INFORMATION SECURITY AND PERSONAL DATA PROTECTION, PROCESSING POLICY

AIRCLOSET ENGINEERING COMPANY LIMITED

Address: 10th Floor, Vietnam 3D Innovation Center Building, No. 3 Duy Tan Street, Dich Vong Hau Ward, Cau Giay District, Hanoi City, Vietnam.

(Issued under Decision No. [DECISION NO.] dated [DAY] [MONTH] [YEAR])

PART I: GENERAL PROVISIONS ON DATA PROTECTION AND PROCESSING

Article 1: Purpose [1]This Personal Data Protection and Processing Policy ("Policy") stipulates the terms and conditions for the Protection and Processing of personal data by AIRCLOSET ENGINEERING COMPANY LIMITED based on compliance with Decree 13/2023/ND-CP dated April 17, 2023, on personal data protection and other relevant current legal regulations. [2]

Article 2: Scope and Subjects of Application [3]

1. **Scope:** Applies to all business operations, information systems, internal networks, and Information Assets owned or managed by the Company.
2. Subjects:

a) All Officers and Employees of AIRCLOSET ENGINEERING COMPANY LIMITED. 4b) Personal Data Providers (applicants, employees, collaborators, interns, apprentices, partners in projects involving personnel performing work...). 5c) Personal Data Subjects. 6d) In this Policy, AIRCLOSET ENGINEERING COMPANY LIMITED is the Data Controller and Processor. 7

Article 3: Governing Legal Documents [8]Civil Code 2015 [9], Cyber Security Law 2018 [10], Law on Cyber Information Security 2015 [11], and Decree 13/2023/ND-CP dated April 17, 2023, on personal data protection[12].

Article 4: Definitions [13]

1. **Personal Data (Data):** Information in the form of symbols, writing, numbers, images, sounds, or the like in the electronic environment attached to or helping to identify a specific person. [14]Personal data includes basic personal data and sensitive personal data. [15]
2. **Basic Personal Data:** Includes: Full name, middle name, and given name, other names (if any); Date of birth; date of death or disappearance; Gender; Place of birth,

place of birth registration, place of permanent residence, place of temporary residence, current residence, hometown, contact address; Nationality; Individual's image; Phone number, ID card number, personal identification number, passport number, driver's license number, vehicle license plate number, personal tax code number, social insurance number, health insurance card number; Marital status; Information about family relationships (parents, children); Information about an individual's digital account; personal data reflecting activity, activity history in cyberspace; Other information associated with a specific person or helping to identify a specific person that is not sensitive personal data. [16]

3. **Sensitive Personal Data:** Is personal data closely associated with an individual's privacy that, if violated, directly affects the legal rights and interests of the individual, including: Political views, religious views; Health status and private life recorded in medical records, excluding blood type information; Information related to racial origin, ethnic origin; Information about genetic characteristics inherited or acquired by the individual; Information about physical attributes, unique biological characteristics of the individual; Information about the individual's sexual life, sexual orientation; Data on crime, criminal acts collected, stored by law enforcement agencies; Customer information of credit institutions, foreign bank branches, payment intermediary service providers, and other permitted organizations; Data on an individual's location determined through positioning services; Other personal data specified by law as unique and requiring necessary security measures. [17]

4. **Personal Data Protection:** Is the activity of preventing, detecting, stopping, and handling violations related to personal data as prescribed by law. [18]

5. **Personal Data Processing:** Is one or more activities impacting personal data, such as: collection, recording, analysis, confirmation, storage, modification, disclosure, combination, access, retrieval, recovery, encryption, decryption, copying, sharing, transmission, provision, transfer, deletion, destruction of personal data or other related actions. [19]

6. **Personal Data Recipient:** Is AIRCLOSET ENGINEERING COMPANY LIMITED and/or a party authorized by AIRCLOSET ENGINEERING COMPANY LIMITED for the purpose of carrying out personal data protection and processing activities as prescribed by law. [20]

7. **Personal Data Provider:** Is an individual or organization that provides personal data to the Personal Data Recipient. [21]

8. **Personal Data Controller and Processor:** Is AIRCLOSET ENGINEERING COMPANY LIMITED which simultaneously determines the purpose, means, and directly processes personal data. [22]

9. **Data Subject:** Is the individual reflected by the personal data. [23]

10. **Data Subject's Consent:** Is the explicit, voluntary expression confirming the allowance for processing the data subject's personal data. [24]

