資料來源：資訊安全網

資訊保安管理
妥善保障個人／公司資產

一、何謂資訊保安？

無論對個人或企業來說，資訊形同一種資產。資訊保安是指對這些資產加以保護，以達到「C-I-A」的目的：

機密性（Confidentiality）：保護資訊免向未經授權人士披露。	
例子	個人：你交給某一網站的個人資料應只供該公司的指定員工存取，作為事先同意的用途。其他人士不可出於好奇而取用該等資料，或將之用作非法用途。
	企業：銷售數字或客戶數據等敏感資料，應只供高級管理人員及銷售團隊等已獲授權人士存取，其他營運部門則不得擅用。
完整性（Integrity）：保護資訊免受未經授權人士更改。	
例子	個人：你交給某一網站的個人資料，不應在數據傳輸過程中或被該網站公司更改。
	企業：重要文件或數字不能在沒有知會的情況下被未經授權人士更改。
可用性（Availability）：讓資訊可供已獲授權人士在需要時取用。	
例子	個人：你應可存取及檢視寄存於某一網站的個人資料。
	企業：已獲授權的高級管理人員應可在需要時存取銷售數據；而客戶亦應可在需要時取得寄存於該公司的個人數據。

資訊保安與我何干？

資訊保安與我們息息相關，因為每個人很多時都會面對資訊保安的風險。如果想知道個人／公司／機構面對的風險有多高，可參考以下的資訊保安自我檢查表。

假如沒有採取以下行動	漏洞	威脅	風險	保安注意事項
1. **下載電子郵件時，用抗電腦病毒軟件予以掃描**	缺乏邊線保護	• 電腦病毒透過電子郵件信息和附加檔案進行侵襲 • 惡意程式碼	• 軟件及數據毀壞 • 拒絕服務	• 機密性 • 完整性 • 可用性

UPM Finesse Classic Matt, 90 gsm

假如沒有採取以下行動	漏洞	威脅	風險	保安注意事項
2. 定期更新抗電腦病毒軟件	缺乏定期更新抗電腦病毒軟件	• 惡意程式碼 • 電腦病毒侵襲	• 軟件、數據及設施毀壞	• 機密性 • 完整性 • 可用性
3. 定期製作檔案備份	缺乏備份設施及過程	• 通訊服務故障 • 技術故障	• 數據及設施毀壞	• 完整性 • 可用性
4. 極少轉寄那些要求我向他人發出警告的電子郵件	缺乏證明	• 惡作劇電子郵件和濫發電郵	• 耗費時間閱讀 • 耗費網絡帶寬 • 拒絕服務	• 可用性
5. 為電腦和電子郵件帳戶設定複雜的密碼，並且定期更改	缺乏足夠的存取保安措施	• 未經授權的數據存取 • 未經授權的撥號存取 • 盜竊及詐騙	• 數據損失 • 數據及軟件毀壞 • 他人以你的名義作非法行為	• 機密性 • 完整性
6. 定期為電腦安裝保安修補程式	缺乏定期更新保安修補程式	• 惡意程式碼 • 電腦病毒侵襲	• 軟件、數據及設施毀壞 • 他人以你的名義作非法行為 • 拒絕服務	• 機密性 • 可用性 • 不可否認性

資訊保安與公司何干？

要知道公司的資訊是否已經妥善保安，可檢閱下列幾點說明：

1. 公司的網頁伺服器放置於安全的地方，並由訓練有素的人員來管理。
2. 公司訂有清晰的政策，規定甚麼人士有權存取甚麼類型的資料。
3. 公司已派員負責資訊保安、更新、備份及維護等工作。
4. 公司有使用保安工具，例如防火牆、加密技術等。
5. 公司已制訂緊急應變計劃及運作復原計劃。

假如以上問題並非全部答「是」，那你的公司可能仍然存有備受威脅的資訊保安漏洞。

保安威脅舉例及相關的保安要點

	受影響的保安要點		
	機密性	完整性	可用性
拒絕服務			*
電源供應故障			*
惡意程式碼	*	*	*
盜竊及詐騙	*		*
網站入侵	*	*	*
未經授權存取數據	*	*	

