電郵安全

www.aoema.org

感到網上世界
不安全?

這本指引可助你
在網上安全通訊。

電郵安全

目 錄

互聯網現已成為廿一世紀的重要溝通工具。目前全球網民超過三億人，互聯網可說掀起了一場通訊革命。它改變了人與人之間的關係，也改變了我們周遭的環境。現在，我們可以接觸到過去遙不可及的人物、地方及資訊。企業及政府精簡運作、祖父母與身在地球另一面的孫兒保持聯繫、學生與遠在外太空的太空人溝通 —— 這些目標全部透過互聯網逐一實現。互聯網已經無處不在，充分滲透了生活各個層面。互聯網確實在改變我們的生活模式。

*不過，對於網上這個新領域，你可能有些擔心。我們時常聽到病毒、特洛伊木馬、侵犯私隱、客戶保障不足、「dot.com詐騙(scams)」，甚至一些叫「網上臭蟲(web bugs)」的東西 —— 這些問題不禁令人擔憂。可是，這就是未來的發展大勢，要完全漠視網上世界越來越困難。對付這些潛在問題的最好方法，就是學會怎樣**防止**這些問題發生。*

簡 介

3

現在，電郵已成為一種不可或缺的商務工具，大部分人都覺得沒有電郵不行。電郵已成為當今公認最具效率及效益的通訊方式，適合各類工作或不同規模的機構。而作為關鍵的商務應用程式，電郵能夠帶來許多好處，以及改善公司的收益。然而，電郵亦有不少潛在問題，例如病毒、黑客入侵系統、濫發電郵(spam)、泄露機密資料及侵犯版權等。不過，只要你遵循本小冊子的建議，即時採取措施，就能保護公司免受上述威脅。

「電郵安全」是「網上安全」的姊妹篇－專門解答安全暢遊網絡世界時所需考慮的四個關鍵問題：

- 怎樣才能確保我的電腦安全呢？
- 怎樣才可以保護我的個人資料呢？
- 我怎樣才能信賴網上交易呢？
- 我怎樣才可避開網上的煩擾、陷阱和詐騙呢？

「電郵安全」對任何電郵用戶來說都是寶貴資源。不過，它的主要對象還是商業用戶。本小冊子的內容包括：

- 信息策略
- 市場推廣策略
- 威脅
- 指引
- 政策考慮因素

本小冊子的目標對象是負責制訂電郵政策的公司行政人員及高級職員，內容包含制定政策文件時所需闡明的一切事項，並提供有關建議。而對於其他商界人士，本小冊子亦提供最佳作業實務指引，讓他們發揮電郵的最大效益，並建議如何**防患未然**。

如欲了解所有課題的進一步資料及最新內容，包括亞太經合組織 (APEC) 個別經濟體系的特定參考資料，請參閱 **www.aoema.org/safetymail**。

做做兩分鐘「電郵安全」測驗，防患未然

	有	否	
你有沒有安裝抗電腦病毒軟件?	☐	☐	參閱第8頁
你有沒有最新版本的抗電腦病毒軟件?	☐	☐	參閱第8頁
你知道你的病毒定義是否最新嗎?	☐	☐	參閱第8頁
你有沒有在個人電腦及內部網絡伺服器上安裝防火牆?	☐	☐	參閱第8頁

網上通訊是否讓你的公司承受風險?你可能認為沒有，或者尚未意識到問題存在。不過，要肯定的話，就做做這個兩分鐘「電郵安全」測驗吧!從百忙中抽出兩分鐘，就能在問題發生前防患未然，節省大量時間及金錢。電郵問題對你的公司、管理層及僱員都有潛在的影響。

4

兩分鐘「電郵安全」測驗

你有沒有最新版本的防火牆軟件?	☐	☐	參閱第8頁
你有沒有為僱員準備書面的政策文件，解釋如何進行網上通訊?	☐	☐	參閱第6頁
你有沒有教導僱員這份政策的內容及其含義?	☐	☐	參閱第28頁
你有沒有正式的商務電郵存檔辦法?	☐	☐	參閱第27頁
你的商務信息中有沒有包括免責聲明及聯絡資料?	☐	☐	參閱第22頁
有沒有管理離職僱員的電郵地址的程序?	☐	☐	參閱第24頁

這個測驗非常簡單 —— 對於以下任何一條問題，你的答案是「否」的話，我們十分建議你閱讀這本小冊子，加深對有關課題的認識。

電郵安全

課題及政策考慮因素

6

網上通訊 (Communicating on the Internet)

信息策略

電郵

隨着互聯網日益普及，電郵已成為不可或缺的商務工具。如今大小企業均利用電郵提升通訊效益及效率。電郵容易使用，但亦容易濫用。許多公司並未意識到這一點，忽視管理及控制使用電郵的環境，最終出現嚴重問題。

小處來看，電郵問題能夠損害一家公司的聲譽。更嚴重的情況是公司可能會遭受幾百萬美元的法律訴訟。這樣說似乎有些危言聳聽，但它確實會發生，而且一旦發生就必然成為頭條新聞。然而，不論是個人或公司，只要能夠妥善處理這類問題，並實行合適的監管措施，就幾乎可以完全杜絕這些情況。

使用電郵其實利多於弊。正如其他業務範疇一樣，成功的關鍵在於妥善管理。

即時通訊

即時通訊是一項服務：它讓用戶知道哪些聯絡人正在上網，並讓他們即時進行通訊，方法通常是在另一個視窗中打字發送信息。利用即時通訊，你可以建立一份聯絡人清單；當其中任何人上網時，系統就會提醒你可以與他們通訊。

過往，即時通訊主要用於個人之間的聯繫。而最近市面亦有多款套裝軟件，讓公司建立自己的內部及外部即時通訊系統。

在商業世界裏，即時通訊是十分有用的工具，普遍應用於管理內部事務及與客戶保持緊密接觸。即時通訊是一種新穎有趣的網上通訊方式。它跟電郵一樣，需要加以管理，以及針對其通訊特性的政策配套。

簡短訊息傳遞

你可以透過短訊傳遞(簡短訊息傳遞)發送不超過160字符的短訊到數碼電話(流動電話/手機),所需的只是一部電腦或另一部數碼電話。如今,許多企業都有採用短訊傳遞,方法包括:

- *通知僱員接收話音郵件信息*
- *通知銷售員客戶的查詢及聯絡資料,以便回電*
- *通知醫生病人的緊急病情*
- *通知服務人員下一個工作時間和地點*
- *通知司機臨時到某個地方接載乘客*

在一些地方,短訊傳遞已經成為生活不可或缺的一部分。商界人士、學生及家長都利用短訊傳遞來改善通訊。許多電話公司如今亦向企業提供短訊傳遞服務,讓他們可以向僱員及客戶發送短訊。

憑藉人們的少許創意,短訊傳遞很快便成為有效商業通訊工具,為企業提高效率之餘又能節省資金。雖然是短短的160字符,已效用無窮。世界各地許多小型企業便單靠短訊傳遞來管理所有企業通訊。當然,正如電郵和即時通訊一樣,短訊傳遞也需要一套管理政策。

過尤不及

儘管電郵、即時通訊及短訊傳遞都是有效的通訊工具,應該在公司佔一席位,不過使用時亦應審慎明智。有時候,打個電話或面對面會談或許更合適。這些先進科技只能是整個通訊策略的一部分。管理層應提防任何僱員過份倚賴某一種通訊方式。作為客戶,我們亦試過打電話無人接聽,或留下話音郵件信息後久久未有回覆。箇中滋味,想必大家也感到厭煩。

