

Internal Information Management Policy

Pro Inside Public Company Limited

This Internal Information Management Policy is established to define operating guidelines and standards for the use, storage, and protection of information, which constitutes the internal data of the organization. This includes business data, employee personal data, intellectual property, and any data related to the company's operations (collectively referred to as "Data" or "Information"). The objective is to prevent unauthorized or illegitimate access to company data, prevent improper use of data, and encourage all employees and relevant parties to utilize the company's internal information responsibly and strictly adhere to the established rules.

1. Purpose and Scope

This Internal Information Management Policy of Pro Inside Public Company Limited ("the Company") is established to promote the accurate, appropriate, and efficient use of internal data, as well as to maintain the security of the organization's critical information. It focuses on ensuring business continuity regarding data operations, preventing issues that may arise from unauthorized access or misuse, and preventing inappropriate utilization.

This policy also covers the prevention of all forms of threats that could impact business operations and helps mitigate potential future risks. The Company has established comprehensive Standards, Guidelines, and Procedures aligned with information security best practices to build confidence and ensure effective internal data governance. This policy shall be reviewed at least once a year, or whenever deemed necessary.

2. Data Classification

To ensure appropriate and secure data management across the organization, the Company has classified data according to its significance and sensitivity into the following tiers:

2.1 Public Information

Public Information refers to company data that can be disseminated or disclosed to the public without restriction and does not adversely affect the Company's security, operations, or reputation. Data in this category is deemed non-sensitive, carries no adverse impact, and can be freely used for communications or public relations.

Examples of Public Information include:

- Company background information, history, and vision
- Publicly released annual reports
- Press releases and official public announcements
- Product and service details published on the official website
- Information regarding Corporate Social Responsibility (CSR) activities

This category of data does not require strict access controls; however, it must be accurate and officially approved for release by authorized personnel to prevent errors in public communications.

2.2 Internal Use Only Information

Internal Use Only Information refers to data restricted for access and use exclusively within the organization. It cannot be disclosed or disseminated to external third parties unless formally approved by authorized personnel. This data may relate to internal operations, policies, or procedures, the disclosure of which could compromise privacy or business operations.

Examples of Internal Use Only Information include:

- Internal company policies, rules, and operating regulations
- Standard operating procedure (SOP) manuals or employee handbooks
- Internal meeting materials, such as agendas and meeting minutes
- Departmental or team performance reports
- Internal training schedules and internal company activities

Internal information must be handled with care. Employees and related parties must strictly adhere to established provisions and measures to prevent data leakage and unauthorized usage.

2.3 Confidential Information

Confidential Information refers to data that is critical and sensitive to the Company's business operations, requiring protection and access restriction to authorized personnel only. Unauthorized disclosure or use of such data may result in negative consequences for the organization, such as damage to reputation, loss of business advantage, or regulatory violations.

Examples of Confidential Information include:

- Financial data, such as income statements, balance sheets, and audit reports
- Employee personal and HR records, such as compensation, salary scales, and employment history

- Strategic business plans and prospective projects
- Marketing data, such as promotional campaign plans or market penetration strategies
- Binding contracts, agreements, and covenants with partners and business associates

The management of confidential data requires appropriate safeguards, including encryption, access rights specification, and formal authorization procedures to ensure security and trust throughout business operations.

2.4 Restricted Personal Data

Restricted Personal Data refers to data of high significance directly pertaining to personnel within the organization. It is sensitive personal data that could cause harm or damage to individuals if disclosed, and is strictly governed by personal data protection laws such as GDPR and the Personal Data Protection Act B.E. 2562 (PDPA).

Examples of Restricted Personal Data include:

- National identification card numbers, passport information
- Health data, physical examination records, and medical histories
- Personal financial records, such as personal bank account numbers
- Criminal background records or individual security clearance data

Safeguards for Restricted Personal Data:

- Implement robust data encryption standards
- Strictly limit access privileges to authorized individuals only
- Strictly comply with relevant privacy legislation (e.g., PDPA, GDPR)
- Strictly prohibit storing or transmitting such data via unsecure channels

2.5 Highly Confidential Information

Highly Confidential Information refers to data of the highest strategic value to business operations or organizational advancement, requiring the most stringent protection and access restriction to the highest level of authorized personnel only. Leakage or unauthorized disclosure of this category could inflict catastrophic harm on the Company financially, reputationally, or competitively.