堵塞保安漏洞並非一個複雜而昂貴的程序。首先，你要劃定公司所需的保安管理範疇，評估公司所能接受的風險程度，因為這樣有助決定符合業務需要的保安管理範圍。

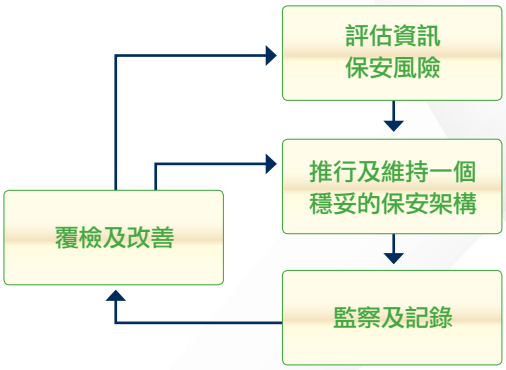
二、資訊保安管理周期

資訊是個人／公司／機構業務最珍貴的資產。使用正確的預防及保護措施，可以減少資訊備受攻擊的成功機會，否則可能招致巨大的金錢損失。某些損失更可能無法挽回，例如因洩露了機密資訊予競爭對手而損失了一宗生意。

透過有效的資訊保安管理，可以為公司提供最佳的策略和合乎成本效益的解決方案，全面保護珍貴資料。資訊保安管理的好處是容易管理，而更重要是可以盡量減低被攻擊的風險，最終有助節省成本。只要簡單地把保安預算列作個人／公司／機構預算中的一個強制性部分，即可盡力保護資產。

資訊保安管理涉及綜合性的預防、偵測及應變過程，是一個包含了反覆活動和過程的周期，需要不斷的監察和控制。這個管理周期大多數應用於機構層面上，但亦可應用於業務上不同的職務和單位，例如營業部、顧客服務小組等，以預防財務損失。

要使資訊保安管理收效，機構中所有成員的參與、理解和支持是計劃成效的關鍵因素，因此這並不是資訊保安部孤軍作戰的工作。



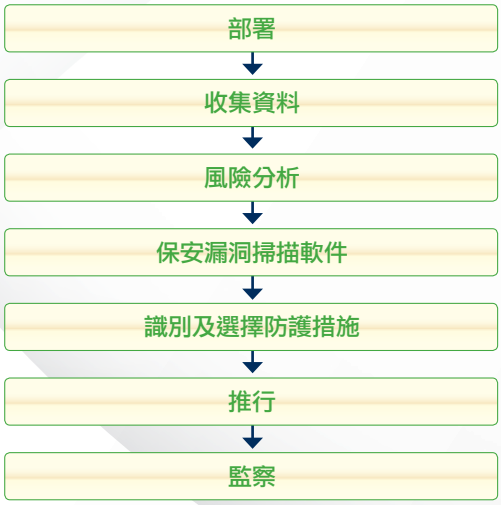
評估資訊保安風險

資訊保安管理周期始於評估資訊保安風險，保安風險評估一開始時便要進行，以找出需要甚麼的保安措施。這是初步評估和識別與保安弱點有關的風險及結果，並提供一個管理基礎，以確立具成本效益的保安計劃。

根據評估結果，便可推行適當的資訊保安防護措施，以維持一個穩妥的保安架構。這包括制訂保安政策和指引、委派保安職責及推行技術性的資訊保安防護工作。

緊隨這個步驟的是周期性的遵行情況覆檢和再三評估，以確保保安措施被正確地執行，以達到用戶的保安要求和應付科技及環境上的急劇轉變，這有賴持續性的回應和監察。覆檢工作可以透過定期的保安審計來進行，以找出必需改進的地方。

通過對一系列關注事項的評估，便能識別出甚麼資產需要保護、它們的相對重要性、迫切性的緩急次序和所需的防護程度。以下的流程圖展示出保安風險評估的主要步驟。



UPM Finesse Classic Matt, 90 gsm

部署

在開始保安風險評估之前，需要部署適當的準備、監察和控制工作。部份主要項目需要先行定義：

- 計劃範圍及目的：評估範圍可以涵蓋防護某些業務上的職務，例如顧客服務部、信貸部和營業部等。
- 背景資料：任何有助評估的相關資料，例如財務單據、組織結構圖和公司宗旨等。
- 限制：例如財政預算、成本、時間和科技等。
- 參與各方的任務及職責：為有份參與的所有組員界定及委派職務。
- 途徑及方法：有關風險衝擊的定性及定量分析、保安問題的影響及適當的保安措施。
- 計劃規模及時間表：計劃所涉及的成本和員工數目，以及推行評估報告中概述的各主要活動所需的時間。

收集資料

為找出風險所在，需要收集相關資料作進一步分析，並了解目前的系統和環境。所需收集的資料類別包括：

- 保安需求和目標
- 系統及網絡結構和基建
- 在網頁上讓公眾使用的資訊
- 實質資產，例如硬件設備
- 系統，例如操作系統、網絡管理系統等
- 內容，例如數據庫及檔案
- 應用程式及伺服器資料
- 網絡，例如所支援的規約及所提供的網絡服務
- 接達控制
- 過程
- 識別及認證機制
- 有關政府法律及條例訂明最低要求的保安措施
- 明文規定或非正式的政策和指引

