PROFIT RISE

C O N S U L T I N G

公開 · 對外

資訊保安政策

香港 · 粵港澳大灣區 · 亞太地區

文件標題	資訊保安政策
文件編號	**PRC-IS-001**
版本	**1.0**
狀態	**已批准**
負責人	**資訊保安總監／保安主管**
批准人	**董事總經理**
生效日期	**2026 年 9 月 12 日**
下次檢討日期	**2027 年 9 月 12 日**
分類	**公開（對外）**

本文件一經列印或下載即屬未受控版本。現行版本刊載於 profitriseco.com。

1. 引言

Profit Rise Consulting（「Profit Rise」、「本公司」、「我們」）賴以向客戶提供服務的基礎，是我們所持有及處理的資料的保密性、完整性及可用性 — 包括客戶資料、我們自身的業務資料，以及我們所建立及提供意見的系統和模型。作為一家提供資訊保安及人工智能管治服務的顧問公司，我們以自身倡導客戶採納的相同標準要求自己。

本政策列明我們的資訊保安承諾，以及規管我們保護資料方式的原則。本政策是我們資訊保安管理方針的最高層級聲明，並由內部備存的各項標準及程序作支援。

2. 目的及目標

本政策的目的是保護 Profit Rise 的資訊資產，以及客戶和合作夥伴託付予我們的資料，以抵禦威脅，並確保我們符合適用的法律、監管及合約保安義務。

我們的資訊保安目標是：

1. 維護資料的**保密性**，確保只有獲授權人士方能存取。
2. 保障資料及系統的**完整性**，確保其保持準確，且不會被未經授權方式更改。
3. 確保合法需要相關資料及系統的人士得以**取用**。
4. 按資料的敏感度及威脅程度相稱地管理保安風險。
5. 遵守 PDPO、PIPL、GDPR 及 PDPA，以及我們客戶和合作夥伴的保安要求。
6. 展現與 ISO/IEC 27001:2022 及 NIST 網絡安全框架（CSF）2.0 相符的持續改進。

3. 適用範圍

本政策適用於：

- Profit Rise Consulting 以任何形式持有或處理的所有資料。
- 用於儲存、處理或傳送該等資料的所有系統、應用程式、裝置、雲端服務及網絡。
- 代表或以 Profit Rise 名義行事的所有人員，包括董事、僱員、承辦商及分判商，以及可存取我們資料或系統的第三方。

4. 資訊保安原則

我們恪守下列原則：

1. **以風險為本的保障** — 管控措施按經評估的風險選取，並考慮資料價值、適用威脅及外洩事件的影響。
2. **最小權限** — 僅按履行職務所需範圍授予存取權，並定期檢討。
3. **分層防禦** — 我們採用互補的技術、實體及行政管控措施，使任何單一管控措施不成為單點故障。
4. **設計上保安及預設保安** — 在建立或採購系統時，保安及私隱自始納入考慮，且系統預設採用安全組態。
5. **共同責任** — 保安是人人的責任；所有人員均須就其所處理的資料承擔保護責任。

5. 資訊保安的組織安排

- **董事總經理** 就資訊保安負有最終責任，並設定保安風險承受程度。
- **CISO／保安主管** 負責本政策、備存資訊資產及風險紀錄、監督管控措施，並協調事故應變。
- **所有人員** 遵守本政策、完成保安意識培訓，並即時匯報懷疑事故或弱點。

管理層至少每年檢討資訊保安一次，並參考風險評估、審核結果及事故經驗。

6. 管控範疇

我們的資訊保安管控措施按下列範疇組織，反映 ISO/IEC 27001:2022 的管控主題：

6.1 資產及資料分類

- 識別資訊資產，並為其保安指派責任。
- 按敏感度為資料分類（例如公開、內部、機密、受限），並按分類處理。
- 客戶資料及個人資料預設按機密或受限資料處理。

6.2 人力資源保安

- 在聘用前按比例進行背景及推薦人審查。
- 所有人員均確認保密義務及本政策。
- 在入職時及其後定期提供保安意識培訓。
- 離職時即時撤銷存取權，並收回公司資產。

6.3 存取控制

- 僅向獲授權人士授予資料及系統存取權，並使用可唯一識別的身分。
- 採取強式驗證；敏感系統及遙距存取須啟用多重身份驗證。
- 定期檢討存取權，並因應職務變更作出調整；特權存取須嚴加控制及監察。
- 密碼及其他憑證按我們的憑證標準處理。

