AiRTS Pte. Ltd.
60 Cecil Street, ISCA House
Singapore 049709
www.airts.sg
hello@airts.sg

Data Classification & Privacy Policy

Version 1.0

Revision History

Revision No.	Revision Date	Nature of Change	Author
1.0	21 Mar 2025	Initial Document	Jazreel Luar, COO

Signature Block

Task	Name	Signature	Date
Prepared by	**Jazreel Luar, COO**		
Reviewed by	**Jazreel Luar, COO**		
Approved by	**Lem Chin Kok, CEO**		

Table of Contents

1. Purpose

1.1. This policy establishes a structured framework for the identification, classification, and protection of information assets based on their sensitivity, value, and regulatory requirements.

1.2. This policy is intended to ensure that AiRTS data is consistently protected from unauthorized access, disclosure, alteration, and destruction, in accordance with applicable laws, contractual obligations, and industry best practices, thereby supporting the organization's operational integrity, legal compliance, and overall security posture.

2. Scope

2.1. This Policy applies to all data and information assets processed, stored, transmitted, or shared by AiRTS, including data exchanged with vendors, suppliers, and third parties. The scope of this Policy includes, but is not limited to:

a. Client data;

b. Internal business records, including financial information and Human Resources (HR) data;

c. Source code, design documentation, and proprietary algorithms;

d. Publicly released materials, including website content and marketing assets.

2.2. All employees, contractors, vendors, and other authorized third parties are required to handle data in accordance with its designated classification level and to comply with the requirements set forth in this Policy, in conjunction with all other applicable AiRTS policies and procedures.

3. Objectives

3.1. AiRTS shall apply standardized information classification levels (Confidential, Internal, and Public) and implement appropriate handling and protection controls.

3.2. Through such measures, AiRTS ensures the safeguarding of sensitive information, compliance with all applicable laws and regulations, including but not limited to the Personal Data Protection Act (PDPA) and the General Data Protection Regulation (GDPR), and the maintenance of a security framework consistent with recognized industry best practices.

4. Roles & Responsibilities

a. **Chief Executive Officer (CEO):** Ensures that data classification aligns with strategic objectives and compliance requirements.

b. **Chief Operating Officer (COO):** Oversees operational adherence to data handling rules, approves exceptions, and ensures vendor compliance.

c. **Data Protection Officer (DPO):** Ensures compliance with the PDPA by upholding its principles, maintaining the privacy and security of personal data, and addressing data protection matters, such as requests and data breaches, in a timely and compliant manner.

d. **System Administrator:** Advises on technical controls (encryption, access restrictions), monitors compliance, and coordinates with other policies to secure data throughout its lifecycle.

e. **All Personnel (Employees, Contractors, Vendors):** Apply appropriate data classification and handling measures, report any mishandling or suspected breaches promptly.

5. Data Classification

5.1. AiRTS classifies data into three categories: Confidential, Internal and Public.

a. Confidential

  i. Highest sensitivity level.

  ii. Unauthorized disclosure can cause **severe** financial loss, regulatory penalties, reputational damage. (Refer to AiRTS_Risk Management Framework for severity computation)

  iii. Examples: Sensitive client data, proprietary source code, authentication credentials, unreleased financial reports.

b. Internal

  i. Intended for internal use only.

  ii. Unauthorized disclosure causes **moderate** inconvenience or internal inefficiencies.

  iii. Examples: Internal documentation, project plans, non-public policies, test environment configurations.

c. Public

  i. Approved for general public release, **minimal** or no harm if disclosed.

  ii. Examples: Marketing materials, public website content, job postings, press releases.

5.2. The handling requirements for each classification level shall be applied in accordance with the guidelines outlined in the table below.

Classification	Access Control & Authentication	Storage	Transmission	Backup & Recovery	Logging & Monitoring
Confidential	Access is strictly on a Need-To-Know basis, mandatory MFA, access records are to be reviewed quarterly	Encrypt at rest (AES-256), store on AiRTS-approved systems only, not to be stored or processed on BYOD devices	Encrypt in transit (TLS/HTTPS)	Full immutable monthly backups, backup restoration to be tested annually	Log all access and modification
Internal	Role-based access	Authorized AiRTS systems only e.g Microsoft 365, AWS test env	Encrypt in transit (TLS/HTTPS) if transmitted through the Internet	N/A	N/A
Public	Minimal restrictions, standard authentication as needed	Public systems authorized, no special encryption	Open transmission allowed	N/A	N/A

6. Personal Data Protection

6.1. “Personal Data” is data about an individual (“Data Subject”) who can be identified from that data or from that data with other information the organization has or is likely to have access. It may include, but is not limited to, the following:

a. Full name;

b. NRIC number or Foreign Identification Number (FIN);

c. Passport number;

d. Photograph or video image of a Data Subject;

e. Mobile and residential telephone number;

f. Personal email address;

g. Name and residential address; and

h. Biometric information such as fingerprint, Iris image and DNA profile.