Examples of Highly Confidential Information include:

- Merger and acquisition (M&A) plans or buyout strategies

- Intellectual property data, such as proprietary formulas or patents under development
- Key client accounts, client proprietary data, or partner trade secrets
- Undisclosed litigation, lawsuits, or pending legal disputes
- Confidential details concerning mission-critical flagship projects

Safeguards for Highly Confidential Information:

- Must be stored in high-security systems featuring advanced encryption and sophisticated access control mechanisms
- Enforce strict role-based access strictly on a need-to-know basis
- Data transmission and distribution must occur exclusively via authorized channels with full audit logging
- Physical zone-based security controls must be strictly enforced for physical access areas

Highly Confidential data must be handled with utmost diligence to mitigate potential risks and safeguard operational integrity. Declassification or downgrading of data classified as "Confidential" or "Highly Confidential" requires explicit written authorization from designated authorities and formal notice to relevant stakeholders.

3. Guidelines for Information Use

3.1 Information Use for Assigned Purposes

- **Authorized Purpose:** Corporate information and data must be utilized solely to support assigned operations and duties. Employees must use data to assist decision-making, analysis, or internal administration in accordance with prescribed policies and procedures.
- **Prohibition of Personal Use:** Employees are strictly prohibited from using data for personal gain, such as utilizing customer or financial records for personal activities, or disclosing data to third parties for commercial or personal benefit.
- **Prohibition of Unrelated Third-Party Disclosure:** Employees must not share internal organizational data with unauthorized external parties, such as disclosing commercial information to competitors or leaking strategic corporate plans.

3.2 Access Through Secure Devices and Channels

- **Device Security:** Employees must access company data using approved devices equipped with password protection or encryption to elevate organizational data security, decrease unauthorized

access opportunities, and prevent operational risks. Heightened caution must be exercised when operating company devices outside corporate premises.

- **Virtual Private Network (VPN):** Must be used to secure remote network connections, encrypting data traffic to prevent eavesdropping and interception.
- **Multi-Factor Authentication (MFA):** Mandatory multi-factor authentication provides enhanced security layers by validating identity through multiple sources (e.g., passwords and OTP sent via mobile devices or email).
- **Approved Access Management Systems:** All data access must go through monitored and logged systems, such as Access Management Systems that restrict access strictly in accordance with data sensitivity tiers.

3.3 Data Modification and Alteration

- **Prohibition of Unauthorized Modification:** Employees are prohibited from modifying or altering data within corporate systems without explicit approval from authorized authorities (e.g., altering financial records, production data, or customer entries).
- **Audit Verification:** Critical data modifications must undergo verification and formal logging, utilizing Audit Trails to systematically track changes.
- **Authorized Dissemination:** Publishing or disseminating business or sensitive data (such as financial or customer data) requires prior authorization from designated authorities.

3.4 Disclosure of Company Information

- **Prohibition of Unauthorized Disclosure:** Classified data or data concerning business strategies/activities must not be disclosed to third parties or used in any manner detrimental to the Company without formal executive authorization.
- **Compliance with Policy and Law:** Any disclosure of corporate information must strictly comply with this policy, related company guidelines, and applicable statutory mandates (such as disclosures under contractual agreements or court orders).

4. Physical and Spatial Access Security

Physical security controls are essential measures designed to govern physical access to areas where company data is processed or housed, preventing unauthorized entry and reducing risks of data theft or leakage.

4.1 Restricted Areas

Specific zones where Confidential or Highly Confidential information resides are designated as Restricted Areas, including:

- **Server Rooms:** Spaces hosting servers and critical data storage hardware subject to strict entrance controls, restricted solely to essential technical staff.
- **Data Centers:** Facilities housing corporate mission-critical information secured by multi-layered physical defense and strict perimeter controls.
- **Executive / Critical Meeting Rooms:** Rooms utilized for discussions regarding highly sensitive topics (e.g., strategic plans, high-level business decisions), requiring managed access and surveillance.