6.4 實體及環境保安

- 限制未經授權人士實際進出辦公室、設備及紙本資料。
- 保護裝置及可移除媒體免遭盜竊、遺失及未經授權存取。
- 機密資料採取清理桌面的做法。

6.5 營運保安

- 按供應商指引及我們的更新時間表為系統及軟件安裝修補程式並加以維護。
- 部署並持續更新防惡意軟件措施。
- 系統更改按照設有適當測試及批准的受管理流程進行。
- 備存及檢討日誌以偵測異常情況，並定期測試備份以確保可復原。

6.6 通訊及網絡保安

- 使用強式加密（例如 TLS）保護傳送中的資料。
- 遙距存取僅可經獲批及已驗證的渠道提供。
- 網絡邊界及雲端環境按預設拒絕存取的組態設定。

6.7 系統採購、開發及維護

- 在採購或建立系統時界定保安要求。
- 開發遵循安全編碼慣例，並在發佈前測試常見漏洞。
- 監察第三方組件及依賴項以察知已知漏洞。
- 我們開發或部署的人工智能系統須受額外管控（見第 7 節）。

6.8 供應商關係

- 在委聘可處理我們資料或存取我們系統的第三方前，先評估其保安水平。
- 合約載入適當的保安及保密義務。

- 在關係存續期間監察供應商保安情況，並在合約結束時終止存取。

6.9 事故管理

- 保安事件及事故須即時匯報，並透過事故應變流程處理。
- 按嚴重性為事故分類，予以控制、清除及復原，並進行根本原因分析及補救。
- 對須呈報的事故，按規定通知受影響客戶、監管機構及資料保護當局。
- 記錄經驗教訓，用以改進管控措施。

6.10 業務持續性

- 我們備存持續性及復原安排，以在發生事故時保護關鍵活動及資料。
- 定期測試持續性及復原計劃。

6.11 法律及合規

- 識別並遵守與資訊保安有關的法律、法規及合約規定（包括資料保護及特定行業規定）。
- 保護知識產權，並遵守我們政策所載的紀錄管理及保留義務。

7. 人工智能系統的保安

反映我們以人工智能管治為重點，在開發、部署或使用人工智能系統時，我們採用額外管控：

- **安全開發生命週期** — 建立及測試人工智能組件時考慮保安因素，包括所使用的數據管道及模型。
- **模型及資料完整性** — 監察訓練資料、模型及其輸出的完整性，並在相關情況下記錄資料來源。
- **對抗式穩健性的認識** — 按使用情境採取相稱的措施，處理已知的人工智能特有威脅，包括提示注入、資料投毒及模型逆向風險。
- **資料外洩防護** — 未經事先書面同意，不會使用客戶及個人資料訓練模型，並採取管控措施，防止敏感資料經模型輸出或第三方模型 API 外洩。
- **人為監督及可稽核性** — 由人工智能支援而影響重大的決定須受人為監督，並記錄人工智能使用情況以供稽核。

該等管控措施支持我們與 ISO/IEC 42001:2023 及獲認可的人工智能風險框架（例如我們諮詢工作中使用的 OWASP AI Exchange）保持一致。

8. 可接受使用

- 公司系統及帳戶僅供獲授權的業務用途使用。
- 人員不得濫用系統、試圖繞過管控措施，或在沒有合法業務需要下存取資料。
- 公司管理的裝置須先符合我們的組態及更新要求方可使用。
- 凡准許將公司系統作私人用途，該用途不得損害保安或妨礙履行職務。

9. 監察及合規

- 在符合法律及我們的私隱義務的前提下，我們可監察系統及活動以保護保安。
- 透過定期內部審核及評估，核實本政策的合規情況。
- 違規可能導致紀律處分，最高可至終止僱傭，而在違法情況下會轉介有關當局。

10. 匯報

懷疑發生保安事故、漏洞或違反本政策的情況，須即時向 CISO／保安主管匯報，或透過舉報及發言政策匯報。所有報告均會獲認真處理、調查及跟進，且不會對舉報人作出報復。

11. 政策檢討

本政策至少每年檢討一次；如在威脅形勢、法律或業務範圍方面出現重大變化或重大事故，則會提前檢討。

批准人： Ron Ng，Profit Rise Consulting 董事總經理

日期： 2026 年 9 月 12 日