11. **Transfer of Personal Data Abroad:** Is the activity of using cyberspace, electronic equipment, means, or other forms to transfer personal data of Vietnamese citizens to a location outside the territory of the Socialist Republic of Vietnam or using a location outside the territory of the Socialist Republic of Vietnam to process personal data of Vietnamese citizens, including: (a) Organizations, businesses, individuals transferring personal data of Vietnamese citizens to foreign organizations, businesses, management departments for processing consistent with the purpose agreed by the data subject; (b) Processing personal data of Vietnamese citizens using automated systems located outside the territory of the Socialist Republic of Vietnam by the Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor consistent with the purpose agreed by the data subject. [25]

12. **Third Party:** Is an individual or organization other than the Personal Data Recipient and Personal Data Provider permitted to Process Personal Data under current Vietnamese law, including but not limited to (a) The parent company of AIRCLOSET ENGINEERING COMPANY LIMITED ("Parent Company"), Parent Company's contractors, representatives, (b) Auditors, legal/tax/accounting/insurance/medical consultants... of AIRCLOSET ENGINEERING COMPANY LIMITED or its partners providing services to AIRCLOSET ENGINEERING COMPANY LIMITED or the Parent Company, (c) Accounting software service providers and those performing maintenance, upgrade, warranty of such software; (d) Competent State Agencies of Vietnam; (e) Any partner cooperating with AIRCLOSET ENGINEERING COMPANY LIMITED to provide products/services within AIRCLOSET ENGINEERING COMPANY LIMITED's business scope; and (f) Any other third party lawful or required by law, order of a competent state agency or by a competent court, international arbitration center, or request from the Government, or requested by internal policies compliant with current Vietnamese law of the Parent Company or AIRCLOSET ENGINEERING COMPANY LIMITED to serve the Personal Data Processing purpose stated in this Policy. [26]

13. **Party Transferring Data Abroad:** Includes the Personal Data Controller and Processor, Personal Data Controller (if any), Personal Data Processor (if any), Third party (if any). [27]

Article 5: Principles of Personal Data Protection and Processing [28]

1. Personal data shall be processed as prescribed by law. [29]
2. The data subject shall be informed about the personal data processing activities related to them, unless otherwise prescribed by law. [30]
3. Personal data shall only be processed in accordance with the purpose announced/declared by the Personal Data Controller and Processor regarding personal data processing. [31]
4. Collected personal data must be relevant and limited in scope to the purpose of processing. [32]Personal data shall not be bought or sold in any form, unless otherwise prescribed by law. [33]
5. Personal data shall be updated and supplemented in accordance with the purpose of processing. [34]
6. Personal data shall be subject to protection and security measures during processing, including protection against violations of personal data protection regulations and prevention of loss, destruction, or damage due to incidents, using technical measures. [35]
7. Personal data shall only be stored for a period appropriate to the purpose of data processing, unless otherwise prescribed by law. [36]
8. The Data Controller, Personal Data Controller and Processor shall be responsible for complying with the data processing principles prescribed in current legal documents and this Policy and demonstrating their compliance with those data processing principles. [37]

PART II: GENERAL INFORMATION SECURITY RULES

Article 6: Information Asset Management [38]

1. **Classification and Assignment of Ownership:**

- All Information Assets must be classified according to their sensitivity and value to the Company. [39]The minimum classification levels include: Public, Internal, Confidential/Strictly Confidential. [40]
- Each Information Asset must be assigned an Owner responsible for the integrity, security, and availability of that asset, while ensuring the asset is protected according to its classification. [41]

2. **Rules for Device Usage:**
    - Devices provided by the Company shall only be used for work purposes. [42]
    - Employees are not permitted to interfere with or change the basic security configurations set by the IT Department. [43]
    - Employees are only permitted to install and use licensed and approved software. [44]
    - The installation of any unauthorized software or P2P applications is strictly prohibited. [45]
3. **Protection of Mobile Devices and Remote Work:**
    - All mobile devices (laptops, phones) used to access the Company's network or process data must have **Disk Encryption** installed. [46]
    - Remote employees must ensure a safe home working environment, use a secure network connection, and comply with the Company's VPN regulations when accessing systems. [47]
    - Storing Confidential/Strictly Confidential Company data on personal devices or unauthorized personal cloud storage services is strictly prohibited. [48]
4. **Asset Disposal and Secure Data Deletion:**
    - When data or records are no longer necessary, they must be **securely and irreversibly deleted**. [49]
    - Physical storage devices containing Confidential/Strictly Confidential data must be destroyed physically (e.g., shredding) before being removed from the Company. [50]
    - All critical Asset Disposal or Data Deletion procedures must be documented in the IT Department's records. [51]
5. **Handling Lost or Stolen Devices:**