6.2. **Personal Data Collection:** AiRTS will only collect personal data in the following circumstances:

a. The personal data is voluntarily provided by the Data Subject or through an authorized representative appointed by the Data Subject, following notification of the purpose and receipt of written consent for the collection and usage of the data; or

b. The collection and use of personal data is permitted or mandated by the PDPA or other applicable laws.

c. Personal data may be collected through the following means:

i. Submission of forms or applications;

ii. Submission of queries, requests, complaints, or feedback;

iii. Interaction with staff via telephone calls, letters, fax, face-to-face meetings, or email;

iv. Capture of images in the form of photographs or videos, including through CCTV cameras within premises or during events;

v. Response to requests for additional personal data; and

vi. Receipt of personal data from business partners, public agencies, employers, or other third parties in connection with the Data Subject's relationship with AiRTS.

6.3. **Purpose Limitation:** Personal data will be collected, used, and disclosed solely for specified, legitimate purposes at the time of collection or as permitted by law. It will not be further processed in a manner incompatible with those purposes, unless consent is obtained or mandated by law.

6.4. **Consent:** AiRTS will obtain consent for the collection, use, and disclosure of personal data and inform Data Subjects of the purposes for which their personal data will be used or disclosed. Consent will also be sought before collecting additional data or using personal data for new purposes, unless authorized by law or directly related to the original purpose.

6.5. **Disclosure:** AiRTS is committed to keeping a Data Subject’s personal data confidential. However, in order to provide the products and services requested and to operate the business effectively, a Data Subject’s personal data may be disclosed to the following:

a. **Service Providers:** AiRTS may share personal data with trusted third-party service providers, such as contractors, consultants, or vendors, who assist in delivering products or services on behalf of AiRTS.

b. **Business Partners:** A Data Subject's personal data may be shared with business partners of AiRTS to help provide products or services that may be of interest to the Data Subject.

c. **Legal or Regulatory Requirements:** AiRTS may disclose personal data to comply with legal obligations, regulations, or lawful requests from government or regulatory bodies.

d. **Professional Advisors:** AiRTS may share personal data with professional advisors, including accountants, legal advisors, or other professionals who provide essential support services to the business.

e. **Business Transactions:** In the event of a sale, merger, or other business transaction, a Data Subject's personal data may be transferred to the new owner or entity.

6.6. AiRTS will ensure that any third parties with whom personal data is shared are obligated to protect the data and use it only for the purposes for which it was disclosed.

6.7. AiRTS shall make the business contact information of the DPO publicly available to ensure that individuals may easily contact the organization regarding personal data protection matters. This contact information shall be published on the company's official website and in relevant privacy notices and communications involving the collection or use of personal data.

6.8. **Accuracy:** Data Subjects shall ensure all personal data submitted to AiRTS is complete, accurate, and up to date. Inaccurate, incomplete or outdated data may impact AiRTS's ability to process requests and/or applications effectively. AiRTS will take reasonable steps to ensure that personal data is accurate, complete, and relevant for the purposes for which it is processed.

6.9. **Access, Correction and Withdrawal:** Data Subjects have the right to submit a request to AiRTS's DPO at any time to:

a. Access to their personal data held by AiRTS;

b. Correct, update, or delete any inaccurate, incomplete or outdated information in their personal data that was previously submitted; and

c. Withdraw their consent at any time, without affecting the legality of any processing conducted before the withdrawal, subject to the legal basis for processing.

6.10. Upon request, AiRTS will assess it in accordance with applicable laws and proceed to update, correct, or delete any personal data as necessary. All requests for access, correction, or withdrawal of consent will be processed within the legally required timeframes. AiRTS will take appropriate action to address any concerns raised by Data Subjects, provided that such requests comply with the relevant legal requirements.

6.11. If personal data has been disclosed to third parties (e.g., data intermediaries or other service providers) with the Data Subject's consent, AiRTS will also inform those third parties of any necessary corrections.

6.12. **Protection:** AiRTS will take reasonable measures to safeguard the personal data it holds or controls by employing a range of technological and physical security measures. These protections are intended to prevent unauthorized access, use, disclosure, alteration, disposal, or loss of personal data.

6.13. **Retention:** Personal data will be retained for as long as necessary to fulfill the purpose(s) for which it was collected, or as required or permitted by applicable laws. AiRTS will stop retaining a Data Subject's personal data or will remove any identifiers that link the data to the Data Subject, once it is determined that the personal data is unsolicited, or that the retention no longer serves the original purpose(s) for which the personal data was collected and is no longer required for legal or business purposes.

