長江生命科技集團有限公司

資訊安全政策

目錄

1. 政策聲明

本文件旨在界定及協助傳達將適用於整個集團（包括長江生命科技集團有限公司（「長江生命科技」或「本公司」）及其附屬公司）的資訊**保密、完整及供應**的共同政策。本文件所述政策為制定所有其他資訊安全政策、程序及準則所依賴的基準。

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集團資訊科技部主管。

本公司致力持續提升其資訊安全常規及管理系統，以應對不斷演變之威脅及網絡安全風險。

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（人手或電腦操作或結合兩種方式）安全遭違反及受到威脅的情況。

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成正比。

- 就資訊的價值及敏感度以及資訊容易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，僅有明確商業理由存取資訊者方可存取資訊。

2.4 組織角色及責任

組織角色及責任須予確定，以制訂、傳達、實施及監管本政策。

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 集團資訊科技部主管

集團資訊科技部主管須負責：

1. 建立及改善整個集團內的資訊安全文化。
2. 管理及制定、部署及維持集團資訊安全政策。
3. 確保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。

集團資訊科技部主管尤其須：

- 按需要發佈遵守本政策的準則。
- 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。
- 為業務部門的資訊安全狀況及重大資訊安全事項實施匯報程序。
- 管理集團層面之資訊安全監管及風險評估方法。
- 促進整個集團對潛在威脅、漏洞及控制技術的了解。
- 監察集團內外的資訊安全趨勢，同時持續知會集團高級管理層有關影響組織的資訊安全相關問題及活動。

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. 確保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，包括檢討及監察業務部門內的安全事故，並在有需要時向集團匯報。
- 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，同時持續知會業務部門高級管理層有關影響業務部門的資訊安全相關問題及活動。

2.4.3 資訊擁有人

各業務部門的管理層須確保每項集團資訊均獲指派一名擁有人，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. 資訊的建立人應為資訊擁有人。
2. 對於從外界接收的資訊，指定接收者應自動成為資訊擁有人。

資訊擁有人負責：

- 決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，但應妥善顧及業務上的需要、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 一致保護資訊

不論資訊在何處、以何種形式儲存及目的為何，資訊應一致獲得保護。

2.5.3 披露資訊

各業務部門的管理層於諮詢資訊安全託管人及遵照集團資訊科技部主管所發出的準則後，將就披露和接收任何敏感資訊（如發出或簽立不披露協議及處理從外界人士取得的敏感資訊）建立及實施特定規則及指引。

2.5.4 控制權變動

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、記錄及通知適當的有關方。應就保密資訊實施正式的控制權變動程序。

2.5.5 數據保留

各業務單位的資訊擁有人將定期更新及審閱個人數據清單，例如：個人識別資訊（PII）、受保障健康信息（PHI）、付款卡行業（PCI）數據，由各種資訊系統維護，並建立明確的數據保留政策，規定敏感數據的保留期限。根據數據保留政策，應建立刪除不再用於原始收集目的之敏感數據的相關流程。

2.6 存取控制

應作出適當控制以對資訊及支援資訊資源的存取與相關風險之間取得平衡。

- 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。每項資訊系統（不論電腦化與否）須予實施授權過程。授權過程須由資訊擁有人及適用的資訊安全託管人批准。

2.7 網絡安全措施

業務部門行政人員應實施網絡安全措施，以保護系統和數據免受網絡攻擊和未經授權的存取。 措施應包括但不限於：

- 安裝端點偵測及回應（EDR）軟件以偵測行為異常並及時就網絡威脅作出回應；
- 限制、控制及執行特權存取權限及秘密身分驗證憑據的分配和使用，必須經特權存取管理（PAM）進行。只有在授權過程完成後方可獲授予特權，並應保留授權記錄，以保障特權存取權免受憑據被盜用造成的網絡威脅；
- 採用多重身份驗證（MFA）以安全進行遠程登入公司網絡及關鍵/敏感系統；
- 保障重要業務資訊及個人數據（例如加密、標記化和雜湊），並妥善管理及保障加密密鑰；
- 安裝網絡安全/防毒軟件，以防止惡意軟件的攻擊；
- 安裝防火牆以限制來自外部網絡的數據存取；及
- 就操作系統定期進行之安全更新。

2.8 漏洞管理

漏洞管理流程及程序應予以界定，以識別、追踪、管理及修復資訊系統的技術漏洞。

- 技術漏洞應通過相關風險與措施進行識別及管理。此舉可能涉及修補易受攻擊的系統、應用更強大的配置設定、修改源代碼或其他補救措施。
- 任何已知漏洞應及時予以修復。就相關技術漏洞的通知作出反應之時間表應予以界定。
- 具敏感或機密資訊或高風險（例如網域控制器）的系統應優先修復其漏洞。

2.9 備份及恢復

備份和恢復政策、流程和程序應予以界定，要求須就所有重要資訊、軟件和系統映像的備份保留副本及進行測試，並且能在災難故障後恢復（例如勒索軟件攻擊）。

- 備份和恢復過程應符合資訊和系統的安全及資訊敏感性要求。

- 各系統流程和程序需反映業務要求、所涉及資訊的安全要求和資訊系統的關鍵性，包括：
  - 備份範圍（例如完整、差異或快照）
  - 頻率

- 流程和程序應包括異地與離線、氣隙或不可變備份，以避免災難性故障所造成的任何損害，例如: 勒索軟件攻擊或主站災難。

- 媒體備份需要定期測試以確保其在緊急情況下可行。同時應測試恢復程序和時間表。

- 監控定時備份並及時解決任何故障，以確保備份完整，符合備份政策。

- 加密機密或敏感數據或所有備份。

2.10 評估

公司應定期評估資訊，資訊系統及網絡安全面對的風險。

- 業務部門的行政人員應確保定期及在有需要之情況下進行風險評估，從而決定用以保障資訊、資訊系統和網絡安全而安裝所設置的控制的有效性。於風險評估過程中識別的漏洞，應在符合風險可能性及影響的時限內處理。