有關資料可以透過不同途徑來收集，例如實地探訪、小組討論、多層式訪問、調查、問卷、主要項目核對清單和實地考察。

風險分析

風險分析有助決定資產價值及其相關風險。因此，保安風險評估及審計可幫助辨識網絡的保安弱點。以下列出有關過程重點：

- 資產識別及估值：包括有形及無形資產，例如硬件及商譽。
- 威脅分析：找出威脅，並決定它們出現的可能性，以及危害系統和資產的潛在能力。
- 漏洞分析：找出並分析系統及環境上的漏洞，例如以保安漏洞掃描軟件找出技術性的保安漏洞，亦可以就接達能力及獲受權用戶的數目來衡量。
- 資產／威脅／漏洞圖譜分析：找出可能導致風險的資產、威脅和漏洞的不同組合和其相互關係。
- 評估影響力及可能性：估計可能出現的危害或損失的整體程度及威脅發生的次數。
- 風險結果分析：利用定性與定量方法，以及矩陣方式來正確分析及演示風險結果。

保安漏洞掃描軟件

保安漏洞掃描軟件可以偵測到資訊系統（包括電腦、網絡系統、操作系統以及應用軟件）各種保安漏洞。這些保安漏洞可能源於軟件生產商、系統管理活動或用戶一般日常活動。一般來說，保安漏洞掃描軟件：

- 可以及早偵測到已知的保安問題及加以處理。
- 可以協助辨認可能未經批准便跟網絡連接的虛假機器。
- 可以驗證網絡上所有設備的清單。這清單包括設備類別、操作系統版本及程式修補程度、硬件配置及系統其它相關資訊。

然而，保安漏洞掃描軟件也有一些限制：

- 只能提供快照（snapshot）：保安漏洞掃描軟件只能夠評估一個短時期內有關系統或網絡保安的狀況。由於新的保安漏洞的不斷出現，以及改變系統配置亦可能導致保安漏洞，所以定期執行掃描是必須的。
- 需要人為判斷：保安漏洞軟件只能根據數據庫預裝的插件（plug-in）報告保安漏洞，而不能決定掃描結果是假陰性（falsenegative）或假陽性（falsepositive）。因此，每次掃描完成後，數據都要經人為判斷。
- 保安漏洞軟件只能發現已知的保安漏洞，它不能辨認出其他的保安威脅，例如那些實體、操作或程序上的威脅。

進行保安漏洞掃描的貼士	
掃描軟件的位置（適用於網絡掃描軟件）	掃描軟件處於防火牆之內還是外面，都會影響掃描結果。因此，為了得到較完整的保安狀況，進行內外掃描是有需要的。
埠掃描的範圍（適用於網絡掃描軟件）	埠掃描能夠偵測出哪些埠是可供使用的（即服務正在聆聽的那些埠）。因為公開的埠可能意味著有保安弱點，埠掃描往往是攻擊者的一項偵察技術，因此保安漏洞掃描必須包括埠掃描。然而，一些保安漏洞掃描軟件已預設埠掃描範圍，例如只掃描0至15,000的埠，系統管理員有需要知道預設埠掃描範圍，以確保所有必須被掃描的埠都包括在內。
設置底線	一般的保安漏洞掃描應包括初步評估、執行建議糾正及再次評估。為確定糾正是否有效，較妥當的做法是保存所有掃描記錄（即制訂一個有效的準則），然後將每次的掃描結果跟準則比對，以進行趨勢分析。
掃描後及持續措施	掃描過程只是良好評估的一部份，正確詮釋掃描結果是重要的，因為這才可以確保保安漏洞能獲辨認及修正，跟進行動的優先次序亦應同時予以制訂。
掃描過程的潛在威脅	掃描對資訊科技系統可以構成威脅，例如所有插件（包括高風險的插件，例如拒絕服務掃描）都啟動時，掃描可能會令脆弱的伺服器崩潰，所以進行掃描前有需要作風險評估及周全計劃。通常，就一個未投入生產的系統而言，掃描時可以啟動包括高風險在內的插件；此外，利用網絡保安漏洞掃描軟件進行掃描時，會產生大量系統要求及網絡傳輸。進行掃描時，管理人員要注意若干群組的系統及網絡的性能有沒有下降。
處理掃描結果	掃描結果包括系統漏洞的資訊，萬一外泄便會容許攻擊者直接針對漏洞發動襲擊，因此應該把掃描結果保管在安全的地方，或予以加密防止未經授權的接達。若評估程序涉及第三者，機構有需要確保對方可信賴程度，而評估所發現的資料及專利的資訊便須安全地保存。
掃描過程的政策及程序	惡意或不恰當使用掃描工具，對資訊系統可以構成重大威脅，甚或導致極大傷害。因此，有需要因應保安漏洞評估工具由誰使用、如何及何時使用而制定政策及程序。在進行掃描前，有關政策規定可能包括預先的安排或通知，獲得管理層批准甚至是法律批准。沒有人可以在未經批准下進行保安漏洞掃描。