網上通訊的三個「必須」

任何使用互聯網的機構都必須做三件事。不論機構的僱員人數是兩個、兩百個甚至兩千個,這三件事都必須完成。

第一:必須制訂一套電郵通訊政策

第一步是制訂一套政策,並且時刻更新,以應付科技及用途的轉變。所謂政策,必須是書面文件,而且必須對公司的每個人都同樣適用。

第二:必須教育公司所有人

如果人們不理解規則,又怎會遵守呢?必須讓所有人知道政策的存在,而且一**定要**遵守。現在,許多公司要求僱員簽署政策文件,來表示他們知道政策的存在,並承諾遵循有關規則。

第三:必須管理及執行政策

今時今日,公司必須善用市面上的監測軟件,來確保僱員遵守公司政策。儘管這樣做帶有侵擾性,而且有點鐵腕手段的感覺,但卻是保障公司與僱員誠信的最佳辦法。如果已安裝監測軟件的話,必須讓所有僱員知道,並講解其運作方式。

8

充分發揮商務電郵的功效
(Getting the most from business e-mail)

市場推廣策略

電郵經常被稱為互聯網的「殺手級應用程式」。全球超過六億網民中，近95%或多或少都有使用電郵。商務電郵已經成為公司接觸寶貴客戶的有效方式，不但經濟實惠，而且能夠做到個人化。與傳統的直接市場推廣方式相比，電郵更加快捷、可測，同時亦可以節省成本。當然，電郵亦有壞處。除了導致「濫發郵件」劇增外，企業亦因此有可能惹上「濫發電郵者」的惡名。正當的電郵市場推廣與「濫發電郵」之間只是一線之差。

有效而又負責任的電郵市場推廣策略，必須以客為本，務求了解及回應消費者的需求。據美國在線(AOL)及其他互聯網服務供應商表示，現時約70%的電郵是「濫發郵件」。消費者受夠了這些不請自來的郵件，也實在不足為奇。這些討厭的信息亦是最常見的病毒「帶菌者」。因此，你的電郵政策必須以許可及私隱兩方面為根本。要在網上取得客戶信賴，維持業務的誠信，這是唯一的途徑。

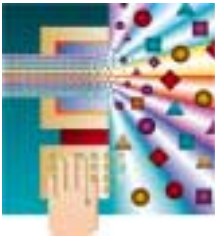
電郵市場推廣策略及技巧有很多，本小冊子不能盡錄。我們會重點講解關於許可及私隱兩方面的一些基本指引及最佳做法。這兩點都十分重要。本節可助你設計一套有效而又負責的電郵市場推廣策略，務求做到以客戶的許可為前提。

收集電郵地址數據

在開展電子市場計劃前，你首先要建立一個電郵數據庫或目標電郵地址清單。這就必須取得客戶的許可，以及投入大量的精力、時間和金錢。你或許認為，既然毋須客戶許可便可以透過郵局寄發廣告，為什麼電郵卻要多此一舉？

有兩個重要原因：第一，在某些司法管轄區，發送電郵須獲許可已屬法例規定；第二，許多互聯網服務供應商會終止對某些客戶的服務，原因是他們相信這些客戶未經許可發送商業或大量電郵。因此應緊記以下要點：

- 未經擁有人同意，切勿收集電郵地址。無論任何情況下，不要從聊天室、電子佈告板、目錄、網站或任何其他公開來源獲取電郵地址。濫發電郵者就是以這種方式建立電郵數據庫的。
- 不要使用「必須填寫」字段。很多網站向用戶提供一些表格，要求他們在不願意的情況下透露資料。換句話說，除非用戶填妥「必須填寫」字段，否則不能按下「提交」鍵。此舉不但激惱用戶，而且你收集得來的可能只是垃圾數據。
- 發出「選擇接受」的確認郵件。當用戶自願提交電郵地址以作市場推廣用途（「選擇接受」）時，應即時發出電郵確認。通常，回信軟件會自動處理這個步驟。雖然有些複雜，但是確認電郵一般能夠減低偽冒或意外註冊的機會。現時，除了發出「選擇接受」確認郵件外，最好亦要求用戶再次確認准許使用其電郵地址。這樣做不但讓客戶有機會改變主意，更有助建立商譽。
- 記錄收集每個電郵地址的日期、時間及互聯網規約地址(IP address)。就某些司法管轄區的新法例而言，這一點非常重要，因為你可能需要證明客戶是自願提交電郵地址加入市場推廣數據庫的。在訴訟中，這些記錄將有助你的公司提出抗辯。



信息傳播

為免你的電郵被誤認為「濫發郵件(spam)」，必須注重其行文格式。請留意以下幾點：

- 切勿填寫虛假的標題資料。標題內的資料可幫助用戶辨別電郵的來源，包括域名、互聯網規約地址、傳輸路徑等。濫發電郵者在標題中使用虛假資訊以

避開消費者及執法部門的耳目。正當的電郵必須顯得可信，包括使用清晰準確的標題。

- 主旨必須真實無訛。雖然廣告語句往往新奇有趣，但始終應該緊守「童叟無欺」的基本原則。切勿有意或無意地誤導你的客戶。「嗨 (Hi)」這類詞語出現在主旨中，會給人一種非常不專業的感覺（濫發電郵者亦是利用這些詞語使收件者以為電郵來自相熟的人）。

  讓用戶可以「選擇不接受」。每一條電郵信息必須包含「取消」的選擇，讓客戶有機會改變主意。

  尊重「取消」的要求。你必須確保你的系統可以處理「選擇不接受」的要求並即時回覆。

轉介電郵推廣

用得負責任的話，轉介電郵推廣可以是很強大的宣傳工具，助你建立社區、品牌及客戶名單。然而，即使是正當的推廣活動，稍一不慎，亦會被認為是「濫發電郵」，並對你的公司及品牌產生負面影響，故應採取下列步驟：

- 首先，必須肯定這種手法是否適合，到底應不應採用。
- 提醒客戶轉發時要「恰當」。請他們在轉介前三思。如果你的電郵最終落在不願接收的人手上，人家只會當你的電郵是「不速之客」。也不要提供獎勵，因為這只會鼓勵不當轉發。
- 註明轉介人的姓名。在「寄件者」或「主旨」行註明要求轉發信息者的姓名。如果沒有轉介人的姓名，收件者只會把信息當作「濫發」的電郵。
- 許可是不能夠轉移的。切勿將透過轉介所得的電郵地址視為「許可地址」，用於日後的推廣計劃。
- 記錄日期、時間及互聯網規約地址。再講一遍，這些資料對公司抗辯訴訟極為重要。

全面披露

除非客戶信任你，否則不會忠於你的公司或品牌。因此，你必須誠實披露以下幾方面的資料：

- 私隱政策。個人資料私隱已經成為當今世上備受關注的問題。歐洲聯盟 (European Union)已制訂非常嚴格的規則，監管電子世界的私隱問題。

其他國家亦紛紛仿效。這些私隱規則所涵蓋的範圍非常廣泛。制訂私隱條文前，必須認定從客戶處收集哪些資料，以及如何使用。私隱政策必須具體，客戶需要知道你收集甚麼資料，以及如何使用。

