PROFIT RISE

CONSULTING

PUBLIC · EXTERNAL-FACING

Information Security Policy

Hong Kong · Greater Bay Area · Asia-Pacific

Document title	Information Security Policy
Document reference	**PRC-IS-001**
Version	**1.0**
Status	**Approved**
Owner	**Chief Information Security Officer / Security Lead**
Approver	**Managing Director**
Effective date	**12 September 2026**
Next review date	**12 September 2027**
Classification	**Public (external-facing)**

This document is uncontrolled when printed or downloaded. The current version is published at profitriseco.com.

1. Introduction

Profit Rise Consulting ("Profit Rise", "PRC", "we", "our") depends on the confidentiality, integrity, and availability of the information we hold and process — including our clients' data, our own business information, and the systems and models we build and advise on. As a consultancy that delivers information-security and AI-governance services, we hold ourselves to the same standards we recommend to clients.

This Policy sets out our information-security commitments and the principles that govern how we protect information. It is the top-level statement of our information security management approach and is supported by standards and procedures maintained internally.

2. Purpose and objectives

The purpose of this Policy is to protect Profit Rise's information assets and those entrusted to us by clients and partners against threats, and to ensure we meet applicable legal, regulatory, and contractual security obligations.

Our information-security objectives are to:

1. Preserve the **confidentiality** of information, ensuring it is accessible only to authorised persons.
2. Safeguard the **integrity** of information and systems, ensuring they remain accurate and unaltered by unauthorised means.
3. Ensure the **availability** of information and systems to those who legitimately require them.
4. Manage security risk in proportion to the sensitivity of the information and the level of threat.
5. Comply with the PDPO, PIPL, GDPR, PDPA, and the security requirements of our clients and partners.
6. Demonstrate continuous improvement aligned with ISO/IEC 27001:2022 and the NIST Cybersecurity Framework (CSF) 2.0.

3. Scope

This Policy applies to:

- All information held or processed by Profit Rise Consulting in any form.
- All systems, applications, devices, cloud services, and networks used to store, process, or transmit that information.
- All personnel acting for or on behalf of Profit Rise, including directors, employees, contractors, and subcontractors, and to third parties that access our information or systems.

4. Information security principles

We are committed to the following principles:

1. **Risk-based protection** — Controls are selected based on assessed risk, considering the value of the information, applicable threats, and the impact of a breach.
2. **Least privilege** — Access is granted only to the extent necessary to perform a role, and reviewed regularly.
3. **Defence in depth** — We layer complementary technical, physical, and administrative controls so that no single control is a single point of failure.
4. **Security by design and by default** — Security and privacy are considered from the outset when building or procuring systems, and systems default to secure configurations.
5. **Shared responsibility** — Security is everyone's responsibility; all personnel are accountable for protecting the information they handle.

5. Organisation of information security

- The **Managing Director** holds ultimate accountability for information security and sets the security risk appetite.
- The **CISO / Security Lead** owns this Policy, maintains the information-asset and risk registers, oversees controls, and coordinates incident response.
- **All personnel** follow this Policy, complete security awareness training, and report suspected incidents or weaknesses promptly.

Information security is reviewed at least annually by management, informed by risk assessments, audit findings, and incident learning.

6. Control domains

Our information-security controls are organised across the following domains, reflecting ISO/IEC 27001:2022 control themes:

6.1 Asset and data classification

- Information assets are identified, and responsibilities for their security are assigned.
- Information is classified (for example, Public, Internal, Confidential, Restricted) according to sensitivity, and handled in line with its classification.
- Client and personal data are handled as Confidential or Restricted by default.

6.2 Human-resource security

- Background and reference screening is conducted proportionately before engagement.
- All personnel acknowledge confidentiality obligations and this Policy.
- Security awareness training is provided on joining and periodically thereafter.
- On termination, access rights are revoked promptly and company assets are returned.

6.3 Access control

- Access to information and systems is granted only to authorised individuals, using uniquely attributable identities.

