六個有效的資安政策範本

讓專家告訴你瞭解密碼、可接受用法、電子郵件、存取控制、自攜設備(BYOD)與事件回應的安全性政策。

文／Neal Weinberg 譯／Nica

任何人都能在網路上找到並下載整套通用、制式的資安政策。雖然採用這些範本可以讓稽核人員或合規性檢查官員直接勾選，陳述該企業備有執行中的資安政策，但這種範本完全無法幫助公司企業減少遭受攻擊的弱點。

為實施確實有效的資安政策，企業組織應採取全面性處理方式，內容含括建立高階管理層支持、確保終端使用者參與且瞭解遵守資安政策的重要性、提供持續不斷的教育，並嚴格執行政策。

首要問題是，若未透過教育、測試、定期重新認證這些手段不斷強化資安政策，員工們容易遺忘這些規則。更嚴重的是員工故意遊走嚴苛資安指導方針的邊緣，因為這些政策被認為沒必要地拖慢或阻礙他們進行工作。因此，終端使用者有可能為了方便而將密碼提供予承包商。

地下IT(Shadow IT)則是員工規避標準IT採購與安全性程序的另一種情況，員工們自由發揮以雲端為基礎的生產力、儲存裝置與協同合作應用，而IT甚至未能查覺這些。

在這種環境下，企業組織必須採取通盤考量並審慎處理，將資安政策書面記錄下來再實施：足以保護企業又不致太過艱鉅致使員工拒絕或忽略的政策。

如何制定資安政策

資安政策的制定是從確認明確的目的與目標開始，定義應該涵蓋哪些人並精確指出哪些資料應受保護等諸如此類的政策範疇。

為建立共識，將企業整體全都納入相當重要，讓每個受政策影響的人，都有權表達如何定義他們。

公司本身也必須瞭解其資安防禦的當下狀態。例如，透過弱點評估或滲透測試的練習確認漏洞所在。對法規責任的瞭解也相當重要。

企業組織必須建構現存文化誠實評估：現有規則是嚴格執行還是經常草率帶過。換句話說，若試圖對之前允許的做法強制實施新禁令，例如上班時間存取社交媒體站台，企業組織面臨員工強烈反對的可能性有多高。

公司也要確保資安政策以清楚、可理解的語言書面記錄成文件，而非以冗長費解的法律詞彙撰寫。公司執行資安教育課程的做法，必須反映員工們各種不同的學習方式。例如，與其要求員工實際出席由人資部門或資安專家舉行的會議，不如提供線上、自主學習的體驗。

若公司決定編寫一套資安政策，接下來便是排列優先順序，因為這是政策範本的確切計分，內容含括所有事物：從「清理桌面」政策【譯註：員工下班離開後，不在辦公桌上留下任何可供利用的資訊。】、到如何淘汰舊設備、到涵蓋各種災難的政策，包括大規模流行疾病。企業會想要找出關鍵痛點，以免員工因太多政策疲於奔命。

以大部份公司企業來說，排名前六大的政策包括密碼的產生與保

護、公司資源可接受用法、電子郵件與其他電子形式通訊、存取控制、自攜設備與事件應變機制。

切記，這些範本只是框架。所有公司行號都必須自行客製化範本，使其符合公司獨一無二的需求。

1 密碼/密碼短語保護政策範本

時至今日，論及密碼已出現部份爭議。多數公司要求使用者固定一段時間變更密碼，通常是九十天。但來自NIST的新指南建議，公司無須要求變更密碼，除非密碼遭破解。Microsoft最近宣告在Windows 10移除密碼強制過期這項規則。免除強制密碼變更的論點在於，要求員工頻繁變更密碼，無疑鼓勵重複利用他們在多個網站上使用的相同密碼或型式。再者，大部份遭竊的密碼是釣魚攻擊所導致，強制密碼變更無法預防這種狀況。不過，許多資安經理人習慣這麼做，不願放棄。無論如何，以下內容是納入密碼/密碼短語新思維的密碼資安政策範本。