- 資料追蹤記錄。如果你會追蹤記錄別人的上網習慣（包括利用點擊進入追蹤、Cookies程式、臭蟲(bugs)及植入編碼）的話，你應該向客戶披露這類活動。
- 業務聯絡資料。如果你能夠提供背景資料及全套聯絡資料（包括實際地址、電話及傳真號碼），客戶將會對你信心大增。對於只提供電郵地址的公司，客戶通常都沒有好感，懷疑對方是否合法經營。

顧客滿意

進行電郵推廣活動時，如果能夠掌握以下竅門，將有助令顧客更加滿意：

- 發送多封電郵時，只須顯示寄件者及收件者的電郵地址。切勿在信息中顯示全部收件者的名單。只要其中一封被截獲，收件者名單就會遭濫發電郵者利用。
- 考慮發送信息的時間。有些人在下班後將信息轉發到手機上。他們一定不會喜歡在凌晨三點收到廣告。

- 鑑於數碼電話及手提設備日漸普及，信息的長度變得十分關鍵。
- 如果你委託其他公司提供電郵推廣服務，必須與該公司共同處理有關事宜。切勿順其自然，或假設有關公司不會出錯。
- 肯定你的電郵中沒有受版權保護的資料。切記要取得許可。
- 盡快回覆客戶的電郵。你可能需要增聘人手，尤其是進行推廣活動期間。

- 公司必須有專人負責回應客戶的投訴。你或許需要訓練一支專門隊伍。如果投訴越來越嚴重的話，詳細記錄互通電郵的時間及日期亦很重要。萬一客戶委託律師解決投訴，這些記錄不但十分有用，而且更是必需。
- 向客戶說明發出電郵的原因。一開始便解釋該電郵是應其要求而發，並表示他們是尊貴的客戶。
- 無論你發出電郵的目的為何，吸引客戶購物也好，介紹新產品也好，盡量減少客戶需要點擊的次數。如果郵件指示客戶進入你的網站，有關連結必須把他們直接帶到「目標網頁」，而不是你的主頁。該網頁的內容亦應該開門見山，切入主題。不要讓客戶感到困惑或失望。
- 配合目標市場，在策略性時機發送電郵。

內部測試

展開電郵推廣計劃前的最佳測試方法之一，就是親自用電郵完成每個步驟，以測試計劃的內容及系統：

- 使用不同的「濫發電郵」過濾器來測試自己的推廣郵件。
- 仔細檢查「寄件者」或「主旨」行，站在客戶的角度設身處地進行評估。
- 檢查申請加入電郵清單的過程。確保設有複核「選擇接受」的程序。
- 檢查取消加入電郵清單（「選擇不接受」）的過程。確保其運作正常及時。
- 仔細測試你的信息及「目標網頁」。檢查每條連結，以確保運作正常。最糟糕的莫過於中斷的連結。

- 確保你的網站伺服器有能力應付繁忙的網絡。
- 如果市場推廣目的是銷售新產品，必須肯定可以滿足不斷增長的產品需求。

保安至上 (Security First and Foremost)

威脅

病毒、特洛伊木馬及蠕蟲

目前，個人及企業使用電郵的情況越趨普及，因而引起了病毒製造者的垂涎，希望藉著電郵廣泛傳播病毒。犯罪分子不斷伺機破壞，不幸的是，這些犯罪分子發現，電郵及即時通訊(Instant Messaging(IM))竟是他們實施惡行的有效渠道。雖然面對這樣的威脅，但必須再次強調的是，我們總可防患於未然。

預防是關鍵所在。首先，我們應採取必要措施，確保病毒無法入侵電腦系統，並定期採取下列步驟，因為電腦系統的威脅無日無之，而且手法層出不窮，我們必須時刻提高警覺。相信大家都在報章上讀過電腦病毒的消息，其實，只要每位互聯網用戶都懂得採取以下的簡單步驟，我們便可叫一眾破壞分子銷聲匿跡。只要不讓他們興波作浪，破壞分子自然也會迅速停止惡行。

病毒製造者最近其中一項「新作」，是讓病毒程式按照你的電郵通訊錄郵址，發送電郵給名單上的所有聯絡人，因此有機會將病毒傳染你的家人、朋友及業務聯繫人的電腦。請緊記，只要採納下列建議，你便可以預防電腦病毒，最終甚至可以遏止病毒傳染。

建議行動

- 必須安裝抗電腦病毒軟件(anti-virus software)，並最好設為定期自動更新病毒定義。
- 開啓檔案附件時要極為小心。正如前文所述，病毒程式所發送的信息可能看似是來自你相熟的人，因此應先行確定電郵所顯示的寄件者確實發送了附件給你。這點非常重要，因為在很多時候，只有當開啓受感染的附件時，病毒才會發揮作用。
- 即使表面看來無傷大雅的檔案，亦可能隱藏病毒。不少人因以為檔案含有圖片或笑話，而在嘗試開啓檔案時讓病毒有機可乘。為以策萬全，請緊記以下原則 —— 除非能夠確定檔案的內容或寄件者的身份，並經最新版本的抗電腦病毒程式分析，否則切勿開啓任何檔案。
- 可疑電郵一般包括：
  * 來自不知名寄件者的電郵
  * 主旨異常或可疑的電郵
  * 名稱含有非文字字符的電郵
  * 主旨帶外文（並非你的母語）的電郵，除非你認識能操該種語言的人士
  * 突如其來而又附帶檔案的電郵
- 安裝防火牆軟件，慎防病毒按照名單上的電郵地址發送電郵。防火牆軟件可自動偵查所有寄出電郵有否任何可疑活動。
- 遇上含有可疑檔案附件的電郵時，應將電郵及隨附的檔案一併移除至資源回收筒，並且將其刪除。
- 開啓任何檔案附件之前，最好先用抗電腦病毒軟件程式檢查檔案。
- 在電郵附加檔案時，應發送有關檔案的資料，讓收件者知道檔案來源真確。
- 切勿轉寄含有病毒威脅警告信息的電郵，這些電郵通常都是惡作劇電郵，轉寄這些電郵只會助長惡作劇蔓延，妨礙全球各地的電郵伺服器正常運作。
- 最新版本的抗電腦病毒軟件可同時檢查寄入及寄出信息有否病毒。為保障每位互聯網用戶的安全，請確保軟件經常設定為啓動狀態。

窺視 (SNOOPING) 及仿冒 (SPOOFING)

窺視及仿冒

(窺視) 如果你未能妥善保護你的電郵密碼，別人就可以閱讀你的信息。這種情況一旦在公司發生即足以造成破壞，因為公司的電郵往往被視為商業秘密。即使在家裏，最好也不要向別人透露密碼。

(仿冒) 假冒他人名字寄發電郵的行為叫「仿冒」。這種情況防不勝防，唯有加強警惕，一經發現應立即通知你的互聯網服務供應商或向公司的資訊科技部門報告。如果你沒有寄出電郵卻又收到寄件被退回的通知，就表示你的電郵地址已經被「仿冒」了。

我們今天所使用的互聯網電郵系統，在設計時並未預料到會在一個開放的環境中供全球各地使用。最初，這個系統只是為方便學者相互溝通，在一個限制性的圈子中使用，因此使用人數非常有限。了解到這一點後，你便會明白為何使用電郵系統會如此不安全及如此容易遭到濫用了。