- Strong authentication is required; multi-factor authentication is enabled for sensitive systems and remote access.
- Access rights are reviewed regularly and adjusted for role changes, and privileged access is tightly controlled and monitored.
- Passwords and other credentials are handled in accordance with our credential standard.

6.4 Physical and environmental security

- Physical access to offices, equipment, and hardcopy information is restricted to authorised personnel.
- Devices and removable media are protected against theft, loss, and unauthorised access.
- A clear-desk and clear-screen approach is applied for confidential material.

6.5 Operations security

- Systems and software are patched and maintained in line with vendor guidance and our update schedule.
- Malware protection is deployed and kept current.
- System changes follow a managed process with appropriate testing and approval.
- Logs are maintained and reviewed to detect anomalies, and backups are taken and periodically tested for recoverability.

6.6 Communications and network security

- Data in transit is protected using strong encryption (for example, TLS).
- Remote access is provided only over approved, authenticated channels.
- Network boundaries and cloud environments are configured to deny access by default.

6.7 System acquisition, development, and maintenance

- Security requirements are defined when systems are acquired or built.
- Development follows secure coding practices, with testing for common vulnerabilities before release.
- Third-party components and dependencies are monitored for known vulnerabilities.
- AI systems we develop or deploy are subject to additional controls (see Section 7).

6.8 Supplier relationships

- Third parties that process our data or access our systems are assessed for security before engagement.
- Contracts include appropriate security and confidentiality obligations.
- Supplier security is monitored during the relationship, and access is terminated on contract end.

6.9 Incident management

- Security events and incidents are reported promptly and managed through an incident-response process.

- Incidents are triaged by severity, contained, eradicated, and recovered from, with root-cause analysis and remediation.
- Reportable incidents are notified to affected clients, regulators, and data-protection authorities as required.
- Lessons learned are captured and used to improve controls.

6.10 Business continuity

- We maintain continuity and recovery arrangements to protect critical activities and information in the event of disruption.
- Continuity and recovery plans are tested periodically.

6.11 Legal and compliance

- We identify and comply with laws, regulations, and contractual requirements relating to information security (including data-protection and sectoral requirements).
- We protect intellectual property and respect the records-management and retention obligations set out in our policies.

7. Security of AI systems

Reflecting our AI-governance focus, we apply additional controls when developing, deploying, or using AI systems:

- **Secure development lifecycle** — AI components are built and tested with security in mind, including the data pipelines and models used.
- **Model and data integrity** — Training data, models, and their outputs are monitored for integrity, and provenance is recorded where relevant.
- **Adversarial-robustness awareness** — Measures address known AI-specific threats, including prompt-injection, data-poisoning, and model-inversion risks, proportionate to the context of use.
- **Data leakage prevention** — Client and personal data are not used to train models without prior written consent, and controls prevent sensitive data from leaking through model outputs or third-party model APIs.
- **Human oversight and auditability** — High-impact decisions supported by AI are subject to human oversight, and AI usage is logged for auditability.

These controls support our alignment with ISO/IEC 42001:2023 and recognised AI-risk frameworks (for example, OWASP AI Exchange) that we use in our advisory work.

8. Acceptable use

- Company systems and accounts are provided for authorised business purposes.
- Personnel must not misuse systems, attempt to bypass controls, or access information without a legitimate business need.
- Company-controlled devices must meet our configuration and update requirements before use.

- Personal use of company systems, where permitted, must not degrade security or interfere with duties.

9. Monitoring and compliance

- We may monitor systems and activity to protect security, to the extent permitted by law and consistent with our privacy obligations.
- Compliance with this Policy is verified through periodic internal audit and assessment.
- Non-compliance may result in disciplinary action, up to and including termination, and — where unlawful — referral to authorities.

10. Reporting

Suspected security incidents, vulnerabilities, or breaches of this Policy must be reported promptly to the CISO / Security Lead, or through the Whistleblowing & Speaking-Up Policy. Reports are treated seriously, investigated, and acted upon without retaliation.

11. Policy review

This Policy is reviewed at least annually or sooner after a significant incident, a material change in threat landscape, law, or business scope.

Approved by: Ron Ng, Managing Director, Profit Rise Consulting

Date: 12 September 2026