6.14. **Destruct, Disposal or Anonymization:** AiRTS will cease the processing of personal data and proceed with its disposal, destruction, or anonymization when the personal data is no longer required for the purposes for which it was collected, has reached the end of its retention period, or is determined to be unsolicited.

6.15. **Transfers of Personal Data Outside of Singapore:** AiRTS generally does not transfer personal data outside of Singapore. However, if such a transfer is necessary, AiRTS will obtain the Data Subject's consent and take appropriate measures to ensure that the Data Subject's personal data remains protected to a standard at least equivalent to that provided under the PDPA. This includes establishing contractual agreements with third parties to whom personal data is transferred, ensuring that reasonable security arrangements are in place to protect the personal data.

7. Data Protection Impact Assessment

7.1. A Data Protection Impact Assessment (DPIA) shall be conducted for any operational functions, business needs and processes that involve personal data (refer to **AiRTS Data Handling & Management Procedure** for details)

7.2. The DPO is responsible for conducting the DPIA, while the CEO oversees the DPIA process to ensure that it aligns with organizational priorities and compliance requirements.

8. Data Inventory Map

8.1. The DPO shall ensure that the Data Inventory Map (DIM) is used and documented to identify the flow of personal data in the possession or under the control of the organization.

8.2. The DIM should contain the following:

a. Type of personal data

b. Purpose for collection

c. Consent status

d. Storage facility and location

e. Retention period and disposal method

f. Usage and disclosure

g. Type of protection

8.3. DPO shall review the DIM on an annual basis or when significant changes to AiRTS's operational environment, regulatory requirements, business objectives, or emerging risks arise.

9. Data Breach

9.1. Any personnel who discover a data breach related to AiRTS shall immediately notify the CISO and DPO.

9.2. AiRTS shall follow the **AiRTS Incident Response Plan** for identifying, reporting, and mitigating the breach, ensuring that the confidentiality, integrity, and availability of such data are protected. All breaches, regardless of severity, will be documented and reviewed to enhance future prevention measures.

9.3. In the event of a data breach involving personal data, AiRTS shall take immediate action to mitigate the breach's impact in accordance with **AiRTS Incident Response Plan**.

9.4. In accordance to Singapore's Personal Data Protection Act, AiRTS shall notify Personal Data Protection Commission (PDPC) within 72 hours if the breach has the potential to cause significant harm to affected individuals, contains sensitive information or when the number of records exceed 500. Information is deemed sensitive if it contains NRIC, financial account information, biometric data, or information about minors or vulnerable individuals.

10. Cloud Shared Responsibility Model

10.1. In the course of its business operations, from time to time, AiRTS may utilize the services of Cloud Service Providers for data storage, processing, and related functions. In the course of its business operations, from time to time, AiRTS may utilize the services of Cloud Service Providers (CSPs) for data storage, processing, and related fuhttps://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html

10.2. https://learn.microsoft.com/en-us/azure/well-architected/

10.3. https://cloud.google.com/architecture/framework

10.4. AiRTS shall review and ensure that appropriate security measures are in place to protect data hosted in the cloud. This includes but is not limited to best practices put out by the CSP such as Microsoft, Amazon, Google.

11. Reporting and Data Requests

11.1. Employees who identify data protection and privacy risks associated with AiRTS shall report them to the CISO. If the risk involves personal data, the CISO shall notify the DPO.

11.2. After the reported risk is assessed in accordance with **AiRTS's Risk Management Framework**, the CISO shall ensure that the ISRC is informed of the risk. Additionally, the CISO shall ensure that data protection and privacy risks, along with relevant mitigation initiatives, are regularly reported to the ISRC to keep them informed of significant developments.

12. Compliance, Audits & Review

12.1. The CISO and DPO shall review this policy annually, or upon significant changes to AiRTS's operational environment, regulatory requirements, business objectives, or emerging risks.

12.2. Lessons learned from incidents, vendor assessments, and changes shall be incorporated into the **Risk Register** to refine classification criteria and controls.

12.3. Any updates to this policy shall be shared with AiRTS's management for approval. Once approved, the CISO or DPO will communicate the updates to all employees.

13. Non-Compliance & Exceptions

13.1. Non-compliance with this policy may result in disciplinary actions, up to and including termination of employment, contract and/or access rights, in accordance with AiRTS policies and applicable laws. Waivers and exceptions to this policy may be requested through the **ISRC** and must be formally documented, including a clear justification and an assigned expiry date (refer to **Risk Management Framework** for details).