建議行動

- 必須保護密碼。選擇密碼時，應最少有八個字符，並含有字母及數字。無論所選的密碼多好，亦必須經常 (不超過45天) 更換密碼。
- 不要與任何人共用密碼。換句話說，**切勿**將你的密碼**告訴任何人**。
- 不要寫下密碼，以防他人看到並使用該密碼。
- 確保所有僱員知悉，在未經同事許可下，一律禁止閱讀有關同事的電郵。
- 保持警覺，提防他人「仿冒」你的電郵地址；如發現電郵遭「仿冒」，應向有關部門報告。
- 僱員不得仿冒公司內外其他人士的電郵。
- 使用公司的電郵系統時，僱員不得偽造或隱藏身份。

如需協助或獲取更多資料，請瀏覽：

www.cert.org/tech_tips/email_spoofing.html

社會工程 (SOCIAL ENGINEERING)

社會工程

「社會工程」是指利用人性弱點，哄騙他人提供個人資料（如密碼）的伎倆，而這種伎倆足以危及系統的安全。

非法電郵有時會看似來自真確的寄發來源，藉此騙取個人資料或敏感資料。此類侵害通常稱為「社會工程攻擊 (social engineering attack)」，具體地說，就是「仿冒詐騙 (Phishing)」。這類攻擊一般會指示那些對郵件深信不疑的用戶進入虛假網站，並慫恿他們輸入敏感資料。這種詐騙伎倆之所以叫人難以辨別真偽，在於那些虛假網站與真實的公司網站非常相似，而且所寄發的電郵亦含有收件者熟悉的圖形及設計。「仿冒詐騙者 (phisher)」因此得以獲取及非法使用用戶所輸入的資料。

建議行動

美國政府聯邦貿易專員公署(Federal Trade Commission (FTC))的網站有以下建議：

- 如在毫無徵兆之下收到電郵，警告你若不重新確認賬單資料便會取消你的賬戶時，切勿回覆或點擊電郵上的連結；相反，你可利用經證實為真確的電話號碼或網站地址，聯繫電郵上所提及的公司了解情況。
- 避免用電郵發送個人資料及財務資料。在透過網站提交財務資料之前，應先找出瀏覽器狀態欄上的「鎖定」圖示，它會顯示在傳輸過程中，你的資料將會受到保護。
- 收到信用卡及銀行賬戶結單後應立即核對資料，確定有無任何未經授權的收費。假如遲了幾天仍未收到賬戶結單，應致電信用卡公司或銀行，確認你的賬單地址及賬戶結餘。
- 向聯邦貿易專員公署**(www.ftc.gov)**或電腦緊急應變小組(CERT) **(www.cert.org)**報告任何「仿冒詐騙」活動。

如需協助或獲取更多資料，請瀏覽：

www.kb.cert.org/vuls/id/652278

即時通訊蠕蟲 (IM WORMS)

即時通訊蠕蟲

即時通訊雖然實用，卻並非私人系統。在參與即時通訊期間，必須緊記所有信息均會在互聯網上公開。他人甚至可以利用即時通訊會話，騷擾參與「交談」的用戶。要防止這類侵擾，最佳方法是在你的即時通訊軟件上選擇適當的「攔截」設定。

雖然即時通訊對於商業社會來說相當實用，但卻會使你更易遭受特洛伊木馬程式、蠕蟲、病毒及社會工程攻擊的威脅。如果你的公司無意使用即時通訊系統進行業務通訊，最好在政策文件中明確規定不允許使用即時通訊系統。若你的公司打算使用即時通訊，便應採納以下建議。

建議行動

- 切勿在即時通訊會話中提供個人資料。
- 切勿在即時通訊會話中下載檔案。
- 若擔心即時通訊蠕蟲會對系統保安構成威脅，最好不要允許僱員使用即時通訊。
- 必須安裝防火牆軟件，並選擇有關即時通訊威脅的特定設定。
- 強烈建議公司應使用企業即時通訊軟件產品，務求有更嚴格的控制及更安全的環境。

如需協助或獲取更多資料，請瀏覽：

www.cert.org

數碼簽署 (DIGITAL SIGNATURES) 及加密 (ENCRYPTION)

數碼簽署及加密

大原則是切勿透過電郵發送敏感資料(如信用卡詳情或僱員背景資料)。在無可避免的情況下,便應利用數碼簽署及加密技術。互聯網電郵系統是公開給全球各地使用的系統,透過公開的電郵發送敏感資料,風險猶似以明信片寄發。

大型的電郵套裝軟件均具有數碼簽署信息的功能,甚至可以按意願加密。不過,某些國家的政府認為加密屬非法技術,因此在加密信息之前,應先行查詢有關發送及接收此類信息的法例。

建議行動

- 制訂有關數碼簽署及加密的公司政策,訂明可使用數碼簽署及加密的情況。
- 對於可能需要使用數碼簽署的僱員,應確保他們完全認識這種科技,了解公司打算如何使用數碼簽署,以及如何獲得經公司核准的數碼簽署。
- 採用最合適的公開密碼匙基礎建設(Public Key Infrastructure),藉以管理公司的數碼簽署。

如需協助或獲取更多資料,請瀏覽:

www.apectelwg.org/apecdata/telwg/eaTG/EA_text.pdf

searchsecurity.techtarget.com/

濫發電郵(SPAM)

濫發電郵

近年，濫發郵件或不請自來的商業電郵不斷增加。據一些用戶報告顯示，在他們收到的電郵中，超過七成是「濫發郵件」。對於現今的企業來說，在考慮有關寄入及寄出電郵的「濫發」問題時，應注意以下幾點：

1. 寄入電郵

讓僱員各自處理收到的「濫發郵件」會造成生產力的巨大損失。還有一個問題就是，「濫發郵件」通常對收件者具攻擊性，使僱員難以有效處理這些郵件。

要提高生產力、避免陷入困境，最佳方法莫過於在整個公司層面處理「濫發郵件」，不讓這些郵件發送至僱員的郵箱。事實上，有些僱員已向僱主採取法律行動，指控僱主未有採取適當步驟控制「濫發郵件」。若要減少公司出現僱傭糾紛的機會，便須認真處理這些問題，並考慮安裝軟件，為公司的電郵系統提供必要的保護。

2. 寄出電郵

在與客戶溝通時，公司必須注意現時的「濫發郵件」數量，並應盡量減少發送電郵。即使是「選擇接受」的電郵通訊，亦可能會引起收件者對發送過量電郵的公司產生反感；畢竟，情況是否可以接受或許只是一線之隔，若要留住忠實客戶，公司必須學懂取得平衡。

建議行動

- 制訂處理「濫發電郵」的政策，並確保所有僱員遵守有關政策。
- 從公司電郵系統的層面處理「濫發電郵」問題，慎防具攻擊性的電郵發送至僱員的郵箱。
- 制訂有關寄出電郵的政策及守則，確保公司不會被視作向客戶「濫發電郵」的公司。

如需協助或獲取更多資料，請瀏覽：

http://spam.abuse.net

www.cauce.org

正確措施 (Doing it Right)

