情圖片和其他非法物件，包括盜版軟件。

### 36. 當使用FON時，用戶要如何保護自己?

- 改變預設設定值，例如管理密碼和WPA加密匙，以加強FON接達點的保護。
- 應在連接於家居網絡的所有電腦裝置安裝防火牆，以抵禦可能來自私人無線局部區域網絡的攻擊。
- 在連接到 FON Wi-Fi 網絡之前，應裝設和運行充足的保安措施（如安裝抗電腦病毒軟件、最新的保安修補程式及個人防火牆）。
- 應採用加密技術保護儲存於流動裝置的敏感或機密資料，以及爲連接至公司伺服器的通訊或其它交易服務提供保障。
- 接駁點必須時常安裝最新的修補程式，如你正使用 La Fonera 路由器，應確保從 FON 提供的自動固件更新功能操作正常。

### 37. 如何安全配置無線寬頻路由器?

- 更改預設用戶名稱和密碼，因爲預設值往往容易被猜出來。有一些製造商也許不會讓你更改用戶名稱，但你至少應要更改密碼。
- 建議用戶應關閉 SSID 廣播或增加「Beacon Interval」至最大值。
- 預設的 SSID 應予以更改，新的 SSID 不應以自己的名字或其它個人資料命名，否則將有助攻擊者收集你的資料。
- 儘可能避免使用 WEP。如果裝置支援的話，應採用 WPA2 或 WPA。
- 不應採用共享式密碼匙認證，反而應考慮 802.11i 標準中訂立的強化相互認證。
- 建議啓動 MAC 位址過濾作爲另一層保護。
- 盡量關閉 DHCP 功能，因爲 DHCP 容易讓惡意攻擊者接達無線網絡。

### 38. 比較因漏洞引起的風險和安裝修補程式的風險。假如管理者決定不應用修補程式，又或沒有可行的修補程式，有什麼其他可行的常見補救性控制?

當評估是否實施一個安全的修補程式時，應該評估安裝修補程式所帶來的風險。小心地比較保安漏洞所造成的影響和安裝修補程式的風險。此時應要準備其他的補救控制措施，可能包括：

- 關掉與保安漏洞相關的服務或功能
- 採用或增加接達控制
- 增加系統的監控以偵測和預防實際的攻擊

### 39. 選擇修補程式管理解決方案的標準是什麼？

當考慮建立一個健全的修補程式管理解決方案時，除了考慮特定用戶和商業需求 (包含產品功能和預算限制) 之外，機構也應該將以下各點列入考慮因素：

#### 較少漏洞

有些修補程式管理產品的保安漏洞比其他的產品多，機構應選擇看起來較不可能成為保安漏洞的解決方案，從而減少修補其軟件的次數。。首先應先進行一些獨立性的產品確認研究，複雜的產品意味著較多的程式和服務，反而可能會帶來更多的保安漏洞。選擇一個簡單但發展成熟的產品可能比較明智。

#### 系統相容性

有一些修補程式管理解決方案是基於代理程式(agent-based)的，而有一些則是無代理程式(agent-less)，如果代理程式被安裝到許多電腦上時，機構應該評估對整個系統的影響（例如表現、穩定性和相容性）。。

#### 供應商對新保安漏洞的反應

機構也關注解決方案供應商對新保安漏洞之修補及更新的回應速度。

#### 簡易的部署與維持

修補程式管理的解決方案越容易部署和維持，則機構所付出的成本就越低。

**審計追蹤**一個良好的修補程式管理解決方案應提供廣泛的事件記錄功能，協助系統管理員更容易追蹤軟件修補和修補程式在個別系統的狀態。