pAI

Policy No.: HR-13 Effective Date: 2025-07-01

Policy Title: Confidentiality & Data Privacy Policy

Revision No.: 1.0

Supersedes: N/A

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Policy Statement
5. Procedures / Guidelines
6. Responsibilities
7. Compliance & Consequences
8. Review & Revision History
9. Purpose

This policy establishes pAI’s commitment to protecting confidential information and ensuring the privacy of personal data. Its purpose is to define the principles and procedures for handling, storing, and transmitting sensitive information, safeguarding intellectual property, maintaining client trust, and ensuring compliance with all applicable data protection laws and regulations.

1. Scope

This policy applies to all pAI employees (full-time, part-time, permanent, temporary), officers, directors, contractors, consultants, and any third parties who have access to pAI’s confidential information or personal data, globally. This includes information in all formats (digital, physical, verbal).

1. Definitions

| **Term** | **Definition** |
| --- | --- |
| **Confidential Information** | Any non-public information related to pAI’s business, including but not limited to, trade secrets, proprietary technology, financial data, customer lists, employee records, business strategies, marketing plans, and unreleased product information. |
| **Personal Data** | Any information relating to an identified or identifiable natural person, such as name, address, email, phone number, employee ID, financial details, health information, or online identifiers. |
| **Data Privacy** | The right of individuals to control how their personal data is collected, used, stored, and shared. |
| **Data Breach** | A security incident where confidential information or personal data is accessed, disclosed, altered, or destroyed without authorization. |
| **Data Controller** | The entity that determines the purposes and means of processing personal data (pAI, in most cases). |
| **Data Subject** | The individual to whom personal data relates (e.g., employees, customers, job applicants). |
| **Processing (of Data)** | Any operation performed on personal data, whether automated or not, such as collection, recording, organization, storage, retrieval, use, disclosure, or destruction. |
| **Need-to-Know Basis** | Access to confidential information or personal data is granted only to individuals whose job responsibilities legitimately require such access. |

1. Policy Statement

4.1 pAI shall protect all confidential information and personal data with the utmost care and in strict compliance with applicable laws and regulations (e.g., GDPR, CCPA, HIPAA).

4.2 All employees and authorized third parties shall treat confidential information as proprietary to pAI and shall not disclose, use, copy, or reproduce it for any unauthorized purpose, either during or after their employment/engagement.

4.3 Personal data shall be collected, processed, and stored only for legitimate business purposes, with transparency, and with respect for the data subjects’ rights.

4.4 Employees are responsible for safeguarding any confidential information or personal data they access, and for reporting any suspected data breaches or privacy incidents immediately.

4.5 Unauthorized access, use, disclosure, alteration, or destruction of confidential information or personal data is strictly prohibited and will result in severe disciplinary action.

1. Procedures / Guidelines

5.1 Handling Confidential Information

5.1.1 Access Control: Access to confidential information shall be restricted to a "need-to-know" basis. Employees shall only access information relevant to their job duties.

5.1.2 Physical Security: Confidential documents and materials must be stored securely (e.g., locked cabinets) when not in use. Desks should be cleared of sensitive information at the end of the workday ("clean desk policy").

5.1.3 Digital Security:

\* Confidential information stored digitally must be on pAI-approved systems and networks.

\* Transmission of confidential information via email or other electronic means must use secure, encrypted channels where appropriate.

\* Employees shall not store confidential information on personal devices (unless explicitly authorized under a BYOD agreement with appropriate security measures, see Policy HR-12).

5.1.4 Disposal: Confidential documents and electronic media containing confidential information must be disposed of securely (e.g., shredding, secure data wiping) when no longer needed.

5.1.5 Non-Disclosure Agreements (NDAs): Employees may be required to sign NDAs as a condition of employment. Third parties accessing pAI confidential information must also sign appropriate NDAs.

5.2 Data Privacy Principles (Personal Data)

5.2.1 Lawfulness, Fairness, and Transparency: Personal data shall be processed lawfully, fairly, and in a transparent manner. Data subjects shall be informed about how their data is used.

5.2.2 Purpose Limitation: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

5.2.3 Data Minimization: Only personal data that is adequate, relevant, and limited to what is necessary for the processing purposes shall be collected.

5.2.4 Accuracy: Personal data shall be accurate and, where necessary, kept up to date.

5.2.5 Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

5.2.6 Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Table 1 – Data Classification and Handling Guidelines

| **Data Classification** | **Description** | **Access Control** | **Handling & Storage** |
| --- | --- | --- | --- |
| **Confidential** | Trade secrets, unreleased product info, financial forecasts, employee salaries, client contracts. | Restricted to "need-to-know" basis; strong authentication required. | Encrypted storage, secure physical locations, limited sharing via secure channels. |
| **Internal Use Only** | Internal reports, organizational charts, internal communications, non-sensitive employee data. | Restricted to pAI employees; general internal access. | Secure internal network drives, pAI-approved cloud services. |
| **Public** | Marketing materials, press releases, public website content, general company information. | No restrictions; freely shareable. | Public servers, company website, social media (as per Policy HR-14). |

5.3 Data Breach and Incident Response

5.3.1 Reporting: Any suspected data breach, loss of confidential information, or privacy incident (e.g., lost laptop, suspicious email, unauthorized access) must be reported immediately to the IT Department and Human Resources.

5.3.2 Investigation: pAI will promptly investigate all reported incidents to determine the scope, cause, and impact.

5.3.3 Response: Appropriate measures will be taken to contain the breach, mitigate harm, notify affected parties (where legally required), and prevent future occurrences.

1. Responsibilities

| **Role** | **Obligation** |
| --- | --- |
| **All Employees** | Understand and comply with this policy. Safeguard confidential information and personal data. Report any suspected breaches or violations immediately. |
| **Managers / Supervisors** | Ensure their teams understand and adhere to this policy. Implement appropriate security measures within their departments. |
| **IT Department** | Implement and maintain technical security measures. Provide secure systems and tools. Respond to security incidents. |
| **Human Resources** | Oversee the privacy of employee personal data. Provide training on data privacy. Collaborate on incident response. |
| **Legal Department** | Provide guidance on data protection laws and regulations. Advise on compliance and breach notification requirements. |
| **Data Protection Officer (if applicable)** | Oversee compliance with data protection laws, advise on data protection impact assessments, and act as a contact point for data subjects and supervisory authorities. |

1. Compliance & Consequences

7.1 Adherence to this Confidentiality & Data Privacy Policy is a mandatory condition of employment or engagement with pAI.

7.2 **Violations:** Any unauthorized access, use, disclosure, alteration, or destruction of confidential information or personal data will be considered a serious violation.

7.3 **Disciplinary Action:** Violations will result in severe disciplinary action, up to and including immediate termination of employment or engagement, regardless of intent.

7.4 **Legal Action:** pAI reserves the right to pursue legal action against individuals who cause harm to the company through breaches of confidentiality or data privacy, and to report such incidents to relevant authorities as required by law.

1. Review & Revision History

| **Version** | **Date** | **Description** | **Author** |
| --- | --- | --- | --- |
| 1.0 | 2025-07-01 | Initial release | HR Director |