TOM 集團有限公司

資訊安全政策

(如中英文版本有差異之處，以英文版本為準。)

目錄

1. 政策聲明

建立本文件旨在界定及有助傳達將適用於整個集團（包括 TOM 集團有限公司（「本公司」）、其附屬公司及受控制聯屬公司）的資訊**保密、完整及供應**的共同政策。本文件所述政策為所有其他資訊安全政策、程序及準則藉以制訂的基準。

本政策適用於集團所有成員公司，包括所有國家的業務部門。

本政策適用於建立、傳達、儲存、傳輸及銷毀集團內所有不同類型的資訊，包括但不限於電子版本、印刷本及口頭披露，且不論以個人、電話或其他方式進行。

有關本政策的問題應直接轉交首席技術官。

2. 原則

2.1 問責

集團內各人均有責任保護資訊。

- 資訊安全問責及責任必須在整個集團中清楚界定及確認。
- 集團內的所有人士（包括僱員、顧問、承包商及臨時員工）均須對存取及使用資訊（如新增、修改、複製及刪除）負責。
- 所有問責方必須以及時與協調的方式行事，以防止或回應資訊及資訊系統安全遭到違反及威脅（人手或電腦化或結合兩者）的情況。

2.2 比例

資訊安全控制應與修改、拒絕使用或披露資訊的風險相對應。

- 就資訊的價值及敏感度以及資訊所遭受的威脅應採取適當資訊安全措施。
- 資訊安全措施應彌補儲存、傳輸、處理或使用資訊的內外環境中固有的風險。

2.3 知情需要

存取公司資訊應受到限制，僅有明顯商業理由存取資訊者方可存取資訊。

2.4 組織角色及責任

須確定組織的角色及責任，以制訂、傳達、實施及監管政策。

除本政策確定的特定角色及責任外，各業務部門的管理層有責任監管本文件內所載政策在其管轄範圍內實施。

2.4.1 首席技術官

首席技術官須負責：

1. 建立及改善整個集團內的資訊安全文化。
2. 管理集團資訊安全政策的發展、部署及維持。
3. 保證整個集團內的資訊安全狀況，包括妥善部署及遵守集團資訊安全政策的情況。
4. 協調與重大安全事項有關的活動。

首席技術官尤其須：

- 按需要發表有關遵守本政策的準則。
- 檢討集團資訊安全措施的有效性，包括在有需要時檢討及監察集團內的安全事故。
- 為業務部門就資訊安全狀況及重大資訊安全事項實施匯報程序。
- 掌有集團層面的資訊安全監管及風險評估方法。
- 促進整個集團內對潛在威脅、漏洞及控制技術的了解。
- 監察集團內外的資訊安全趨勢，同時通知集團高級管理層有關資訊安全相關問題及影響組織的活動。

2.4.2 資訊安全託管人

各業務部門的管理層須為業務部門委任一名資訊安全託管人。資訊安全託管人須負責：

1. 建立及改善業務部門的資訊安全文化。
2. 確保制訂及部署業務部門的額外政策、程序及準則，以支援本政策及相關政策、程序及準則。
3. 保證業務部門資訊安全狀況，包括妥善部署及遵守業務部門及集團資訊安全政策、程序及準則的情況。
4. 協調與重大安全事項有關的活動。

資訊安全託管人尤其須：

- 界定業務部門內的額外資訊安全角色及責任。
- 確保部署方法、程序及風險評估，以支持集團的資訊安全政策、程序及準則。

- 提供資訊安全教育，並確保舉辦及出席培訓課程。
- 協助業務部門管理層制訂處理資訊安全事故的有效對應計劃。
- 就資訊安全狀況在業務部門實施匯報程序，並於有需要時向業務部門管理層及集團匯報。
- 檢討業務部門資訊安全措施的有效性，包括在有需要時檢討及監察業務部門內的安全事故並向集團匯報。
- 協助業務部門考慮持續及計劃業務中的資訊安全風險。
- 與業務部門的管理層合作進行資訊安全風險評估。
- 促進業務部門內對潛在威脅、漏洞及控制技術的了解。
- 監察業務部門內外的資訊安全趨勢，同時通知業務部門高級管理層有關資訊安全相關問題及影響業務部門的活動。

2.4.3 資訊擁有人

各業務部門的管理層須確保集團每項資訊均獲分配予一名擁有人，稱為「資訊擁有人」。本文件內資訊擁有人一詞僅適用於與本政策有關的資訊安全事項，並不代表對資訊有任何形式的法定擁有權。