4.2 Access Control Mechanisms

- **Access Cards:** Smart card systems maintaining detailed entry/exit logs. Authorized personnel must utilize their access cards, and designated badge-exchange protocols must be enforced for visitors.
- **Security Passwords:** High-security areas must require robust, complex, and sufficiently long passwords/passcodes to prevent unauthorized physical entry.
- **Facial Recognition:** Deployment of biometric facial recognition technology provides highly accurate verification that is exceptionally difficult to forge.

4.3 Access Control Protocols for Restricted Areas

4.3.1 Entry and Exit Logging

Comprehensive and continuous logging of physical entry and exit into restricted zones must be maintained for forensic tracking:

- **Timestamps:** Automated recording of arrival and departure timestamps via badge readers or biometric systems.
- **Identity Credentials:** Full name and official title/position must be logged. External personnel (contractors, auditors) must pre-register identity credentials prior to entry.
- **Purpose of Access:** The explicit business purpose (e.g., hardware maintenance, specialized review) must be documented. Personnel without prior authorized justification are denied entry.

4.3.2 Third-Party Access Procedures

- **Advance Notification:** External visitors must submit advance access requests specifying exact purposes, duration, and responsible company chaperones.
- **Formal Approval:** Must be officially approved by relevant unit managers or designated executives upon assessing operational necessity.
- **Continuous Supervision:** External visitors must be accompanied by designated company personnel at all times and are prohibited from unmonitored interaction with devices or data.

4.3.3 Monitoring and Log Retention

- **Access Monitoring Systems:** Restricted zones must be monitored by Closed-Circuit Television (CCTV) alongside digital access logs, reviewed periodically (weekly or monthly) for irregularities.
- **Log Retention:** Access logs must be securely archived with restricted administrator access for an appropriate period not exceeding one (1) year for audit and investigation purposes.

4.3.4 Alerts and Incident Response

- **Automated Alerts:** Unauthorized access attempts trigger immediate alerts to corporate security personnel and relevant department heads.
- **Anomaly Investigation:** Physical Security officers must promptly investigate incidents, examine CCTV footage, verify identities, and report findings to executive management.

4.4 Storage Device Encryption

Mandatory passcodes or encryption must be enforced across all devices containing company information to safeguard corporate data, reduce unauthorized access risks, and protect business interests, with elevated caution when operating devices off-premises.

5. Access Control and Authorization Management

5.1 Role-Based Access Control (RBAC)

- **Employee Level Alignment:** Data access permissions are granted strictly in accordance with employment level and job necessity (e.g., in the Orbit operational system, managerial tiers and above access administrative management data, while general staff access only operational records relevant to their tasks, such as time attendance).

- **Departmental Segregation:** Enterprise systems must implement role-based access controls segregating duties across departments (e.g., Finance, Human Resources, IT) to prevent unauthorized cross-functional access.

5.2 Security Communication and Training

- **New Employee Onboarding:** Prior to commencing work, all newly hired employees must undergo mandatory security awareness training covering corporate secrecy and data protection policies, cyber threats (such as phishing and malware), legal compliance (PDPA B.E. 2562), and secure data access procedures (complex passwords, MFA).
- **Third-Party Obligations:** External parties (auditors, contractors, business partners) accessing non-public corporate data must be briefed on data governance terms and execute a formal Non-Disclosure Agreement (NDA) when accessing data classified as Internal Use Only or higher.

5.3 Revocation and Periodic Privilege Review

- **Immediate Access Revocation:** Upon employee termination, resignation, contract conclusion, or role reassignment, the Human Resources Department (PD) must immediately notify the IT Department to revoke access rights across all systems and data repositories.
- **Periodic Privilege Audit:** User permissions for employees and third parties must undergo systematic review at least every six (6) months to ensure current validity and alignment with existing responsibilities.

