PROFIT RISE

C O N S U L T I N G

公开 · 对外

信息安全政策

香港 · 粤港澳大湾区 · 亚太地区

文件标题	信息安全政策
文件编号	**PRC-IS-001**
版本	**1.0**
状态	**已批准**
负责人	**信息安全总监／安全主管**
批准人	**董事总经理**
生效日期	**2026 年 9 月 12 日**
下次评审日期	**2027 年 9 月 12 日**
分级	**公开（对外）**

本文件一经打印或下载即属未受控版本。现行版本刊载于 profitriseco.com。

1. 引言

Profit Rise Consulting（「Profit Rise」、「本公司」、「我们」）赖以向客户提供服务的基础，是我们所持有及处理的信息的保密性、完整性和可用性 — 包括客户数据、我们自身的业务信息，以及我们所构建和提供建议的系统及模型。作为一家提供信息安全及人工智能治理服务的咨询公司，我们以自身所倡导客户采纳的相同标准要求自己。

本政策列明我们的信息安全承诺，以及规范我们保护信息方式的原则。本政策是我们在信息安全管理方面的最高层级声明，并由内部保存的各项标准及流程予以支持。

2. 目的与目标

本政策的目的是保护 Profit Rise 的信息资产，以及客户和合作伙伴托付给我们的信息，以抵御威胁，并确保我们符合适用的法律、监管及合同安全义务。

我们的信息安全目标是：

1. 维护信息的**保密性**，确保只有经授权人员方可访问。
2. 保障信息及系统的**完整性**，确保其保持准确且未经授权方式不被篡改。
3. 确保合法需要相关信息及系统的人员能够**获取和使用**。
4. 按照信息的敏感性及威胁程度，相称地管理安全风险。
5. 遵守 PDPO、PIPL、GDPR 及 PDPA，以及我们客户和合作伙伴的安全要求。
6. 体现与 ISO/IEC 27001:2022 及 NIST 网络安全框架（CSF）2.0 相符的持续改进。

3. 适用范围

本政策适用于：

- Profit Rise Consulting 以任何形式持有或处理的所有信息。
- 用于存储、处理或传输该等信息的所有系统、应用程序、设备、云服务及网络。
- 代表本公司或以本公司名义行事的所有人员，包括董事、员工、承包商及分包商，以及可访问我们信息或系统的第三方。

4. 信息安全原则

我们恪守以下原则：

1. **基于风险的保护** — 管控措施依据经评估的风险选取，并考虑信息价值、适用威胁及泄露事件的影响。
2. **最小权限** — 仅按履行职责所需的范围授予访问权限，并定期评审。
3. **纵深防御** — 我们采用互补的技术、物理和行政管控措施，使任何单一管控措施不成为单点故障。
4. **设计安全与默认安全** — 在构建或采购系统时，安全与隐私自始即纳入考虑，且系统默认采用安全配置。
5. **共同责任** — 安全是每个人的责任；所有人员均须就其所处理的信息承担保护责任。

5. 信息安全的组织安排

- **董事总经理** 对信息安全负最终责任，并设定安全风险承受度。
- **CISO／安全主管** 负责本政策、保存信息资产及风险记录、监督管控措施，并协调事件响应。
- **所有人员** 遵守本政策、完成安全意识培训，并立即报告疑似事件或弱点。

管理层至少每年评审信息安全一次，并参考风险评估、审计结果及事件经验。

6. 管控领域

我们的信息安全管控措施按以下领域组织划分，体现 ISO/IEC 27001:2022 的管控主题：

6.1 资产与数据分级

- 识别信息资产，并为其安全指派责任。
- 按敏感性为信息分级（例如公开、内部、机密、受限），并按分级处理。
- 客户数据及个人信息默认按机密或受限信息处理。

6.2 人事安全

- 在聘用前按比例进行背景及推荐人审查。
- 所有人员均确认保密义务及本政策。
- 在入职时及之后定期提供安全意识培训。
- 离职时立即撤销访问权限，并收回公司资产。

6.3 访问控制

- 仅向经授权人员授予信息及系统访问权限，并使用可唯一识别的身份。
- 采用强认证；敏感系统及远程访问须启用多因素认证。
- 定期评审访问权限，并因应职责变更作出调整；特权访问须严格管控并监测。
- 密码及其他凭证按我们的凭证标准处理。

