POLICY

DATA PROTECTION AND MANAGEMENT

Document No.	AD-GSD-DPM-POL
Document Type	FOR REFERENCE ONLY
Issue	00
Revision	00
Effective Date	04/09/2024

AERODYNE GROUP
Aerodyne Campus,
Persiaran Cyber Point Selatan,
Cyber 8, 63000 Cyberjaya,
Selangor, MALAYSIA
Tel: +603 8310 9200

	POLICY **DATA PROTECTION AND MANAGEMENT**	Document No	AD-GSD-DPM-POL
		Issue	00
		Revision	00
		Effective Date	04/09/2024

DOCUMENT REVIEW & APPROVAL

Prepared by:		Reviewed by:	
Signature:		Signature:	
Designation:	Manager – Intellectual Property & Data Governance	Designation:	Legal Associate
Date	9/3/2024	Date	9/3/2024

Reviewed by:		Reviewed by:	
Signature:		Signature:	
Designation:	Senior Executive, System Engineer	Designation:	Cybersecurity Engineer
Date	9/4/2024	Date	9/4/2024 4th September2024

Approved by:		Approved by:	
Signature:		Signature:	
Designation:	Chief Global Solutions Officer	Designation:	Founder & Group CEO
Date	9/3/2024	Date	9/3/2024

REVISION HISTORY

Issue No.	Rev. No.	Effective Date	Affected Page	Description of Revision
00	00	04/09/2024	All	New Issue

DOCUMENT DISTRIBUTION LIST

The document is distributed subject to the organizational structure of Aerodyne Group.

Copy No.	Dept. / Position	Date
Master	Document Controller Coordinator	04/09/2024
AD-C-07	Global Solution Development Department	04/09/2024

1.0 PURPOSE

This Data Protection and Management ("DPM) Policy outlines the principles and guidelines governing the collection, use, processing, storage, and protection of data that includes personal and sensitive personal data as well as confidential information by **Aerodyne Group** ("AG").

This Policy applies to all employees, subsidiaries, affiliates, contractors, partners, and third parties who handle or have access to personal and sensitive personal data as well as confidential information on behalf of AG. This Policy is to ensure that all data is classified, protected, retained and securely disposed of in accordance with its importance to the organization.

2.0 SCOPE

This Policy applies to all personal and sensitive data, and all AG's confidential information and information systems collected, processed, stored, or transmitted by AG, regardless of the format or medium in which it is stored, including electronic, paper-based, and verbal information.

In addition, this Policy aims to preserve the confidentiality, integrity, and availability of all the information and information assets of AG's business activities both internal and external.

3.0 THE POLICY

3.1 AG classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that data and information are given the appropriate level of protection.

3.2 Data Stewards and Data Custodians are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

3.3 Information systems and applications shall be classified according to the highest classification of data that will be stored or processed.

3.4 The key Policy statements are as follows:

a. Privacy & Confidentiality:

We are dedicated to protecting the privacy and confidentiality of all personal and sensitive data, ensuring compliance with all relevant laws and regulations.

b. Data Security Commitment:

We employ security measures, including encryption and access controls, to safeguard data from unauthorized access, alteration, or loss.

c. Data Accuracy & Integrity Commitment:

We strive to maintain accurate and complete data, with processes in place to allow updates and corrections as needed.

d. Responsible Data Retention & Disposal Commitment:

We retain data only as long as necessary and use secure methods to dispose of data that is no longer required.

e. Data Breach Preparedness Commitment:

We are committed to provide a data breach response plan to address incidents transparently, including notifying affected individuals and authorities when necessary.

f. Data Access & User Rights Commitment:

We respect individuals' rights to access, correct, and control their personal data, providing clear and accessible procedures for these requests.

g. Compliance & Continuous Improvement:

We regularly review and update our data protection policies to stay compliant with legal requirements and industry standards, supported by internal and external audits.

Contact Information

For questions, concerns, or requests relating to data protection, data subjects may contact the Data Protection Officer at dpo.aerodyne@aerodyne.group.

4.0 REFERENCES

Statutes, Laws, Regulations

a. Personal Data Protection Act 2010, Malaysia (PDPA).

b. General Data Protection Regulations, European Union (GDPR).