- Employees are responsible for **immediately reporting** (within **1 hour**) to the IT Department and direct Management upon discovering a loss or theft of Company devices. [52]
- The IT Department has the right and responsibility to implement emergency measures, including **Remote Wipe** and disabling access accounts. [53]

Article 7: Access Control [54]

1. **Principles of Granting Access:**
    - **"Need-to-Know" Principle:** Access rights shall only be granted when the employee genuinely requires that access to perform their assigned duties (Principle of Least Privilege). [55]
    - All requests for new, modified, or revoked access rights must receive official approval from the Asset Owner and/or direct Management. [56]
2. **Identity and Password Management:**
    - Passwords must be a minimum of **8-12 characters long** [57]and include a combination of uppercase letters, lowercase letters, numbers, and special characters[58].
    - Passwords must be changed at least once every **90 days**. [59]
    - Accounts and passwords are personal and shall **not be shared** in any form. [60]
    - Mandatory activation of **Multi-Factor Authentication (MFA)** for all remote access accounts and systems containing Confidential/Strictly Confidential data. [61]
3. **Privileged Account Management:**
    - Highest-level administrative accounts shall **only be used for system maintenance and management purposes** and shall not be used for routine work activities. [62]
    - Privileged accounts must use stronger than normal passwords and must use **Multi-Factor Authentication**. [63]
    - All actions using privileged accounts must be logged in detail, stored, and periodically reviewed and monitored by the IT Department. [64]

Article 8: Physical and Environmental Security [65]

1. **Access Control:**
    - Areas containing critical assets must be designated as **restricted areas**. [66]
    - Visitors must always be registered, issued a badge, and accompanied by a Company employee. [67]
2. **Protection of Working Areas:**
    - **"Clear Screen/Clear Desk" Policy:** Employees must **lock their computers** immediately upon leaving their desk. [68]
    - Documents and physical storage devices containing Internal or higher level information must be stored securely (locked cabinets, locked drawers) when employees leave the office. [69]

Article 9: Network and System Security [70]

1. **System Protection and Anti-Malware:**
    - All endpoints must install and maintain approved anti-malware software, ensuring automatic updates and periodic scans. [71]
    - **Patch Management:** Employees must ensure that operating systems and critical applications are updated with security patches promptly (e.g., within **7 days** of the patch release). [72]
2. **Email and Internet Safety Rules:**
    - Strictly prohibited to send **Confidential/Strictly Confidential** documents outside the Company network without using encryption or password protection measures. [73]
    - Strictly prohibited to access, download, or transmit illegal, malicious, or inappropriate content through the Company's network and devices. [74]
3. **Vulnerability Assessment and Penetration Testing:**
    - The IT Department must conduct periodic **security vulnerability assessments** (at least **once per year**) on critical systems and applications. [75]
    - Discovered security vulnerabilities must be addressed and remediated according to the established Patch Management procedure. [76]

Article 10: Human Resources Security Management [77]

1. **Information Security Training:**
    - All employees must attend information security and personal data protection **awareness training** at least **once (1) per year**. [78]
    - The training program must include content on recognizing and reporting threats such as **phishing emails and social engineering attacks**. [79]
2. **Termination Procedure:**
    - The IT Department must **immediately disable or delete** all accounts and system access rights of the terminating employee by the end of their last working day. [80]
    - All physical assets of the Company must be returned and checked before the employee leaves. [81]

PART III: SPECIFIC PROVISIONS ON PERSONAL DATA PROCESSING

Article 11: Prohibited Acts in Personal Data Protection and Processing [82]

1. Processing personal data contrary to personal data protection laws. [83]
2. Processing personal data to create information or data aimed at opposing the Socialist Republic of Vietnam. [84]
3. Processing personal data to create information or data that affects national security, social order and safety, and the legitimate rights and interests of other organizations and individuals. [85]
4. Hindering personal data protection activities of competent authorities. [86]
5. Abusing personal data protection activities to violate the law. [87]

Article 12: Responsibilities of the Personal Data Controller and Processor [88]

1. Implement appropriate organizational and technical measures to demonstrate compliance with personal data protection laws. [89]
2. Record and store system logs of the personal data processing process. [90]
3. Report violations of personal data protection regulations as prescribed by current law. [91]
4. Ensure the rights of the data subject as prescribed by current law. [92]