- 每個業務部門的網絡安全實施應由外部各方定期，或每當業務部門的重大修改可能改變其風險環境時獨立審查。進行審查的人士應具備適當的技能、資格和經驗。

- 當獨立審查發現任何漏洞或安全性不足時，需要採取補救措施。

2.11 意識

有需要知情的所有人士，應可存取適用或可供查閱有關資訊及資訊系統安全的原則、標準、慣例或機制，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，集團關係的合約中顯示的特定語言獲告知彼等的資訊安全責任。

- 集團資訊科技部主管應設立渠道及組織，在集團業務部門之間分享及溝通資訊安全的相關知識及經驗。

2.12 教育

本政策須傳達予集團內所有人員，讓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，以及未有遵守有關規定的後果。公司應定期進行培訓及複修訓練。

- 所有集團的人員必須獲提供支持參考資料，以容許他們適當地保護及以其他方式管理集團的資訊。

2.13 事故管理

公司應盡快及有效回應所有網絡安全事故，從而盡量減低對任何業務的影響，以及減少遇到同類事件的可能性，必須定期測試網絡安全事件響應計劃和程序。

- 網絡安全事故（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，包括相關法律部（集團法律部或業務部門法律部（如適用））（或長江生命科技公司秘書部（如適用））、資訊擁有人、資訊安全託管人、網絡事故協調人（如適用），以及在業務部門或集團內其他公司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網絡安全事故應變計劃。該計劃應說明（其中包括）：(i) 公司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）的溝通程序；(iii) 將用於識別、監測、檢測、分析安全事件和事件的技術手段、工具和資源；及(iv) 應對事件的程序，包括遏制、根除、恢復和升級。

2.14 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援業務的持續性。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。

2.15 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（包括適用的保護個人資料及私隱法律）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，以及監管要求。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。

2.16 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，以及保護資訊私隱及資料之政策。

2.17 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。該等指引必須指定個人實體或組織實體獲授權承擔的責任、酌情權水平，以及風險水平。

本政策是一份不斷更新的文件，需要定期審閱及更新。此過程可包括（其中包括）監管關注及法例、核心業務及技術的改變。

2.18 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。例外情況必須根據資訊安全託管人的建議及經集團資訊科技部主管批准後，經業務部門的負責人授權。

- 例外情況包括該等情況的理據、期限及詳情，必須在合理時限內記錄。
- 當業務或風險、負責的行政人員出現變動時，或集團資訊科技部主管決定的一段時間後（以較早者為準），公司須重新評估及重新批准例外情況。

2.19 違反政策

違反本政策被視為嚴重違反行為並將獲適當處理，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。

3. 對本政策之責任

本政策已經董事會審閱、批准及採納。可持續發展委員會監督並監察本政策及集團網絡安全策略之實施與執行，並可不時向董事會提出修訂建議以尋求批准。

生效日期: 二零二零年十二月
更新日期: 二零二五年十一月

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。現建議三項預設分類，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，只有該等有明確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，並應被作出相應處理。

在本附錄內：

- 資訊的存取控制名單為獲授權有權獲取資訊之人士或各方的名單。
- 分派名單為實際獲分派資訊之人士或各方之名單。

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將資訊分類為公開。

只有獲指定人士方可披露公開資訊。披露有關資訊須依循既定的程序、規則及指引。

1.2 內部使用

「內部使用」分類適用於資訊，即其不慎地或無取得授權下獲披露，可能對業務部門、營運公司或集團造成負面影響，並在處理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獲取限制以外的任何其他人士披露。於集團內，可披露並無存取控制名單之供內部使用資訊。

資訊擁有人亦可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、營運公司或集團造成重大負面影響，並在就處理有關影響時可能招致重大成本。

保密資訊應經常存置分派名單或存取控制名單，以及在無獲得資訊擁有人的事先批准下，不應向存取控制名單以外的任何人士披露。如無存取控制名單，分派名單被視為存取控制名單。如無分派名單及存取控制名單，在無獲得資訊擁有人事先批准下，不應向任何人士披露保密資訊。

資訊擁有人亦可以對保密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。

此外，保密資訊必須在處理（包括展示、儲存、傳送及棄置）時，就故意或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就其各自業務部門的資訊標籤評估、設計及實施適用的特定程序。然而，有關活動應獲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，個別標籤是持份者可能獲提醒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就資訊提供標籤，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提供標籤。
- 只有資訊擁有人或資訊擁有人指定的人士應獲授權更改分類標籤。
- 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顯而易見的方式表達。例如，一項分類標籤可能是「內部使用－僅供 X 公司使用」或「保密－僅供 XX 部門使用」或「內部使用－僅供長江生命科技集團內部使用」。

- 存取控制名單或額外限制不能取代分類，即不論任何額外限制，資訊分類（如「保密」）應列明在標籤上。