5.0 GLOSSARY OF TERMS

5.1 "Confidential Information" means any information or data of a confidential nature, including oral and visual information or data, information or data recorded in writing or in any other medium or by any other method, and any other information and data which is either owned by or related to AG or made available to AG by other parties or companies under obligation, whether contractual or otherwise, which includes but not limited to:

a. communication and all information containing or consisting of material of a commercial, financial, technical, operational or other information directly or indirectly relating to the past, present or future operations of affairs relating to commercial transactions including but not limited to all business plans, strategies, analysis, all information relating to clients, customers and suppliers, trade secrets, discoveries, ideas, concepts, designs, devices, drawings, materials, specifications, techniques, models, data, documents, processes, procedures, "know-how", improvements, budgets, projections, forecasts, marketing and development plans, and financial and accounting;

b. all information relating to investment opportunities or other circumstance that is the subject of a commercial transaction;

c. all notes, summaries, extracts, compilations, analyses, calculations, models, conclusions, opinions or other information made or derived in whole or in part;

d. non-public information;

e. proprietary or is reasonably understood and expected to be confidential;

f. any information directly or indirectly related to commercial transactions concerning the contacts, contracting party(ies), clients, networks, partners and agents;

g. any information directly or indirectly related to commercial transactions pertaining to all business activities of AG or other parties or companies made available to AG which are classified as confidential and secret which include, but not limited to, certain projects and contracts which AG or other parties or companies are involved in, pursuing or existing regardless of whether directly or indirectly related to commercial transactions; or

h. any information marked “Confidential Information” made available by AG or by other parties or companies to AG.

5.2 “Executive Management Committee or EMC” means the highest level of authority and has the final decision-making and accountable for completion for specific levels of DPM.

5.3 “GSD” means the Global Solutions Development Department.

5.4 “Data” means information that includes but not limited to Personal Data, Sensitive Personal Data, Confidential Information received, prepared, managed, used, or retained by a department or employee of AG or a data user relating to the activities or operations of AG including personally identifiable information (PII).

5.5 “Data Confidentiality” means the protection of data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information.

5.6 “Data Integrity” means the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

5.7 “Data Availability” means the property that data or information is accessible and usable upon demand either by a Data Controller or required to be disclosed by law and/or by an order of a court of competent jurisdiction.

5.8 “Data Custodian” means the person responsible for the technical environment (e.g. database or system). The Data Custodian and Steward may be the same person.

5.9 “Data Steward” means the person with day-to-day management responsibility of individual databases, datasets, or information systems. In general, a data steward has business knowledge of the data and can answer questions about the data itself.

5.10 “Data Controller” means employee, contractor, or other individual affiliated with AG who is eligible and authorized to collect, access and/or use the data. A dataset may have more than one user group.

5.11 “Data Classification” means categorization of data assets based on their sensitivity, confidentiality, and criticality. Data classification’s primary purpose is to label or tag data to indicate how it should be handled, accessed, and protected based on its classification level.

5.12 “Data Breach” means any external act or internal act or omission that results in Information and/or Personal Data being disclosed incorrectly or unlawfully; altered, destroyed, or made otherwise unavailable.

5.13 “Data Subject” means a natural living person whose personal data is processed by AG.

5.14 “Data / Information Asset” refers to a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

5.15 “Personal data” means any information that directly or indirectly relates to an identified or identifiable natural living individual.

5.16 “Processing” means any operation or set of operations which is performed on data, including personal data (collecting, storing, amending, sharing, deleting, etc.).

5.17 “Record” means information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

5.18 “Records Management” means controlling records within a comprehensive regime made up of policies, procedures, systems, processes and behaviours. Together they ensure that

reliable evidence of actions and decisions is kept and remains available for reference and use when needed.

5.19 "Sensitive Personal Data" means personal data which requires more protection because it is sensitive e.g. racial or ethnic origin, religious or philosophical beliefs, biometric, and health.

6.0 DATA CLASSIFICATION

6.1 Table below contains descriptions of each data classification and its associated potential adverse impact.

Data Class	Description	Potential Impact
Level 4: Restricted / Protected	Data that triggers requirement for notification to affected parties in case of a security breach. Highly sensitive information such as personal data, financial information, customer data, salary data and proprietary data must be store at company NAS (Network Attached Storage) outlined based on the AG's Information Technology (IT) Policy.	Moderate - High
Level 3: Sensitive / Confidential	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.	Low - Moderate
Level 2: Internal Use	Data that is normal operating information, but is not proactively released to the public. Viewing and use is intended for employees, and it could be made available group wide or to specific employees in a department, division or business unit. Certain data may be made available to external parties upon their request.	Low
Level 1: Public	Data available for public access or release.	None - Low

7.0 DATA PROTECTION PRINCIPLES

AG is committed to upholding the following principles in relation to the processing and management of personal and sensitive data:

7.1 Lawfulness, Fairness, and Transparency:

Personal and sensitive data shall be processed lawfully, fairly, and transparently in accordance with applicable data protection laws and regulations.