5. Be responsible to the data subject for damages caused by the personal data processing process. [93]
6. Coordinate with the Ministry of Public Security and competent state agencies in personal data protection, providing information for investigation and handling of violations. [94]
7. Fully implement personal data protection measures prescribed in relevant legal documents. [95]

Article 13: Measures and Conditions Ensuring Personal Data Protection Activities [96]

1. Personal data protection measures shall be applied from the beginning and throughout the personal data processing process. [97]
2. Measures include: Management measures (developing regulations)[98]; Designating a department and personnel in charge of personal data protection[99]; Implementing appropriate technical and organizational measures[100]; Performing network security checks before processing[101]; Implementing measures appropriate to the Company's field[102]; Informing the data subject when sensitive personal data is processed[103]; Organizing training to raise personal data protection awareness for employees[104]; Complying with current legal regulations[105].

Article 14: Notification of Personal Data Processing [106]

1. Notification shall be carried out once before proceeding with personal data processing activities. [107]
2. Content of the notification: Purpose of processing; Type of personal data used; Method of processing; Information about other organizations and individuals involved; Potential unintended consequences and damages; Start and end time of data processing. [108]
3. The notification must be in a format that can be printed and copied in writing, including electronic form or a verifiable format. [109]
4. The Company is not required to notify when: The data subject is fully aware of and agrees to the content before collection[110]; Personal data is processed by a competent state agency for public service operations[111].

Article 15: Rights of the Data Subject [112]

1. **Right to be informed** [113], **Right to consent/object to processing** [114], **Right to access, view, modify** [115], **Right to withdraw consent** [116], **Right to data deletion**[117].

2. **Right to restriction of data processing:** Restriction shall be carried out within **72 hours** of receiving the request. [118]
3. **Right to data provision** [119], **Right to object to data processing** (The Company shall comply within **72 hours**). [120]
4. **Right to complaint, denouncement, lawsuit** [121], **Right to claim compensation for damages** [122], **Right to self-protection**[123].

Article 16: Data Subject's Obligations [124]

1. Self-protection of their personal data; requesting others to protect their personal data. [125]
2. Respecting and protecting the personal data of others. [126]
3. Providing complete and accurate personal data when consenting to processing. [127]
4. Immediately notifying the Company if they discover or suspect their own or others' personal data has been compromised, or is at risk of compromise. [128]

Article 17: Data Subject's Consent [129]

1. Consent is required for all personal data processing activities, unless otherwise prescribed by law. [130]
2. Consent is only valid if the data subject is **voluntary** and fully aware of the **Type of data**, **Purpose**, **Organization/Individual** processing the data, and their **Rights/Obligations**. [131]
3. Consent must be **explicit and specific**, expressed in writing, verbally, by checking the consent box, or another action demonstrating this. [132]
4. Silence or non-response from the data subject **shall not be considered consent**. [133]
5. For sensitive personal data processing, the data subject must be notified that the data is **sensitive personal data**. [134]

Article 18: Personal Data Processing without the Data Subject's Consent [135]

1. In **emergency cases** where immediate processing is required to protect the life or health of the data subject or another person. [136]
2. Public disclosure of personal data as prescribed by law. [137]

3. Data processing by a competent state agency in cases of **emergency regarding national defense, national security, major disasters, dangerous epidemics**, or for performing obligations under the data subject's contract. [138]

Article 19: Data Subject's Withdrawal of Consent [139]

1. Withdrawal of consent shall **not affect the legality** of data processing agreed upon before the withdrawal. [140]
2. Upon receiving the request, the Company shall notify the data subject of the potential consequences and damages. [141]
3. The Company must **cease** and request relevant organizations to cease processing the data of the data subject who withdrew consent. [142]

Article 20: Personal Data Storage and Provision [143]

1. **Storage:** Personal data may be stored in Vietnam or abroad, including cloud computing solutions [144], for the necessary period to fulfill agreed purposes[145].
2. **Provision Request Form:** Requests must be in Vietnamese and include: Requester's information, authorization (if any), the personal data requested (specifying document name), form of provision, and reason/purpose. [146]
3. **Provision Deadline:** The Company shall provide personal data within **72 hours** of receiving the data subject's valid request. [147]
4. **Refusal to Provide:** The Company shall not provide personal data if it causes harm to national defense, security [148], affects the safety/health of others [149], or the data subject does not consent[150].