6.4 物理与环境安全

- 限制未经授权人员实际进入办公场所、设备及纸质资料。
- 保护设备及可移动介质免遭盗窃、丢失及未经授权访问。
- 机密资料采取整洁桌面的做法。

6.5 运行安全

- 按供应商指引及我们的更新时间表为系统及软件安装补丁并维护。
- 部署并持续更新防恶意软件措施。
- 系统变更遵循设有适当测试及批准的受管理流程进行。
- 保存及评审日志以侦测异常情况，并定期测试备份以确保可恢复。

6.6 通信与网络安全

- 使用强加密（例如 TLS）保护传输中的信息。
- 远程访问仅可经由获批及经认证的渠道提供。
- 网络边界及云环境按默认拒绝访问的配置设置。

6.7 系统采购、开发与维护

- 在采购或构建系统时明确安全要求。
- 开发遵循安全编码规范，并在发布前测试常见漏洞。
- 监测第三方组件及依赖项以识别已知漏洞。
- 我们开发或部署的人工智能系统须受额外管控（见第 7 节）。

6.8 供应商关系

- 在委托可处理我们数据或访问我们系统的第三方之前，先评估其安全水平。
- 合同中载入适当的安全及保密义务。

- 在合作关系存续期间监测供应商安全情况，并在合同结束时终止访问。

6.9 事件管理

- 安全事件及事故须立即报告，并通过事件响应流程处理。
- 按严重性为事件分级，予以遏制、清除及恢复，并进行根因分析及补救。
- 对须报告的事故，按规定通知受影响的客户、监管机构及数据保护机构。
- 记录经验教训，用于改进管控措施。

6.10 业务连续性

- 我们保存连续性及恢复安排，以在发生中断时保护关键活动及信息。
- 定期测试连续性及恢复计划。

6.11 法律与合规

- 识别并遵守与信息安全有关的法律、法规及合同要求（包括数据保护及特定行业要求）。
- 保护知识产权，并遵守我们政策所载的记录管理及留存义务。

7. 人工智能系统的安全

体现我们以人工智能治理为重点，在开发、部署或使用人工智能系统时，我们采用额外管控：

- **安全开发生命周期** — 构建和测试人工智能组件时考虑安全因素，包括所使用的数据管道及模型。
- **模型与数据完整性** — 监测训练数据、模型及其输出的完整性，并在相关情况下记录数据来源。
- **对抗鲁棒性认知** — 按使用场景采取相称措施，应对已知的人工智能特有威胁，包括提示注入、数据投毒及模型逆向风险。
- **数据泄露防护** — 未经事先书面同意，不使用客户及个人信息训练模型，并采取管控措施，防止敏感数据经模型输出或第三方模型 API 泄露。
- **人工监督与可审计性** — 由人工智能辅助且影响重大的决定须受人工监督，并记录人工智能使用情况以供审计。

这些管控措施支持我们与 ISO/IEC 42001:2023 及经认可的人工智能风险框架（例如我们在咨询工作中使用的 OWASP AI Exchange）保持一致。

8. 可接受使用

- 公司系统及账户仅供经授权的业务用途使用。
- 人员不得滥用系统、试图绕过管控措施，或在没有正当业务需要的情况下访问信息。
- 公司管控的设备须先符合我们的配置及更新要求方可使用。
- 凡允许将公司系统用于私人用途，该用途不得损害安全或妨碍履行职责。

9. 监测与合规

- 在符合法律及我们隐私义务的前提下，我们可监测系统及活动以保护安全。
- 通过定期内部审计及评估，核验本政策的合规情况。
- 违规可能导致纪律处分，直至解除聘用，且在违法情况下将移送有关机构处理。

10. 报告

怀疑发生安全事件、漏洞或违反本政策的情况，须立即向 CISO／安全主管报告，或通过举报及发声政策报告。所有报告均将得到认真处理、调查及跟进，且不会对举报人实施报复。

11. 政策评审

本政策至少每年评审一次；如威胁形势、法律或业务范围发生重大变化或发生重大事件，则提前评审。

批准人： Ron Ng，Profit Rise Consulting 董事总经理

日期： 2026 年 9 月 12 日