7.2 Purpose Limitation:

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

7.3 Data Minimization:

AG shall only collect and process personal and sensitive data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

7.4 Accuracy:

AG shall take reasonable steps to ensure that personal and sensitive data is accurate, up-to-date, and relevant for the purposes for which it is processed.

7.5 Storage Limitation:

Personal and sensitive 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 data is processed.

7.6 Integrity and Confidentiality:

AG shall implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal and sensitive data.

7.7 Accountability:

AG shall be responsible for demonstrating compliance with data protection laws and regulations, and shall implement measures to ensure ongoing compliance.

8.0 OBLIGATIONS

Anyone who processes data and personal data within or on behalf of AG shall comply with the principles of data protection. This means that you are required to acquaint yourself with this Aerodyne's DPM Policy, the related guidance, and to complete any related training from time to time.

9.0 GENERAL EMPLOYEE GUIDELINES

Data Protection Responsibilities

9.1 All employees are responsible for protecting the integrity, confidentiality, and availability of data within AG. This includes, but is not limited to, the following:

9.1.1 Confidentiality: Ensure that sensitive and confidential information is accessed only by authorized personnel.

9.1.2 Integrity: Protect data from unauthorized modification or corruption.

9.1.3 Availability: Ensure that data is accessible to authorized users when needed.

Access Control

9.2 All employees are responsible for applying access control as outlined in AG's Information Technology (IT) Policy as follows:

9.2.1 Authorized Access: Only access data for which explicit authorization and a legitimate need have been duly obtained.

9.2.2 Unique Credentials: Using unique user credentials to access data and never to share login information with others, except for duly authorized and legitimate access.

9.2.3 Secure Passwords: Create strong, unique passwords and change them regularly in accordance with the organization's password policy.

Data Handling

9.3 All employees are required to observe the following for data in use:

9.3.1 Data Storage: Store data securely using approved storage solutions and avoid saving sensitive information on local devices or unauthorized cloud services.

9.3.2 Data Transmission: Use of encryption methods for transmitting sensitive data over networks. Avoid using unsecured communication channels such as personal email for sensitive data.

9.3.3 Data Disposal: Dispose of data securely when it is no longer needed, following the AG's data retention and disposal policies as outlines in AG's IT Policy.

Physical Security

9.4 All employees are required to observe the following:

9.4.1 Device Protection: Securely lock computer and mobile devices when unattended. Keep devices in secure locations.

9.4.2 Workspace Security: Ensure that sensitive information is not left in open or unattended areas. Use secure storage for physical documents.

9.4.3 Access to Restricted Areas: Only authorised employees are allowed to access restricted areas as will be defined time to time, such as but not limited to server rooms. If not authorised, such employee requires approval and be escorted by an authorised employee.

Incident Reporting

9.5 All employees are required to observe the following:

9.5.1 Immediate Reporting: Report any suspected data breaches, security incidents, or unauthorized access immediately to the IT department or designated security team via Aerodyne Helpdesk (https://internal-helpdesk.aerodyne.group/).

9.5.2 Cooperation: Cooperate fully with any investigations related to data protection and security incidents.

Use of Organization Resources

9.6 All employees are required to observe the following:

9.6.1 Authorized Use: Use organizational resources, including data, systems, and networks as authorized, for legitimate AG's business purposes only.

9.6.2 Prohibited Activities: Not to engage in activities that compromise data security, such as installing unauthorized software, bypassing security controls, or engaging in illegal and unlawful activities.

Compliance and Accountability

9.7 All employees are required to observe the following:

9.7.1 Policy Adherence: Adhere to all AG's organizational policies and procedures related to data protection and management.

9.7.2 Accountability: Non-compliance with these guidelines may result in disciplinary action, including termination of employment and potential legal consequences.

10.0 ROLES AND RESPONSIBILITIES

10.1 Data Governance Council shall:

10.1.1 be the body vested with authority for deliberating and making decisions on data protection and management policies, guidelines, data security and access control matters, data retention and disposal, and regulatory compliance.