檔案
附件指引

- 幾乎所有的電子郵箱均受到互聯網服務供應商或內部電郵系統的容量限制。因此，若嘗試發送大型檔案，電郵系統或會因檔案容量過大而拒絕發送。
- 此外亦應注意，很多用戶無法使用高速連線，因此在透過撥號連接接收電郵的過程中，大型檔案或會導致嚴重延誤或其他問題。
- 避免發送大型檔案，超過150千字節的檔案通常屬於過大。
- 發送大型檔案時，應用壓縮軟件縮小檔案容量，甚至可能要將檔案分成若干部分，以多個電郵發送。
- 在發送大型檔案前，必須先通知收件者，因為收件者可能不在辦公室，如你不必要地以大型檔案堵塞他們的郵箱，他們要直至返回辦公室才可清理。
- 發送大型檔案的最佳方法是將檔案上載至互聯網，然後告訴收件者可下載檔案的網址。此舉亦可讓收件者在方便時自行下載檔案。請向你的互聯網服務供應商或資訊科技部查詢怎樣將檔案上載至互聯網。

- 若非已安裝硬件或軟件加密設備，你應假設互聯網上交流的所有信息都不安全。不適宜寫在明信片上的東西，亦不適宜寫在電郵裏！
- 如要轉寄或轉貼你收到的某個信息，不要更改信息內的任何字眼。如果那是別人寄給你的私人信息，在轉寄給另一人或一群人前，應先得到寄件者的同意。
- 切勿透過電子郵件寄發連鎖信，這種行為在互聯網上是嚴禁的，否則你在網絡上享有的權利可能會被取消。如收到任何連鎖信，請立即通知你的互聯網服務供應商。
- 寄發信息或回覆電郵時要特別小心，因為部分電郵的收件者一欄雖然顯示為某個別人士，但事實上卻會分發給一群收件者。
- 寫電郵時，應善用大小楷字母。在日常書信中，全大楷的信息代表**責罵對方的意思。**

- 在主旨一欄，註明信息的內容。這樣，收件者便可輕鬆和有效地整理寄入電郵，優先處理要立刻回覆的重要信息，以及將郵件存檔，方便日後查閱。
- 收到信息時，你未必有時間立刻仔細回覆，所以最好先寄出一封簡短的電郵，讓對方知道你已收到他的信息，稍後會再詳細答覆。
- 不請自來的電郵廣告往往不受歡迎，在某些情況下甚至是犯法的。

寄送電郵指引
(Guidelines for sending E-mails)

- 有些人喜歡用「笑臉」符號表達語氣或態度。開心的符號是:-)，而憂愁的符號是:-(，這些都是由鍵盤上的符號組成的。如果真的要用這些符號來表達，最好盡量避免濫用，並須緊記其他國家文化的人未必明白這些符號的意思。
- 有些人每日須處理大量電郵，往往希望事先知道哪些電郵篇幅較長，需要較多時間去處理。一般來說，電郵內容如超過100行，便屬於篇幅較長的郵件，應當在主旨一欄註明，通知收件者。
- 信息應盡量簡潔，但又要避免予人草率的感覺。簡短生硬的信息會被視為無禮或憤怒的表現。

- 現代的信息系統可以設定「讀取回條(read receipts)」功能，又或在信息附上「急待處理(urgent flags)」標幟。可是，經常使用這些功能卻會減低成效。如果凡事也使用這些功能，更可能會對收件人造成滋擾。
- 不要建立過於冗長的收件者名單，要將信息同時寄發給許多人時，可用「特別副本送(blind carbon copy (BCC))」功能。
- 切勿濫用「急待處理」標幟。

- 在加入任何通訊錄或新聞組前，應先花一至兩個月時間了解這個組別，否則不要發表任何信息。
- 雖然用戶的不正當行為與系統管理員無關，但系統管理員有責任採取行動，阻止任何違規行為。
- 一旦按下「傳送」鍵，便會無法取消已發出的信息。因此，發表信息前必須仔細考慮，以免後悔莫及。
- 力求信息簡潔、貼題。
- 有些通訊錄歡迎用戶發表廣告，但也有些表明嚴禁發表廣告。
- 回覆或發表信息時，應確保你引述的原文足以交代事情的始末，否則對方未必明白你所述何事。
- 如要加入及離開通訊錄，請將有關信息傳送至適當的電郵地址。
- 如果你有一段長時間無法檢查電郵，應考慮退出通訊錄或設定「不收取郵件」選項（如有）。
- 若向不止一個通訊錄發表信息，尤其是各通訊錄關係密切的話，應為重覆發放道歉。
- 切勿透露你的用戶名稱或密碼。即使是系統管理員需要你的賬戶資料，藉以進行維修或修正問題，他們也可隨時登入你的賬戶，毋須事先向你索取任何資料。

參與通訊錄指引
(Guidelines for participating in Mailing Lists)

- 發表私人回覆時要小心。若只按下「回覆寄件者」的話，很可能整個通訊錄的人都收到你的回覆，有違你只想回覆某人的原意。
- 萬一不小心將私人信息傳送給組別的所有人，應當立即向當事人及該組別道歉。
- 如對某人發表的信息有強烈感覺，應透過私人電郵表達。
- 不要捲入任何「筆戰 (flame wars)」中。切勿發表煽風點火的信息，也不要回覆這類信息。應留待通訊錄管理員解決這些問題。
- 避免使用不標準的字型，因為這些字型在不同的系統上會有不同的顯示方式，令用戶難以閱讀。
- 如只以數目字代表日期，日子和月份會容易混淆。為免引起誤會，應以下列格式表示日期：11 Feb 2004。
- 縮略語可以減省用字，但若然信息裏有太多縮略語，便會令其難以理解，對讀者造成不便。以下是部分常用的縮略語：

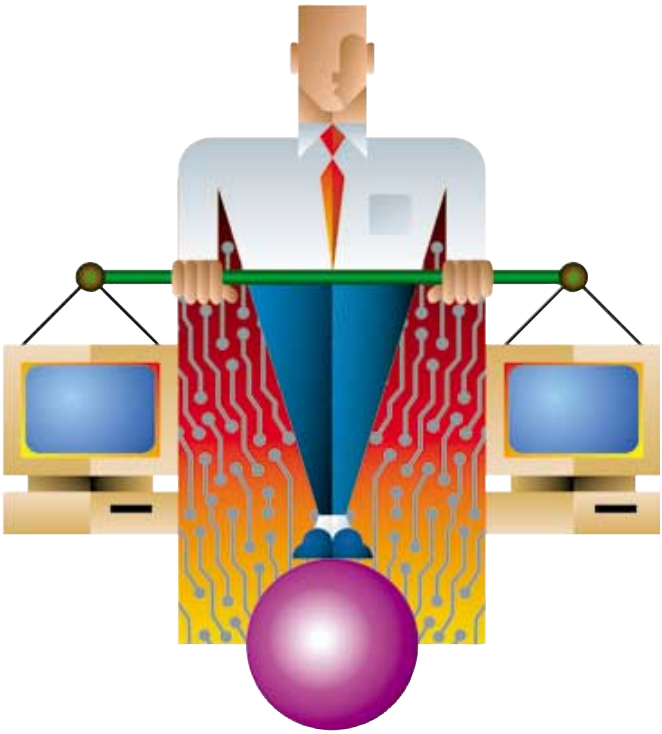
IMHO = 我認為

FYI = 僅供參考

BTW = 順帶一提

電郵安全

政策考慮因素



24

政策問題 (Policy Agenda)

政策考慮因素

本節會協助你解決有關互聯網通訊政策等重要問題。每家公司都應正式制訂一份文件，並經全體員工簽署及同意，而此舉正是保障公司及員工合法權利的唯一方法。雖然本節所談及的部分問題已於前文提及，但為確保提供全面而完整的資料，本節會探討與政策相關的所有考慮因素。