一般而言，除非另有指定，否則，

1. 一項資訊的建立人須被假定為資訊擁有人。
2. 對於從外界接收的資訊，指定接收者須自動成為資訊擁有人。

資訊擁有人負責：

- 確定與資訊相關的授權及處理程序。
- 採取措施確保儲存、處理、發佈及定期使用資訊方面已採用適當的控制。
- 確保資訊提供予所有需要知情的相關人員。

2.5 資訊管理

2.5.1 分類及標籤

為管理及控制資訊的存取，業務部門的行政人員應考慮將資訊正式分類及標籤，但應當適當考慮業務上的需要、成本（內部及外部）和實際性。正式分類指引載於附錄一。

2.5.2 一致地保護

資訊不論資訊在何處、以何種形式儲存及目的為何，應當一致地保護資訊。

2.5.3 披露資訊

各業務部門的管理層在與資訊安全託管人諮詢，並遵照首席技術官所發出的標準後，將就披露和收取任何敏感資訊（如發出或簽立不披露協議及處理從外界人士收取的敏感資訊）建立及實施特定規則及指引。

2.5.4 控制權變動

與資訊安全過程有關的變動，包括系統及程序上的變動，必須獲得適當批准及記錄並通知適當的有關方。應就保密資訊實施正式的控制權變動程序。

2.6 存取控制

應作出適當控制以平衡對資訊的存取以及支援資訊資料的相關風險。

- 資訊的存取必須由與其分類相若的特定商業規定指引並根據「知情需要」基準加以控制，不論要求取得資訊人士的職級。
- 存取資訊須取得授權。須就每個資訊系統（不論電腦化與否）實施授權過程。授權過程須由資訊擁有人以及適用的資訊安全託管人批准。

2.7 評估

公司應定期評估與資訊及資訊系統有關的風險。

- 業務部門的行政人員應確保定期及在情況需要時進行風險評估，從而決定用以保障資訊控制的有效性。透過風險評估過程識別的弱點應符合風險可能性及影響的情況下在時限內處理。
- 公司應定期或當業務部門作出重大修改，令其風險環境可能出現變動時，獨立地檢討就每項業務部門實施的資訊安全措施。

2.8 意識

所有有需要知情的人士，應可存取適用或可供查閱有關資訊安全及資訊系統的原則、標準、公約或機制，並應獲告知有關資訊安全的適用威脅。

- 與所有人士的誠信、知情需要及技術能力有關的適當資歷，須在存取資訊或提供資訊支援資源前核實。
- 所有集團的人員必須明白集團有關資訊安全的政策及程序，並必須同意根據該等政策及程序履行其工作。
- 集團的業務夥伴、供應商、客戶及其他商業聯繫人士，必須透過合約中指定的特定語言獲告知其資訊安全的責任，有關責任界定他們與集團的關係。

- 首席技術官應設立渠道及組織，在集團的業務實體內分享及溝通資訊安全的相關知識及經驗。

2.9 教育

本政策須傳達予集團內所有人員，確保他們明白本政策及政策下的責任。

- 公司必須向所有僱員提供有關資訊安全的培訓。培訓須包括政策、標準、底線、程序、指引、責任、相關強制執行措施以及未能遵守有關規定的後果。公司應定期進行培訓及復修培訓。
- 所有集團的人員必須獲提供支持參考資料，以容許他們適當地管理及以其他方式管理集團的資訊。

2.10 事故管理

公司應盡快及有效地回應所有資訊安全事故，從而確保盡量減低對任何業務的影響以及減少日後遇到同類事件的可能性。

- 資訊安全事故（即影響或可能影響資訊安全的任何事件）必須向適當人士匯報，包括集團首席執行官、業務單位主管、企業系統及資訊科技部及相關業務部門的法律部（或集團法律部，如事故發生於集團層面）、資訊擁有人、資訊安全託管人，以及在業務部門或集團其他實體內可能受到事故影響的人士。有關人士亦應匯報處理及解決事故的步驟。
- 各業務部門應設有有效的資訊安全事故應變計劃。該計劃應說明（其中包括）：(i)實體內應對事故人員的組成及角色；(ii)與內部及外界人士（後者包括客戶、執法機構、監管機構及傳媒）溝通；及(iii)識別事故成因以及恢復受影響數據所用之技術方法、工具及資源。

2.11 持續營運及應變計劃

資訊系統應按保存機構營運持續性之方式設計及運作。

各業務部門須設有計劃確保維持資訊的保密性、完整性及可用性，以在業務中斷或災難情況發生時支持業務的持續性。該計劃必須予以記錄及告知相關人士，並定期進行相關的演習。

2.12 法律、監管及合約要求

所有與資訊安全有關的法律、監管及合約要求（包括適用個人資料保護及私隱法律）必須加以考慮及處理。

- 當處理資訊安全時，集團最低限度必須符合所有適用法律及監管要求。各業務部門有責任確保其遵守各自的監管及其他法律要求。

2.13 資訊私隱

各業務部門須審慎實施資訊安全措施，以符合業務部門及集團適用的法律及資訊私隱及資料保護政策。

2.14 政策文檔及管理

公司須開發及維持解決資訊安全各方面的政策及支持標準、底線、程序及指引。該等指引必須指定責任、酌情權水平，以及個別人士或機構實體獲授權承擔的風險水平。

本政策是一份不斷發展的文件，需要定期審閱及更新。此過程可以包括但不限於監管關注及法例、核心業務及技術的變化。

2.15 政策例外情況

有時須就業務或實際目的規定本政策的例外情況。例外情況必須就資訊安全託管人的建議經業務部門的負責人授權及經首席技術官批准。

- 例外情況包括該等情況的理據、期限及詳情，必須在一段合理時間內記錄。
- 當業務或風險、或負責的行政人員出現變動時，或首席技術官決定的一段時間後（以較早者為準），公司須重新評估及重新批准例外情況。