10.2 Data Stewards shall:

10.2.1 as set out in requirements of this DPM Policy, determine the appropriate classification of the data generated by the department according to this DPM Policy, in consultation with personnel appointed as cybersecurity officer or liaison, data custodian, data privacy or protection officer, data governance officer, legal counsel, risk management and/or other appointed personnel as needed and/or necessary;

10.2.2 review and/or modify the classification of the data as set out in this DPM Policy;

10.2.3 ensure communication of the data classification when the data is released or provided to another party or entity; and

10.2.4 ensure that appropriate privacy and security controls are implemented with respect to the data classification.

10.3 Cybersecurity Officers or Liaisons shall:

10.3.1 advise on acceptable levels of risk and the appropriate level of security controls for information systems in accordance with this DPM Policy and Cybersecurity Policy.

10.4 Data Governance Officer shall:

10.4.1 adequately support Data Stewards to classify data and adhere to this DPM Policy and implementation of requirements and standards.

10.5 Data Custodians shall:

10.5.1 adequately support their department's Data Stewards and Cybersecurity Officer or Liaison in conducting their roles and responsibilities in this DPM Policy.

10.6 Cloud and Infra Officer shall:

10.6.1 adequately support departments in their efforts to classify data and adhere to the Cybersecurity Policy and implementation of requirements and standards.

10.7 Data Controllers shall:

10.7.1 obtain permission to collect, access or use data from the Data Steward or their designee (this includes pre-set permissions based on job assignment);

10.7.2 comply with the handling and security requirements specified by their department's Cybersecurity Officer or Liaison or their designee; and

10.7.3 be familiar with Federal, state and local confidentiality or privacy laws pertaining to the data they collect, access, use, or maintain in conducting their work.

11.0 DATA STORAGE

11.1 This section is to establish guidelines for the secure storage of data within AG to ensure the protection of data integrity, confidentiality, and availability. This applies to including but not limited to digital data, physical documents, and backups:

11.1.1 Data Classification and Storage Requirements

Data Class	Storage Requirements
Level 4: Restricted / Protected	Stored in highly secure, encrypted systems with strict access controls. Physical copies must be stored in secure, access-controlled environments.
Level 3: Sensitive / Confidential	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Level 2: Internal Use	Stored in secure systems accessible only to authorized personnel.
Level 1: Public	May be stored in publicly accessible systems with minimal security controls.

11.1.2 Digital Data Storage Requirements:

Process	Requirements
Encryption	All sensitive and confidential data must be encrypted both at rest and in transit using industry-standard encryption methods outlined based on AG's Information Technology (IT) Policy.
Access Control	Only authorized personnel with a legitimate need should have access outlined based on AG's Information Technology (IT) Policy. Access to stored data must be restricted based on the principle of least privilege. Need to know basis.
Backup and Recovery	Regular backups must be performed to ensure data can be recovered in case of loss or corruption. Backup data must be stored securely and protected with the same level of security as the original data.
Cloud Storage	Use only approved cloud storage services that comply with the organization's security and compliance requirements. Ensure cloud storage providers implement robust security measures, including encryption and access control outlined based on AG's Information Technology (IT) Policy.

11.1.3 Physical Data Storage Requirements:

Secure Storage Facilities	Physical documents and storage media containing sensitive information must be stored in secured facilities with restricted access.
Document Handling	Sensitive documents must be handled with care and stored in locked cabinets or secure rooms when not in use.

11.1.4 Storage Data Retention and Disposal Requirements:

Disposal of Physical Media	Physical documents and storage media no longer needed must be disposed of securely using shredding or other approved methods to prevent unauthorized access.
Retention	Data must be retained only for as long as necessary to fulfil its intended purpose and in accordance with legal, regulatory, and business requirements.
Secure Disposal	Data that is no longer needed must be disposed of securely. Digital data should be deleted using methods that prevent recovery, and physical media should be destroyed or rendered unreadable.

12.0 DATA INTEGRITY

12.1 This section is to establish guidelines and procedures to ensure the accuracy, consistency, and reliability of data within AG. Maintaining data integrity is critical for making informed decisions and supporting organizational operations. This section applies to all data collected, stored, processed, and transmitted by AG, including digital and physical formats:

Data Integrity Principles	Accuracy	Data must be accurate and free from errors.
	Consistency	Data must be consistent across different systems and over time.
	Reliability	Data must be reliable and maintain its intended purpose and integrity.
Data Collection and Entry	Validation and Verification	Implement validation checks to ensure data accuracy at the point of entry. Verification processes must be in place to cross-check data from multiple sources for consistency and accuracy.
	Standardized Procedures	Use standardized data entry procedures to minimize errors and ensure consistency.
Data Storage and Maintenance	Regular Audits	Conduct regular data audits to identify and correct inaccuracies, inconsistencies, and anomalies. Document and address any issues identified during audits.