識別及選擇防護措施

檢討保安風險評估結果後，便要定出防護措施，並評估措施能否把識別出來的威脅及漏洞的可能性和其影響力，有效地減低至可以接受的水平。防護措施可以是技術性或程序性的，以下列出部份防護措施的例子：

- 重新配置操作系統、網絡組件及設備，以修補在保安評估過程中找到的漏洞。
- 推行密碼措施或安裝認證軟件。
- 使用加密或認證技術來保護數據傳輸。
- 制訂或加強保安政策、指引或程序，以確保獲得有效保障。

推行及維持一個穩妥的保安架構

隨著從保安風險評估過程中取得風險評估結果，資訊保安管理周期便進入推行及維持的階段，以推行適當的保安防護措施來維持一個穩妥的保安架構。這包括制訂保安政策和指引、委派保安職務，以及推行技術及行政上的保安防護措施。所有這些步驟均大大有助保衛你的業務資產。

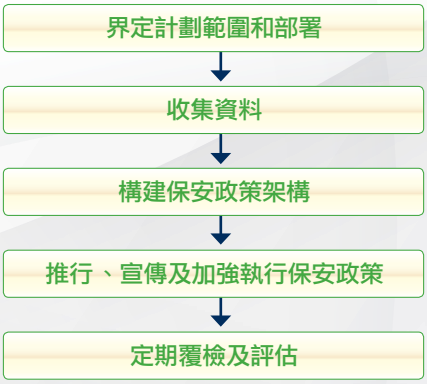
制訂及推行保安政策

保安政策乃就資訊保安設定基本守則，這些守則是強制性的，及必須由整家機構的人員遵守。由於每家機構的保安需求均有不同，故其保安政策亦會各異。因此，最重要是保安政策應合乎該機構的保安需求、業務目標和業務政策，才可得到支持和落實施行。

事實上，保安政策可以非常高層次而跨越個別科技界限，又或非常詳細而特指某一科技界限。保安政策可以分為三個基本類別：

- 程式層面政策
- 問題特定政策
- 系統特定政策

系統特定政策著眼於管理某一特定系統的政策問題，只會處理一個系統，而程式層面政策及問題特定政策兩者則會處理廣泛層面上的問題，通常包含整家機構。選擇制訂哪一種保安政策乃視乎機構的需要，但最重要的是政策必須定出方向，以作為作出其他較低層次決策時的基礎。



資訊科技保安政策應涵蓋公司對可以適當使用其電腦及網絡資源的預期，以及防止和應付保安事故的程序。在草擬政策時，應要考慮公司本身的保安需求。草擬政策時應考慮以下範疇：

- 公司目標及方向
- 現行政策、守則、規條及香港政府的法例
- 公司本身的要求和需要
- 推行、分發及加強執行事宜

（如需參考有關資訊保安國際認可標準、指引及有效保安作業實務指引，可前往資訊安全網的網站，詳情請瀏覽：www.infosec.gov.hk）

制訂及推行管理和行政程序

根據保安政策所定的方向和範圍，便可設定管理及行政程序來支持政策的推行。這裡是部分主要的管理及行政活動。

委派任務及職責

制訂資訊科技保安政策需要來自多個職位及職務單位人士的積極支持和持續參與。因此，在

保護公司資訊及系統資產時，必需明確界定責任及適當委派職責，並會視乎業務需要和環境而涉及以下職務，包括資訊科技保安主任、高級管理人員、資訊擁有人、資訊系統用戶。

指引及標準

指引及標準是推行保安政策的工具。由於政策可能在一個廣泛的層面上擬訂，故必需制訂有關標準、指引和程序，以給予用戶、管理人員、電腦人員及高層管理人員一個較為清晰的方法，去推行保安政策及達成部門的任務。