1. 字元越長，密碼越強健，因此密碼應至少14個字元。密碼短語建議由多個單字組成。
2. 所有工作帳號都應該擁有不同、獨一無二的密碼。
3. 使用者不應在工作上使用與個人帳號相關的密碼。
4. 員工應使用企業組織提供的密碼管理程式。
5. 盡可能使用多因認證。
6. 只有深信密碼遭破解時，才應該變更密碼。
7. 密碼禁止與任何人分享，包括同事與上司。
8. 密碼不應該出現在電子郵件訊息內容裡。
9. 不要使用網站瀏覽器或其他應用程式的「記得密碼」功能。
10. 任何使用者只要懷疑密碼可能被破解，就必須回報事件並變更所有密碼。
11. 資安團隊會驗證合規性，當員工被發現有違反政策的行為時，必須懲戒處分。

六個有效的資安政策範本：

1. 密碼 / 密碼短語保護政策範本。
2. 可接受使用方式政策範本。
3. 電子郵件安全性政策範本。
4. 存取控制政策範本。
5. 事件應變 (IR) 政策範本。
6. 自攜設備 (BYOD) 安全性政策範本。

2 可接受使用方式政策範本

新進員工簽署的第一份資安政策相關合約，便是取用公司擁有的電子設備時，被要求簽署的可接受使用方式同意書。由於有些員工會希望在家或路途中能夠存取公司資源，企業審慎考量可接受使用方式政策，與這些政策如何在資安疑慮與員工從辦公室以外地點、於非正常工時工作的能力間取得平衡，非常重要。以下內容為範例範本：

1. 通常來說，電腦設備、軟體、儲存媒體與公司電子郵件帳號，皆屬於公司資產且應僅供業務使用。
2. 員工有責任保護公司裝置裡存放的專屬資訊。
3. 專屬資訊遭竊、遺失或未授權公開時，員工應儘速回報。
4. 各部門有責任建立公司資源的個人使用指南。
5. 連結至公司網路的所有行動裝置，必須遵守存取政策。
6. 社交媒體文章應含括免責聲明，亦即表達的主張全屬作者觀點。
7. 禁止以下行為：違反著作權、專利權或其他智慧財產權、使用盜版軟體、網路置入惡意程式、向其他人-包括家庭成員揭露密碼、傳送將被視為垃圾

郵件或騷擾的電子郵件。

8. 公司也可能想要建立應用程式白名單與黑名單，明定員工可以存取哪些應用程式與哪些禁止使用。

3 電子郵件安全性政策範本

估計90%的安全性外洩是成功的釣魚式攻擊所導致，因此擁有一套強健的電子郵件政策，再輔以持續不斷的教育強固，乃所有資安舉措的關鍵。估計90%的安全性外洩是成功的釣魚式攻擊所導致，因此擁有一套強健的電子郵件政策，再輔以持續不斷的教育強固，乃所有資安舉措的關鍵。許多公司為了讓員工保持警惕並協助他們瞭解釣魚式攻擊的樣貌，會利用傳送假釣魚郵件的程式增強電子郵件的保護。

1. 電子郵件僅供業務用途。這看來是理所當然的事，但必須明確規範。公司還必須決定，是否嚴格禁止將業務電子郵件帳號用於任何個人用途，或者是否政策有彈性機制，允許員工在某種特定狀況與限制下使用業務電子郵件。
2. 禁止員工使用業務用電子郵件，註冊與工作無關的帳號。
3. 電子郵件乃公司資產，雇主可合法監控與檢視。
4. 勿開啟未知來源寄出的電子郵件附件。
5. 不點選電子郵件內容出現的連結。
6. 透過電子郵件傳送的所有專利權與機敏資訊都要加密。
7. 電子郵件訊息不可用於騷擾、威脅、攻擊或製造混亂。
8. 電子郵件訊息內容不得含有關於種族、性別、性傾向、色情、宗教或政治信仰、國籍或殘疾的語言與影像。
9. 收到不適當或可疑的電子郵件，員工應向主管或經理人回報。
10. 電子郵件政策應定義哪些電子郵件應保留與保留多久。

4 存取控制政策範本

談到何種處理方式最好時，存取控制是另一個有趣的思辯領域-廣受歡迎且廣泛佈署以角色為基礎的存取控制或屬性為基礎的存取控制，甚至還能精細到哪個特定資源可以讓某個員工存取。無論是使用以角色為基礎還是以屬性為基礎的方式，下面介紹的通用範本都可以用來執行身份驗證與授權。