2.16 違反政策

違反本政策被視為嚴重違反行為並將會受到適當處理，其重點在於防止日後發生違反行為。

不遵守資訊安全政策、標準或程序為紀律處分（包括終止聘用）的依據。

附錄一：有關數據分類及標籤的指引

1. 數據分類

所有資訊應按敏感度水平加以分類。現建議三項分類，此等分類為：

- 公開
- 內部使用
- 保密

此等分類的目在於根據「知情需要」的政策保護資訊免受任何未經授權披露、使用、修改或刪除，即存取公司資訊應受到限制，只有該等有明顯商業理由存取資訊的人士方可獲授權存取資訊。

並無特定分類的資訊應被審查以確定其分類，如無法分類則預設的安排是有關資訊被視作分類為內部使用，並應作出相應處理。

在本附錄內：
- 一項資訊的存取控制表為獲授權有權獲取資訊之人士或一方的名單。
- 分派名單為實際獲分派資訊之人士或一方之名單。

1.1 公開

「公開」分類適用於已獲相關業務部門的管理層明確批准向集團以外之公眾人士公開披露的資訊。

只有獲指定人士方可分類資訊為公開。

只有獲指定人士方可披露公開資訊。披露有關資訊須依循預設的程序、規則及指引。

1.2 內部使用

「內部使用」分類適用於資訊，即其意外地或無取得授權下獲披露，可能對業務部門、部門或集團造成負面影響並就解決有關影響時可能招致成本。

不得在無獲得資訊擁有人事先批准的情況下向集團以外的任何人士披露供內部使用的資訊。如供內部使用的資訊附有任何存取控制名單，則在無獲得資訊擁有人的事先批准下其不應向該獲取限制以外的任何其他人士披露。可以在集團內披露無存取控制名單供內部使用的資訊。

資訊擁有人亦對供內部使用的資訊施加額外披露或處理限制。額外限制不得削弱本文件

所述的基本披露規則。

1.3 保密

「保密」分類適用於資訊，即如不慎地或在無授權情況下披露，可能對業務部門、部門或集團造成重大負面影響，或就處理此等影響可能引致重大成本。

保密資訊應經常設有分派名單或存取控制名單，以及在無資訊擁有人的事先批准下，不應向該分派名單或存取控制名單以外的任何人士披露。在無存取控制名單的情況下，分派名單被視為存取控制名單。在無分派名單及存取控制名單的情況下，沒有保密資訊擁有人的事先批准，不應向任何人士披露保密資訊。

資訊擁有人亦可以進行額外披露或處理保密資訊的限制。額外限制不得削弱本文件所述的基本披露規則。

此外，保密資訊必須在處理（包括展示、儲存、傳送及棄置）時，就故意及不慎作出未經授權披露時受到進一步保護。

由於集團業務多元化及基於當地需要，業務部門應進一步考慮其業務需要、遵守多項法例及行業規定以設立合適的類別。然而，最終的類別應納入三個預設的分類及不得違反或抵觸本政策所載的原則。

2. 資訊標籤

業務部門的管理層負責評估、設計及實施其各自業務部門的資訊標籤適用的特定程序。然而，有關活動應按以下基準證明及支持：

1. 當地法例所規定，或
2. 在無其他替代方法的情況下，個別標籤是持份者得知資訊敏感度的唯一方法，及
   I 其在技術上可行，及
   II 其在經濟上可行，即該項行動的總利益超出包括持續維護成本的成本。

如某個業務部門決定不進行資訊標籤，下列規則應適用：

- 保密資訊應首先被標籤。
- 資訊擁有人負責按照分類對資訊進行標籤。
- 只有資訊擁有人或資訊擁有人指定的人士獲授權更改資訊的標籤。
- 分類標籤應是顯而易見。
- 存取控制名單以及任何額外限制應在分類標籤清楚說明或以其他方式顯而易見。例如，一項分類標籤可能是「供內部使用 - 僅供 X 公司使用」或「保密 - 僅供 XX 部門使用」或「供內部使用 - 僅供 TOM 集團內部使用」。
- 存取控制名單或額外限制不得取代分類，即不論資訊的任何額外限制及分類（如保密）應附有標籤。