電郵是公司的正式記錄

信息內的免責聲明

信息一旦離開公司範圍，便無法得知收件者會如何使用或詮釋信息所載的資料，也無法知悉信息最終會否給收件者以外的人士閱讀。

政策考慮因素

- 確保電郵政策訂明，規定公司發出的所有信息必須於信末加入免責聲明。
- 清楚列明發送的資訊只供收件者使用，並可能載有機密及/或有法律特權的資料。
- 列明在未經信息作者同意的情況下，不得轉寄、披露或散播有關資訊。
- 在信息內列明電郵地址及電話號碼，讓誤收信息的人可根據資料通知或寄回信息，這一直是傳真封面的標準作業實務。

知識產權及版權

可以透過互聯網獲得的資料，數量難以想像，加上電腦和文字處理，我們更可迅速發佈資料，無遠弗屆。公司員工必須明白到，在互聯網發佈或透過電郵傳送資料，也可能引致知識產權問題。

公司須承擔僱員侵犯版權所引起的責任，因此必須制訂政策處理有關問題，並指導僱員在使用互聯網上的資訊時，應注意甚麼能做，甚麼不能做。

政策考慮因素

- 所有僱員必須明白知識產權和版權的概念，並學習有關知識。目前有多宗官司裁定有關公司及個別人士須就侵犯知識產權及版權負上法律責任，後果非常嚴重，絕對不容輕視。
- 應指導員工除非獲得明確批准及原作者認同，否則切勿在電郵內引述他人編撰的資料。

私隱考慮因素

必須再次鄭重強調，透過互聯網傳送電郵並不可靠，所以必須將任何寄出的資料視為向全世界公開。若在未經允許的情況下，向第三者寄發某人的個人資料，則或須就侵犯他人私隱而負上責任，並且遭受檢控。

向一大群人發送信息時，亦必須非常小心。當你在「寄 (To)」或「副本送 (cc)」上輸入電郵地址清單時，你可能已經不知不覺地為他人提供了可「濫發電郵」的清單。

政策考慮因素

- 寄發個人資料時，不論資料是在電郵內文或是在電郵的附件內，都必須先將資料加密。（請跟你的電郵系統支援人員討論怎樣可以將資料加密）。
- 向眾多收件者寄發電郵時，必須在電郵地址清單上選用「特別副本送」工具，這樣便不會向所有人公開電郵地址。

信息文體及內容

凡是公司有份參與的任何通訊，不論以書面或電子郵件形式，都應視為公司對通訊內容的合法承諾。所以，我們應該嚴謹對待所有通訊，包括電郵通訊，並應制訂相關守則保障公司利益。

顯然，並非所有通訊都以合約協議形式進行，所以必須訂立通訊種類，而且每種類別也應受到適當規則規限。

政策考慮因素

- 針對各種不同種類的通訊制訂行事程序。在為電郵方式所進行的合約磋商訂立行為守則時，必須格外審慎。
- 內容與文體都是重要的考慮因素，應盡可能採用紙張文本的文體。在罕有情況下，如果這種方法不可行，應確保你已慎重考慮電子文件的法律後果，並且小心審閱文件內容。也有可能需要諮詢法律意見。
- 同樣重要的是，必須制訂相關的管理批核程序，審批透過電子儀器發出並且在法律程序中對公司具有法律約束力的文件。

保護資訊財產

存檔政策

現時，電郵及即時通訊信息均被視為公司記錄，而眾所周知的是，公司記錄必須根據特定法例存置。小心別把備份和存檔程序混淆。備份是讓公司可在經歷電腦災難後復原運作，而根據政府規定保留存檔的檔案則會用來保存商業文件，以供日後參考。

公司應同時審閱內部或外部發出的信息種類，並且決定每種信息最合適的存檔規定。或需處理的信息種類包括：

- 行政通訊
- 財務通訊
- 一般通訊
- 即時通訊
- 加密通訊

各種通訊的保存時間毋須相等，亦毋須將各種通訊存檔。

確保存檔政策涵蓋所有電子通訊方式。緊記通訊是雙向的過程，接收訊息的公司亦可能會將這些文件存檔。

政策考慮因素

- 制定政策，列明僱員提交信息以作存檔用途的方法及時間。
- 設立中央處理點（通常為內部電郵地址），在需要保存信息時，可透過中央處理點發送或複製信息，方便存檔。
- 制訂守則及政策，規定僱員須於電腦內保存甚麼訊息，以及保存方法及時間。

在辦公室外使用電郵

現在，閱讀電郵是一件簡單輕易的事，不論僱員身處何地，均可保持聯繫。不過，對於僱員在辦公室以外地方讀取他們的商業電郵賬戶，公司亦須考慮一些重要的因素。

最值得關注的兩個範疇是密碼及登出程序。若不正確地保管密碼，便會潛伏危機，特別是在旅遊途中，危機就更大。假如僱員未能完成登出程序的所有步驟，公司的電郵系統便會面臨被黑客入侵的危機，起碼下一位使用該公用接入電腦的人就可以閱讀僱員的公司郵件。

在公眾地方如火車、咖啡店或無線上網「熱點」閱讀或撰寫電郵時，亦須同樣謹慎。別人要在背後偷看你的資料並非甚麼難事。

筆記簿型電腦、數碼電話及記錄媒體（如軟磁碟、光碟等）被盜或遺失時特別危險，因為公司以外的人便可藉此閱讀公司電郵及文件。

政策考慮因素

- 在解決這個問題時，必須緊記這些全是在辦公室以外地方登入公司電腦系統所引起的風險。雖然帶有風險，但顯然可加以控制，而且大部分公司都相信此舉可提高生產力，優點比潛在風險更多。
- 在制訂辦公室以外地方使用電郵的守則時，必須先假設流動/手提電話及手提設備很容易會遭遺失或被盜。
- 即使允許在辦公室以外地方使用公司的電郵，也絕不能將敏感資料寄出公司範圍以外。
- 必須教導僱員有關在辦公室以外地方使用電郵的風險。
- 必須嚴禁將公司的電郵自動轉寄至公司以外的郵箱，因為向不明人士寄發資料會對公司的資訊保安構成威脅。

保持公司資料機密

電郵在傳送途中須經過多個網絡及伺服器，期間有可能會被竊取或竄改。如今資訊系統使用簡便，懷有異心或粗心大意的僱員可能會複製公司資料，傳送給公司的競爭對手或有興趣人士。

心懷不軌或粗心大意的僱員固然可能會將敏感資料寄給公司以外的郵件通訊錄或電子佈告板，而僱員要將電郵從公司電郵賬戶轉寄至個人電郵賬戶，亦非難事。

若不小心處理電郵，在有意無意間，可能會在信息加上未經授權的地址，以致公司內部信息外洩。

政策考慮因素

- 全體僱員必須簽署保密協議，此舉對大公司或小公司都極為重要。
- 訂立「啓動接達控制系統」，限定只有指定的高級僱員才可讀取重要資料。
- 寄出辦公室以外的電郵應自動複製一份副本給指定的負責經理。

- 必須制訂相應政策，規限轉寄內部電郵至公司以外郵址的事宜。
- 教導僱員在寄發電郵時必須檢查收件人地址，特別在選用「全部回覆」功能時應加倍注意。

僱員的權利及責任

信息回覆時間

如果你的公司網站載有電郵地址，不論是一般查詢的電郵地址，還是指定聯絡人的電郵地址，公司都有責任要及早回覆。不回覆電郵就像不接聽電話一樣，而你卻要靠積極回應各種溝通方式來建立聲譽和盈利。