	Data Synchronization	Ensure that data is consistently updated across all systems and databases. Implement synchronization mechanisms to maintain consistency between different data sources.
Data Processing	Controlled Access	Restrict data processing to authorized personnel with a legitimate need. Ensure that data processing activities are logged and monitored for any unauthorized changes.
	Change Management	Implement a change management process to control modifications to data and ensure changes are documented, reviewed, and approved. Maintain an audit trail of all changes to critical data.
Data Backup and Recovery	Regular Backups	Perform regular backups of critical data to prevent loss and ensure data can be restored in case of corruption or loss.
	Data Integrity Checks	Implement integrity checks for backup data to ensure it is complete and uncorrupted. Test backup and recovery procedures regularly to verify their effectiveness.

13.0 DATA COLLECTION AND USE

13.1 AG shall only collect personal and sensitive data for specified, explicit, and legitimate purposes, and shall inform data subjects of the purposes for which their data is being collected.

13.2 Personal and sensitive data shall only be processed with the consent of the data subject, or where permitted by law for the performance of a contract, compliance with a legal obligation, protection of vital interests, or legitimate interests pursued by AG.

13.3 AG shall not use personal and sensitive data for purposes other than those for which it was collected, unless the data subject has provided explicit consent for such use or where permitted by law.

13.4 Data Classification

This DPM Policy identifies the following classes of data:

Data Class	Description	Examples
Level 4: Restricted / Protected	Stored in highly secure, encrypted systems with strict access controls. Physical copies must be stored in secure, access-controlled environments.	• Internal policies • Legal documents • Meeting minutes and internal presentations • Contracts • Internal reports • Email
Level 3: Sensitive / Confidential	Highly sensitive data requiring high levels of protection, and access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or an authorised personnel.	• Customer Data • Personally identifiable information (PII) • Company financial and banking data • Salary, compensation and payroll information • Strategic plans • Incident reports • Risk assessment reports • Technical vulnerability reports • Authentication credentials • Secrets and private keys • Source code • Litigation data
Level 2: Internal Use	Data that is normal operating information, but is not proactively released to the public. Viewing and use is intended for employees, and it could be made available group wide or to specific employees in a department, division or business unit. Certain data may be made available to external parties upon their request.	• Company catalogs • Employee handbooks • Business materials • Email messages
Level 1: Public	Documents intended for public consumption which can be freely distributed outside AG.	• Marketing materials • Product descriptions • Release notes • External facing policies • Company's newsletters

13.5 Labelling

All physical and digital assets of AG must be labelled in accordance with this DPM Policy's data management standards. Labels should include appropriate classification, ownership, and access control information to ensure proper handling, storage, and security. This policy applies to all data, including documents, files, and storage media.

13.6 Data Handling

The following are requirements for handling public data, confidential data and restricted data:

Process	Description
Public Data Handling	Public data does not require special protection or handling controls. It may be freely distributed, provided it remains accurate and unaltered. Ensure access is monitored and usage complies with AG's policies.
Confidential Data Handling	Confidential data is subject to the following protection and handling requirements: • Access for non-preapproved roles requires documented approval from the data owner. • Access is restricted to specific employees, roles and/or departments. • Confidential systems shall not allow unauthenticated or anonymous access. • Confidential Customer Data shall not be used or stored in non-production systems/environments. • Confidential data shall be encrypted at rest and in transit over public networks in accordance with the Cryptography Policy outlined based AG's Information Technology (IT) Policy. • Mobile device hard drives containing confidential data, including laptops, shall be encrypted. • Mobile devices storing or accessing confidential data shall be protected by a log-on password (or equivalent, such as biometric) or passcode and shall be configured to lock the screen after five (5) minutes of non-use • Backups shall be encrypted. Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's. • Paper records shall be labeled "confidential" and securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures. • Hardcopy paper records shall only be created based on a business need and shall be avoided whenever possible. • Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed. • Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner.
Restricted Data Handling	Restricted data is subject to the following protection and handling requirements: • Access is restricted to users with a need-to-know based on business requirements.