保安認知和培訓

保安認知對確保有關各方面能了解風險、接受和採納良好保安作業實務是十分關鍵的。培訓和教育可以為用戶、制訂人員、系統管理人員、保安管理人員及任何有關方面，提供推行保安措施所必需的技術和知識。除非用戶或有關方面作出承諾和進行溝通，否則沒有政策可以落實推行。這是指用戶及有關方面：

- 已透過簡報或介紹會得悉有關政策；
- 已獲邀參與制訂政策建議書；
- 已跟從政策所需接受的技術培訓；
- 覺得保安措施是為他們的利益而制訂；
- 定期提醒、注意及獲知最新的問題；
- 已簽署確認；及
- 已獲得適量的政策指引。

落實執行

這是指施行來自推行政策的權力，以及糾正侵犯此等權力的工作。公司應設定程序，為調查破壞保安系統的事宜上提供及時的協助。成立公司事故管理小組和設定保安事故處理程序，均能改善保安政策的效用。

各方的持續性參與

一個有效的保安政策亦有賴用戶與公司之間持續性地交換資料、諮詢、協調和合作。從有關方面引入標準、方法、業務守則及資訊科技其他方面的專門知識，將有助保持保安政策追上時代和切題。

選擇及推行技術措施

除了管理和行政過程外，推行保安政策可能涉及技術措施的使用，透過選擇和推行合適技術和產品。技術措施應在正式操作前接受適當的測試。

選擇及推行

- 抗電腦病毒軟件
- 接達控制系統
- 防火牆
- 入侵偵測系統
- 加密技術
- 密碼匙的管理及密碼匙分發系統
- 網絡管理系統及保安管理系統

操作

- 採取適當程序來處理問題
- 採取適當程序來追蹤系統活動和警告
- 採取適當程序來監察保安基建的健全狀況
- 採取適當程序來處理及控制變動

監察及記錄

除了要展開推行及維修工作來提供穩妥的保安架構外，也要恒常地進行監察及記錄，才能在處理保安事故時作出適當的安排。此外，日常運作如用戶在使用資源或資訊時的接達嘗試及活動，也要妥善監察、審計和記錄，例如個人用戶身份識別需要包含在審計記錄中，以加強個人責任。每位用戶在使用公司資源時應了解其責任，並為本身的行為負責。主要活動包括：

- 維持保安事故處理及匯報程序。
- 維持主要業務系統及重要應用程式的審計追蹤。
- 維持操作系統的事件記錄及誤差記錄。
- 維持進入經營場址的訪客或嘉賓的出入記錄。
- 維持記錄以追蹤重要業務活動的授權情況。

覆檢及改善

持續性覆檢綜合了資訊保安管理周期中各項主要活動及過程，例如評估資訊保安風險、推行及維持一個穩妥的保安架構、監察及記錄等，以找出需要改善的地方。這一系列對於遵守情況的周期性覆檢和重新評估，確保能適當地執行保安措施以達至保安要求，並應付技術和環境上的急劇轉變，這意味著需要持續的回應和監察。檢討工作可以透過定期的保安審計來進行，並在一個持續性的基礎上進行監察和檢討保安作業實務及策略。

保安審計

保安審計是一個重複性的覆核過程，以確保在任何時候保安措施均被妥善地執行。保安審計的工作比保安風險評估進行得更為頻繁，旨在找出目前環境是否按照既定的保安政策而受到安全保護。

保安審計的目的

- 提供恪守保安政策的證據。
- 檢查及分析系統及操作環境的防護。
- 評估保安設計的技術及非技術性推行情況。
- 確認所有保安功能是否適當或不適當地整合及操作。

審計步驟

- 界定審計範圍及活動
- 部署
- 收集審計數據
- 進行審計測試
- 匯報審計結果
- 保護審計數據及工具
- 改善及跟進

保安覆檢控制

機構應積極及定期監控和覆檢服務供應商及用戶的保安控制遵行情況，並保留審計服務水平協議所界定責任的權利、安排獨立第三方進行審計。為了確保有效及全面地進行檢討，機構須保存：

- 一份載有服務內所有的伺服器和系統的清單，以及那些系統會儲存敏感或個人資料。
- 一份服務供應商支援人員的名單，包括授予的用戶帳戶和接達權限。
- 一份已移交給服務供應商的資料（尤其是敏感或個人資料）的清單。■

如果想了解更多有關資訊保安管理的內容，請參閱以下的資料：

資訊安全網

網址：www.infosec.gov.hk
電郵：webmaster@infosec.gov.hk
傳真：(+852)2989-6073
地址：香港數碼港道一百號數碼港一座六樓