許多情況都可以阻礙電郵的傳送，例如郵箱已滿、郵件伺服器操作失靈，又或互聯網通訊閘出現問題（即兩個電郵系統之間無法傳遞電郵），公司必須確保電郵的接收不會受到阻礙。

政策考慮因素

- 有關電郵的政策，必須訂明閱讀及回應電郵的規則。經理級人員必須確保僱員貫徹遵守這些規則。
- 確保在接收重要客戶的電郵時暢通無阻。

臨時僱員

不必讓只工作數天的臨時僱員接達公司的電郵系統。假若預計臨時僱員需要使用公司的電郵，便須讓他們知悉及簽署政策文件。任何僱員，包括臨時僱員，都有機會令公司負上法律責任，若要避免公司惹上麻煩，唯一方法是要全體僱員細閱、了解及簽署政策文件。

政策考慮因素

- 為協助所有經理級人員，必須清楚制訂分發電郵地址給臨時僱員的政策。
- 很多僱主會問，究竟應該分發部門級的郵址予臨時僱員，還是個人的郵址呢？對於這個問題，不同的人會有不同看法，但在嘗試解決這個問題時，兩個選擇都應該加以考慮。
- 若預期臨時僱員需要使用公司的電郵賬戶，便應確保有關的臨時僱員完全明白政策文件的內容，並簽署有關文件作實。

騷擾

差不多每個有電郵賬戶的人，都收過親友以電郵寄來的笑話。事實上，只要利用互聯網，便可輕而易舉地與友人分享這些詼諧有趣的笑話、卡通、故事和照片。但問題是，每個人對幽默、有趣的看法各有不同，有些人覺得有趣的色情笑話，卻可能會引起他人反感或構成滋擾。透過私人電郵賬戶寄發私人電郵是一回事，但僱員若利用公司的電郵賬戶寄發電郵，則可能會引發很多問題，甚至令公司牽涉入法律訴訟。

公司必須清楚知道，公司電郵系統使用不當，有可能會因為在工作場所構成騷擾而被檢控。應付這個問題的最佳處理方法，就是禁止僱員下載及散佈任何與公司業務無直接關係的資料。

切勿透過公司電郵賬戶收發笑話、故事或相片。僱員只可透過私人電郵賬戶傳遞這類資料。

僱主必須明白，如果僱員提出證據，顯示有人在工作場所散佈不當的電郵，而僱主又沒有採取任何行動，則僱主可能會面臨法律訴訟。

政策考慮因素

- 確保公司的電郵政策，包含規管下載及/或散佈可能令人反感的資料的守則。
- 立即跟進所有有關違反政策的投訴。
- 各級僱員都必須明白違反政策規定的後果。

監測電郵

制訂周全的電郵政策文件只是第一步，下一步就是要落實執行政策。但這並不表示要站在僱員背後，查看他們電腦螢幕上的資料。現今，有些軟件可報告及概述全體僱員的所有活動。

監測的需要

若沒有電子監測的幫助，根本沒可能知道僱員有否寄發敏感資料給公司以外的收件人。

僱員也可能在辦公時間內使用互聯網或聊天室作私人用途，這樣不但會減低生產力，更糟的是，此舉可能令公司面臨法律訴訟風險。

此外，令人反感的資料亦可以透過公司內部網絡傳送。

監測風險

除非已知會僱員設有監測系統，否則公司或須負上侵犯他人私隱的責任，同時亦可能觸犯法例。

假若僱員的行動受到監測，並且發現有人傳送非法或令人反感的資料，但管理層卻沒有採取任何行動加以制止，那麼，公司可能需要就此負上法律責任。

政策考慮因素

- 決定是否使用監測軟件。
- 如決定使用監測軟件，公司必須發表政策聲明，通知僱員將會受到監測，並說明實施監測的原因，以及清楚解釋一旦違反任何特定守則，僱員所須承擔的後果。
- 監測是唯一可以確保僱員百分百遵守公司政策的方法。
- 公司每年都應向僱員發出通告，說明監測的形式和目的。
- 必須讓僱員知悉當私隱遭受侵犯時，僱員有權對僱主採取行動。

參與通訊錄

現時，互聯網可透過電郵提供大量有趣的通訊，而且題材包羅萬有，所有想像得到的商業和個人生活資訊，均應有盡有。網上亦有以電郵形式的論題通訊錄，所討論的課題相當廣泛，吸引了很多人和公司的興趣。

相應的印刷本是貿易報章、雜誌和通訊，對僱員來說大多是寶貴的資源。不論電子版本或印刷本，這些資料來源都是寶貴的教材。但是，太多資源也未必是件好事，公司亦多半不會喜歡僱員一整天坐著閱讀。所以，公司必須對僱員參與這些電郵通訊錄加以規管。

政策考慮因素

- 確保電郵政策提及參與通訊和通訊錄的事宜，並清楚訂明你認為有必要訂立的規定或限制。同樣，必須讓僱員明白，公司期望僱員怎樣行事。
- 教導經理級人員在僱員時間管理方面，應該擔當一個怎樣的角色。

私用公司資源

公司必須決定僱員可否將公司的電郵地址作私人用途，以及作私人用途的使用程度。換句話說，公司需要決定是否對僱員實施相關規定或限制，以及會否真的監測僱員活動。僱員必須明白，電腦操作時間、電腦儲存容量及互聯網帶寬都是有限的資源，而且由他們任職的公司負責支付費用。

若決定使用監測軟件管理僱員如何運用資源，有一點非常重要，就是此事必須讓全體僱員知道（現在，某些司法管轄區已立法規定公司必須這樣做）。

現時，採納電郵記錄作為證據的法律案件，在世界各地均非常普遍。因此，公司必須了解本身的資訊流通情況，並教導僱員有關不恰當使用電郵的潛在風險。

政策考慮因素

- 僱員必須清楚明白，在公司系統內傳送的所有電郵均屬公司所有，不恰當使用可能會導致法律訴訟。
- 清楚訂明在公司系統使用私人電郵的守則和責任。如需採用監測軟件，應確保所有僱員均知悉這個安排，並讓所有僱員簽署一份列明有關安排的政策文件，以表示同意作此安排。

培訓

假如僱員並非完全明白政策文件的內容，這份文件對公司來說亦毫無用處。事實上，如果僱員與高級管理層之間全無共識，訂立政策文件也只會增添更多麻煩。所以在推行政策之餘，亦應確保公司能夠提供適當的培訓課程加以配合，相比之下，為僱員提供培訓的麻煩程度，確實遠比本小冊子所述的種種潛在問題為小，因此在這方面多花點時間和精力也是值得的。

公司上下每位成員，由高級經理以至各級員工都需要參加培訓，即使臨時僱員亦應該參與。必須讓高級經理明白，他們在整個培訓過程的管理上有何責任，而僱員亦須明白有關的規定及限制。