	• Restricted systems shall not allow unauthenticated or anonymous access. • Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner. • Paper records shall be securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures. • Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed.

14.0 DATA SECURITY

14.1 Data Governance Council shall implement appropriate technical and organizational measures to ensure the security of personal and sensitive data, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

14.2 Access to personal and sensitive data shall be restricted to authorized personnel on a need-to-know basis, and access controls shall be implemented to prevent unauthorized access, use, or disclosure.

14.3 Data Governance Council shall regularly review and update its security measures to address emerging threats and vulnerabilities, and shall provide training to employees on data protection best practices.

15.0 DATA RETENTION AND DISPOSAL

15.1 Personal and sensitive data shall be retained only for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable law or regulation.

15.2 Data Governance Council shall establish retention periods for different categories of data, taking into account legal, regulatory, and business requirements, and shall securely dispose of data that is no longer necessary for the purposes for which it was collected.

15.3 Data Retention

15.3.1 AG shall retain data as long as there is a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data.

15.3.2 Sensitive Personally Identifiable Information (SPII) and Personally identifiable information (PII) shall be deleted or de-identified as soon as it no longer has a business use.

15.3.3 Retention periods shall be documented in the Data Retention Matrix in Appendix B to this policy.

15.4 Data & Device Disposal

15.4.1 Data classified as restricted or confidential shall be securely deleted when no longer needed. Data Governance Council shall assess the data and disposal practices of third-party vendors in accordance with the third-party management policy. Only third-parties who meet AG's requirements for secure data disposal shall be used for storage and processing of restricted or confidential data.

15.4.2 Data Governance Council shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of, disposal.

14.4.3 Confidential and Restricted hardcopy materials shall be shredded or otherwise disposed of using a secure method.

15.4.4 Sensitive Personally Identifiable Information (SPII) and Personally identifiable information (PII) shall be collected, used and retained only for as long as the company has a legitimate business purpose. SPII and PII shall be securely deleted and disposed of following contract termination in accordance with company policy, contractual commitments and all relevant laws and regulations. SPII and PII shall also be deleted in response to a verified request from a consumer or data subject, where the company does not have a legitimate business interest or other legal obligation to retain the data.

16.0 DATA SUBJECT RIGHTS

16.1 AG shall respect the rights of data subjects in relation to their personal and sensitive data, including the right to access, rectify, erase, restrict processing, object processing and portability.

16.2 Data subjects shall be provided with clear and accessible information about their rights and how they can exercise them, and AG shall respond promptly to requests from data subjects to exercise their rights.

17.0 DATA BREACH RESPONSE

17.1 Data Governance Council shall establish procedures for detecting, assessing, and responding to data breaches in accordance with applicable data protection laws and regulations.

17.2 In the event of a data breach, Data Protection Officer shall promptly notify affected data subjects and relevant regulatory authorities, and shall take appropriate remedial action to mitigate the impact of the breach and prevent recurrence.

18.0 THIRD-PARTY DATA PROCESSING

18.1 Where AG engages third parties to process personal or sensitive data on its behalf, such as cloud service providers or data processors, appropriate contractual safeguards shall be implemented to ensure that the third party provides sufficient guarantees regarding the security and protection of the data.

19.0 COMPLIANCE MONITORING AND REVIEW

19.1 Data Governance Council shall regularly monitor and review its data protection practices to ensure compliance with this Policy and applicable data protection laws and regulations.

19.2 Compliance with this DPM Policy shall be subject to regular audits and assessments, and any identified non-compliance shall be addressed promptly through corrective actions and training.

19.3 Executive Management Committee shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this DPM Policy.

19.4 Under certain circumstances, should AG become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by AG's legal counsel, such records and information are exempt from any other requirements specified within this DPM Policy and are to be retained in accordance with requirements identified by

the legal counsel. All such holds and special retention requirements are subject to annual review with AG's legal counsel to evaluate continuing requirements and scope.

19.5 Data Governance Council will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits.

19.6 Requests for an exception to this policy must be submitted to the Data Protection / Governance Officer (DPO) for approval.

19.7 This Policy shall be reviewed and updated periodically to reflect changes in business practices, technology, and regulatory requirements. Any updates to this Policy shall be communicated to all relevant stakeholders, and employees shall be required to acknowledge their understanding and compliance with the updated Policy.