5.4 External Party Access Governance

- **Written Authorization:** External parties must receive formal written approval prior to being granted access to any company data.
- **Need-to-Know Limitation:** Access is strictly restricted to the minimal scope necessary for operational delivery (Need-to-Know basis).
- **Access Logging:** Comprehensive access records must be maintained, logging full name, organization, timestamp, specific data/systems accessed, and operational justification.
- **Disclosure Prevention Controls:** Dedicated, segregated working spaces must be established for auditors or contractors. Physical documents must not leave controlled areas, wide-angle CCTV surveillance must be active, mobile phones/recording devices are banned from the area, and assigned company chaperones must remain present throughout operations. System actions (downloads, modifications) must be monitored continuously.

- **Equipment and Network Restrictions:** External personnel operating within company facilities may only utilize company-supplied hardware and network resources. The use of public Wi-Fi or personal devices (laptops, USB flash drives) is strictly prohibited without explicit IT approval.
- **Data Handover Safeguards:** All data delivered to external parties must be vetted and approved. Confidential or Highly Confidential information must be encrypted (e.g., AES-256) prior to transfer and must never be transmitted via unsecure personal emails or unapproved messaging applications.

6. Confidentiality and Data Protection

6.1 Data Encryption

Data classified as Confidential and Highly Confidential must undergo industry-standard encryption (such as AES-256) across digital environments to prevent unauthorized interception or exposure.

6.2 Handling Data on Personal Devices

Employees are prohibited from storing confidential corporate data on personal devices (laptops, personal computers, mobile phones) unless explicitly approved and equipped with mandated security controls in accordance with the Information Technology Security Policy.

6.3 Physical Document Management

- **Secure Storage:** Physical documents containing confidential data must be housed in secure locked cabinets (via physical keys or electronic locks) or controlled document storage rooms accessible only by authorized personnel.
- **Removal Prohibition:** Confidential paper documents must not be removed from designated workspaces without authorized written permission.
- **Secure Disposal:** Outdated or obsolete confidential documents must be completely destroyed using cross-cut paper shredders or certified third-party document disposal services.

6.4 Prevention of Unauthorized Disclosure

- **Restricted Disclosure:** Employees must not disclose Confidential or Highly Confidential information to unauthorized individuals, including unauthorized coworkers, without formal written approval from supervisors or data owners.

- **Unsecure Environments:** Discussions concerning confidential data are strictly prohibited in open areas (cafeterias, elevators, public transit). Avoid discussing sensitive topics near audio/video recording devices.
- **Meetings and Presentations:** Before presenting or distributing materials, sensitive data must be redacted or masked for participants without clearance. Documents must prominently display classification labels (e.g., "Confidential", "Highly Confidential"). Online meetings must verify attendee lists, and physical confidential meetings must be held in secured, lockable rooms.
- **Electronic Communications:** Transmitting confidential information via personal email or unencrypted chat apps is strictly forbidden. Approved encrypted channels with verified recipient authentication must be used. Unauthorized screen sharing or recording during online conferences is prohibited.

7. Monitoring and Audit

7.1 Monitoring Rights

The Company reserves the right to monitor and audit all information system usage, including but not limited to: data access, data transfers/sharing, modifications/edits, and file downloads/saves. Monitoring shall be conducted through automated security platforms such as Log Management Systems, Intrusion Detection Systems (IDS), and Data Loss Prevention (DLP) solutions.

7.2 Proactive Monitoring and Threat Detection

The Company maintains proactive monitoring to identify anomalous behavior, including access attempts outside business hours, bulk file downloads over short durations, and unauthorized privilege escalation or access attempts.

8. Policy Violations and Penalties

Employees who violate this Internal Information Management Policy shall be held accountable and subject to disciplinary action under corporate regulations, up to and including termination of employment, as well as legal prosecution where applicable by law.

External parties who breach this policy shall face immediate revocation of data access privileges and may be subject to civil or criminal legal action.

9. Whistleblowing and Reporting

Any individual who detects or suspects an action that violates or fails to comply with this policy is urged to submit a complaint or report immediately in accordance with corporate Whistleblowing procedures. Whistleblowers shall receive full protection; reports and identities shall be treated with strict confidentiality without adverse consequences to their employment or duties, both during and following the investigation.

Mr. Wisudhi Srisuphan

Chairman of the Board