政策考慮因素

- 為全體僱員和經理級人員設立培訓課程，確保所有人都知悉並且明白，公司所制訂的電郵政策所帶來的後果。
- 確保新入職僱員在使用電郵前已就有關政策接受培訓。

僱員調動及退休

當僱員退休、離職或調派到其他部門，不應刪除他們的電郵地址，因為顧客及供應商很可能只是靠這個電郵地址來與你的公司保持聯繫。因此，必須監測這些舊電郵地址一段時間，藉以保持聯繫。此外，該名僱員以往也可能一直以這個電郵地址，作為取得公司一些必要資訊或服務的聯絡點。總之，關鍵就在於監測這位前僱員所用的郵箱，並且採取所須步驟，以便接替的僱員能夠順利接任。

政策考慮因素

- 應就前僱員電郵地址的處理方法訂立守則，並貫徹遵從有關守則。
- 如把舊電郵地址分派給另一位僱員使用，便應通知有關的前僱員。
- 如郵箱內的所有活動均已處理妥當，並已順利移交工作，那麼便可停用該電郵地址。
- 僱員離職後，應立即更改該僱員的電郵賬戶密碼。

其他信息策略

即時通訊

即時通訊服務可讓公司與客戶或供應商取得即時聯繫，採用這種即時聯繫的服務支援策略，更可使公司的表現脫穎而出。但是，如果僱員在工作場所使用即時通訊處理私人事務，這將會嚴重降低公司的生產力。

使用即時通訊服務的僱員亦要明白，即時通訊服務可能會使公司承受額外的保安風險，除非你所用的抗電腦病毒軟件 (anti-virus software) 能夠特別監測即時通訊的交往，否則很難保障公司免受這種威脅。

政策考慮因素

- 查察一下倘若使用即時通訊這種技術能否提升公司的溝通能力。
- 如公司選用即時通訊，必須列明僱員在使用即時通訊與業務聯繫人溝通時，有甚麼是可以接受，有甚麼卻不可以。雖然看似是眾所周知的事，但最好還是確切地通知僱員，公司絕不能容忍僱員使用粗言穢語或作有損專業形象的行為。請緊記，互聯網是你「通向世界的窗口」，因此必須採取一切必要措施來維持及提高公司的名聲。

- 應設立特定措施，專門處理僱員在工作場所或辦公時間以外使用即時通訊處理私人事務的問題。
- 為消除使用即時通訊在保安方面所引起的疑慮，應確定電腦桌面和伺服器均安裝了抗電腦病毒軟件，並已妥為選取所有有關設定。

簡短訊息傳遞（短訊傳遞）

短訊傳遞提供了一個既簡便又相宜的通訊方法，不論僱員、客戶及供應商身在何地，均可讓你取得即時聯繫。現今的系統技術更可讓公司電腦將短訊傳遞的信息，即時廣播至一個或多個流動或手提電話。

若決定使用短訊傳遞聯絡顧客，便應在一般電郵用不著時才選用這種通訊方式。舉例說，短訊傳遞可以用來傳輸送貨安排的更新資料，但用來傳送廣告就不大合適了。短訊傳遞若使用不當，常會引起顧客不滿；相反，只要使用得宜，短訊傳遞卻可成為功效卓越而又受客戶歡迎的服務工具。

政策考慮因素

- 先決定應否選用短訊傳遞作為通訊策略的一部分。請緊記，對於大部分顧客來說，數碼電話快將成為一種無所不在的通訊工具，公司正好藉此機會提升客戶服務水平，務求脫穎而出，但切勿過量使用短訊傳遞，又或在不適當的情況下使用。
- 在使用短訊傳遞時，應確保顧客和供應商有權選擇接受或拒絕你所提供的短訊傳遞服務。換句話來說，你必須問明準收件者是否願意「選擇接受」服務，並須另設「選擇不接受」的選項，以便收件者將來改變初衷時也可另作安排。
- 可考慮使用短訊傳遞，方便與僱員溝通，特別是對於長時間在辦公室以外工作的營業銷售隊伍來說，這點尤其重要。
- 不要以為僱員一定懂得使用短訊傳遞。為他們提供培訓，以便能有效及專業地使用短訊傳遞。
- 必須決定是否容許僱員在辦公時間內使用私人流動/手提電話和短訊傳遞。很多公司都訂有關於使用公司電話的政策，卻未必設有守則規管僱員如何使用每天帶著上班的私人電話。從僱主的角度來看，若僱員花大量時間在私人通話或私人的短訊傳遞信息上（即使是使用自己的電話），也會令生產力下降。

其他資源

只要在搜索引擎 (search engine) 輸入「電郵政策(email policy)」一詞，便可找到提供有關服務的公司協助你制訂電郵政策文件。

以下所列的網站來自世界各地，可為你提供更多有關本小冊子討論內容的資料。如欲查詢有關私隱法例、濫發電郵的規例及其他關於電郵使用的問題，請瀏覽所屬地區政府轄下的監管機構網站，或瀏覽www.aoema.org網站，查閱亞太經合組織成員國的網址。

政府推薦網站

www.oecd.org/sti/cultureofsecurity

病毒資料

www.f-secure.com
www.mcafee.com
www.symantec.com

濫發電郵

www.cauce.org

私隱

http://epic.org
www.privacy.net

消費者權益保障

www.econsumer.gov

網絡禮儀指引

公認為首份「網絡禮儀指引」

www.ietf.org/rfc/rfc1855.txt.

Asia-Pacific Economic Cooperation
亞太經合組織刊物 #204-TC-01.1
www.apec.org

亞洲大洋洲電子市場協會
www.aoema.org

E-Japan 論壇
(E-Japan Forum)
www.ejf.gr.jp

由多媒體交流協會
(FMMC)（日本）資助
www.fmmc.or.jp

Nisso 22 Building 5th Floor, 1-11-10 Azabudai, Minato-ku, Tokyo 106-0041 JAPAN

如有任何回應、提議或查詢，請電郵至info@aeoma.org。

二零零四年三月

電郵安全

信息策略

市場推廣策略

威脅

指引

政策考慮因素

網上安全 與電郵安全是一套實用的指引，可助互聯網初用者及富經驗的互聯網用戶自行設定「安全網絡」，防禦網上詐騙及威脅。

•消費者的保護•Cookies程式•數碼簽署•防火牆•身份盜竊•即時通訊、聊天室等
•知識產權•互聯網誘騙轉接•互聯網詐騙•法律問題•監測互聯網的使用
•網上誹謗•聯機爭議處理•聯機滋擾•密碼•個人資料私隱
•公用接入•安全網頁•濫發電郵•軟件更新•仿冒•間諜軟件•特洛伊木馬程式•病毒
•電郵信息指引•通訊錄指引•方便消費者使用的網站指引
•安全網上購物指引•網上拍賣指引

ISBN: 981-05-0925-1

本小冊子為AOEMA所出版的Safety Mail英文版的中文譯本；
Safety Mail的英文原版刊載於網址：http://www.aoema.org/safetymail/index.htm。
香港特別行政區政府資訊科技總監辦公室獲AOEMA授權翻譯及出版本小冊子。
如對本中文譯本的內容有任何查詢，請電郵至 webmaster@infosec.gov.hk。
This booklet is a Chinese translation of Safety Mail published by AOEMA in English.
The original English version of Safety Mail can be found at http://www.aoema.org/safetymail/index.htm.
The Office of the Government Chief Information Officer of the Hong Kong Special Administrative Region Government has obtained the approval of AOEMA to translate and publish this booklet.
For enquiries about the contents of the translation, please email us at webmaster@infosec.gov.hk.

政府物流服務署印
（所用紙張取材自可再生林木）
Printed by the Government Logistics Department
(Printed on paper made from woodpulp derived from renewable forests)