1. 安全的遠端存取，必須以加密(VPN)、強健的密碼短語與多因認證，嚴格控管。
2. 取得授權的使用者應保護其登入與密碼，面對家庭成員也不例外。
3. 遠端使用者應確保裝置未連結任何其他網路。
4. 透過遠端存取技術連結到公司網路的所有主機，都必須使用最近更新過的防毒軟體。
5. 遠端存取事件記錄必須保留一段時間至少九十天，並定期檢視。
6. 使用者自公眾場所連結時必須行事謹慎，像是機場、咖啡廳等，並且切勿從不安全的、公共網路連結到公司內部網路。
7. 第三方使用的存取帳號，只能在必要的時間區段啟用，且必須在此期間後立即停用。
8. 必須要求得到授權的第三方使用者，在被允許存取保密資訊前進行驗證。

5 事件應變(IR)政策範本

事件應變是公司希望永遠不要用到的政策，但備妥一套有效的事件應變政策，在安全性外洩事件發生時能立即執行絕對至關重要。有效回應事件，有助於公司止血、定義引發事件的源頭，提升公司防禦，協助阻檔未來攻擊。

1. 以確認政策、工具、程序、有效的管理與溝通計畫等手段做好萬全準備。針對先前事件作事後剖析，可以形成持續改進的基礎。建立由通訊、營運永續、法律與保險等多重部門員工組成的事件應變團隊，並實施模擬事件應變演練。
2. 可透過內部安全性工具進行事件偵測，不過公司企業被外部單位通知發生意外事件的狀況其實更常見。快速反應團隊必須對事件進行初步歸類。
3. 抑制屬於分門別類的階段：受影響主機或系統被確認、隔離或以其他方式緩解、通知受影響單位，以及調查狀態的建立。此階段內容包括處理證據，以及與相關單位進行事件溝通。
4. 調查，是資安員工確認優先順序、範疇與事件引發源頭的階段。
5. 補救，是受影響系統的事後修補、確定威脅已被抑制的分析，與確認監管單位是否要求回報事件。
6. 復原，是對程序與政策影響的事件分析、指標的收集，並將學到的經驗納入未來應變活動與訓練裡。
7. 公司還必須有一套應急方案，處理當事件應變團隊內部成員，涉嫌必須為事件負責的狀況，無論是有意為之或是失誤。

6 自攜設備(BYOD)安全性政策範本

就大部份公司而言，自攜設備已然成為可接受的現況，因為員工們造就了能夠在自己的智慧型手機或其他行動設備上工作促進生產力的狀況。事實上，就近期Frost & Sullivan的調查指出，單行動力而言便能增加34%的生產力。另一份報告則指出，運作得當的BYOD政策，可以讓公司企業平均每年每位員工節省350美元。

不過，BYOD同樣打開了非處理不可的新攻擊面向與弱點。整合BYOD安全性政策，需要審慎考量各個計分議題，只能由業務經理、IT執行、HR與法律群集結而成的團隊決定。

1. 公司應指定並限制哪些裝置可以連結網路，並且明確指出僅目前版本的作業系統，例如Android或iOS是被允許的。
2. 公司也應該要求員工自有裝置在能夠存取網路前，應安裝行動裝置管理軟體。
3. 裝置必須以加密密碼存儲的方式，存放所有使用者保存的密碼。
4. 裝置必須設定安全的密碼，而密碼必須遵守公司的密碼政策。該密碼絕對不能與任何其他用於組織內的憑證相同。
5. 使用者僅能下載工作必要的資料到他們的行動裝置上。
6. 使用者必須立即向IT回報任何遺失或遭竊的裝置。
7. 如有使用者疑似未經授權透過行動裝置存取公司資料，必須立即回報。
8. 裝置不能破解(jailbroken；越獄)、獲取最高權限(rooted)，或安裝任何用來獲得被禁止應用軟體存取權的軟體/韌體。
9. 使用者不得下載盜版軟體或非法內容到自有裝置。
10. 應用程式只能從已獲核准的來源安裝。
11. 裝置必須與製造商或網路提供的修補程式保持同步更新。
12. 公司是/否補償一定程度的員工裝置成本或服務方案成本。
13. 員工裝置遺失時、員工終止雇用時，或IT偵測到資料或政策外洩、病毒或類似威脅危及公司資料與技術架構安全性時，可以遠端抹除。
14. 員工被預期全時以道德的方式使用裝置，並遵循公司可接受使用方式政策。
15. 員工因作業系統癱瘓、錯誤、臭蟲、病毒與任何其他軟硬體失效造成裝置無法使用時，對公司與/或個人資料的損失全權負責。