20.0 GOVERNANCE AND ACCOUNTABILITY

20.1 AG's Data Protection Officer (DPO) shall be responsible for overseeing compliance with this Policy and applicable data protection laws and regulations.

20.2 The DPO shall have the authority to investigate complaints and incidents related to data protection, and to recommend corrective actions and disciplinary measures where necessary.

21.0 ENFORCEMENT

Violations & Enforcement

Any known violations of this policy should be reported to the DPO. Violations of this policy shall result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

APPENDIX A

Internal Retention and Disposal Procedure

AG's Data Stewards / Data Custodians are responsible for setting and enforcing the data retention and disposal procedures for AG managed accounts and devices.

Customer Accounts:

1. Customer accounts and data shall be deleted within 6 years of contract termination through manual data deletion processes.

Devices:

1. Employee devices will be collected promptly upon an employee's termination. Remote employees will be sent a shipping label and the return of their device shall be monitored.
2. Collected devices will be cleared to be re-provisioned or removed from inventory. AG will securely erase the device when reprovisioning.
3. Device images may be retained at the discretion of management for business purposes

Destroying devices or electronic media

In cases where a device is damaged in a way that AG cannot access the Recovery Partition to erase the drive, AG may optionally decide to use an E-Waste service that includes data destruction with a certificate. AG will keep certificates of destruction on record for one year. Physical destruction can be optional if it is verified that the device is encrypted with Full Disk Encryption, which would negate the risk of data recovery.

Management will review this procedure at least quarterly.

APPENDIX B

Data Retention Matrix

System or Application	Data Description	Retention Period
Aerodyne Group SaaS Products (AWS)	Customer Data	Up to 6 years after contract termination
Aerodyne Group AutoSupport	Customer instance and metadata, debugging data	Subjected to this DPM Policy
Aerodyne Group Customer Support Tickets	Support Tickets and Cases	Subjected to this DPM Policy
Aerodyne Group Customer Support Phone Conversations	Support Phone Conversations	Subjected to this DPM Policy
Aerodyne Group Security Event Data	Security and system event and log data, network data flow logs	On-Premise - Indefinite AWS Instance - 1 year
Aerodyne Group Vulnerability Scan Data	Vulnerability scan results and detection data	6 months - host (asset) data is retained until removed and purged from Qualys
Aerodyne Group Customer Sales	Opportunity and Sales Data	Subjected to this DPM Policy
Aerodyne Group QA and Testing Data	QA, testing scenarios and results data	Subjected to this DPM Policy
Security Policies	Security Policies	1 year after archive
Temporary Files	AWS /tmp ephemeral storage	Automatically when process finishes

APPENDIX C

Responsibility Assignment (RACI) Matrix

Deliverable or Task	Threshold	Roles	EMC	GCEO	Data Governance Council	Data Protection Officer (DPO)	Cybersecurity	Cloud & Infra	Product Team	Operations	Legal Team	Project Delivery & Quality	Business Development	IP & Data Governance	Data Stewards / Custodian	Remarks
Data Governance Compliance Requirements																
Policy, notice, manual, procedures and guidelines, as well as all related policies such as data management, risk management, data breach impact mitigation (including PDPA, GDPR and relevant	Policy		A	I	C	C	C	C	C	C	C	C	C	R	R	
	Procedures & Guidelines		I	I	A	C		C		C		C		R	R	
Data Management (including database, data assets, master data, data architecture, metadata, data classification, data quality)			I	I	A	C		C	C	C		C		R	R	
Data Security and Access Control			C	I	A	I	R	C					C	R	R	
Data Retention and Disposal			C	I	A	I	C	C		C		C	C	R	R	
Risks, Incidents and Data Breach, as well as Remediation			C	I	C	A	R	R		C	C		C	R	R	
Notification of Data Breach			C	I	C	A	R	R		C	C		C	R	R	
Regulatory Compliance			C	I	A	C	C	C		C	C			R	R	
Training and Awareness Programs			C	I	A	C	C							R	R	
Internal Data Governance Auditting			C	I	A	C	C							R	R	

*__Data Stewards__: Focal persons who is responsible for ensuring the quality and fitness for purpose of the organization's data assets, including the metadata for those data assets.

R
A
C
I

Responsible : Assigned to complete the task or deliverable.
Accountable : Has final decision-making authority and accountability for completio
Consulted : A stakeholder, or adviser who is consulted before decision or action.
Informed : Must be informed after a decision or action.