Article 21: Receiving and Resolving Requests for Personal Data Provision 151

The Company is responsible for receiving and monitoring the process of data provision upon request. If the data is not within its jurisdiction, the Company must notify and instruct the requester to contact the competent authority. 152

Article 22: Modification of Personal Data [153]

1. The data subject has the right to access, view, and modify their personal data. [154]
2. If modification cannot be performed due to technical reasons, the Company shall notify the data subject within **72 hours** of receiving the request. [155]

Article 23: Deletion and Destruction of Personal Data [156]

1. **Grounds for Deletion:** The data subject may request deletion when: Data is no longer needed for the agreed purpose [157], consent is withdrawn [158], objection to processing [159], data is processed unlawfully [160], or deletion is required by law[161].
2. **Exemption from Deletion:** Data deletion shall **not** apply when: Law prohibits deletion [162], data is processed by state agencies [163], data is publicly disclosed [164], or in cases of emergency (national security, disaster, etc.). [165]
3. **Deletion Deadline:** Data deletion shall be carried out within **72 hours** of receiving the data subject's valid request. [166]

Article 24: Notification of Personal Data Protection Violations [167]

1. If a violation is discovered, the Company shall notify the Ministry of Public Security no later than **72 hours** after the violation occurs. [168]If the notification is late, the reason for the delay must be included. [169]
2. **Content of the notification** includes: Description of the violation's nature (time, location, types, and volume of data) [170], Contact details of the responsible personnel [171], Description of potential consequences [172], and Description of mitigation measures taken. [173]

PART IV: INCIDENT MANAGEMENT AND CONTINUITY

Article 25: Information Security Incident Management and Violation Handling [174]

1. **Incident Reporting:** All employees are responsible for **immediately reporting** any Information Security Incident (e.g., virus, lost laptop, cyber attack)[175]. Employees must **disconnect the device from the network** in case of malware discovery[176].
2. **Incident Handling Procedure:** The Company shall maintain an Incident Response Team (IRT) to coordinate the stages: Detection, Containment, Investigation, Eradication, Recovery. [177]
3. **Notification:** Notification regarding Personal Data violations shall be carried out in accordance with Decree 13/2023/ND-CP (within **72 hours**). [178]

Article 26: Backup and Business Continuity [179]

1. **Data Backup Policy:** All critical data and systems must be backed up periodically. [180]Backups must be stored in a **separate location** [181]and subject to **Recovery Testing** at least **twice (2) per year**[182].

2. **Disaster Recovery Plan (DRP):** The Company shall maintain a DRP to ensure essential business processes can recover promptly[183]. The DRP must clearly define **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)**. [184]

Article 27: Security Risk Management and Third-Party Security [185]

1. **Information Security Risk Management:** The Company shall conduct periodic information security risk assessments (at least **once (1) per year**). [186]
2. Third-Party Security Management:

a) Require partners to sign a Non-Disclosure Agreement and commit to implementing security measures equivalent to or higher than the Company's standards. 187b) Contracts must include a clause allowing the Company the right to inspect and evaluate (audit) their security measures. 188c) For Third Parties abroad, the agreement must clearly stipulate their obligation to assist the Company in completing the Impact Assessment Dossier for Personal Data Transfer Abroad (NĐ 13/2023/NĐ-CP). 189

Article 28: Personal Data Processing Impact Assessment [190]

1. The Company shall establish and retain its **Personal Data Processing Impact Assessment Dossier** from the commencement of processing. [191]
2. The Dossier must always be available for inspection and evaluation by the Ministry of Public Security and must be submitted to the Ministry of Public Security within **60 days** from the commencement of processing. [192]
3. The Dossier content includes: Purpose, Types of data, Organizations receiving data, Time of processing, **Description of protection measures**, and Assessment of impact/risk mitigation measures. [193193193193]

Article 29: Transfer of Personal Data Abroad [194]

1. Data transfer is permitted if the Party Transferring Data Abroad establishes the **Impact Assessment Dossier for Personal Data Transfer Abroad** and implements the required procedures. [195]
2. The Dossier must be submitted to the Ministry of Public Security within **60 days** from the commencement of processing. [196]
3. The Party Transferring Data Abroad must **cease transferring** personal data abroad if requested by the Ministry of Public Security when: Data is used for activities violating national security [197]; or an incident of **compromise or loss of personal data** of Vietnamese citizens occurs. [198]

PART V: IMPLEMENTATION AND FINAL PROVISIONS

Article 30: Mechanism for Implementing the Data Subject's Right to Feedback and Complaint [199]

1. The Data Subject must immediately contact/send feedback to AIRCLOSET ENGINEERING COMPANY LIMITED via email **aircloset-engineering-admin@air-closet.com**, or directly at the company office. [200]
2. In case of a complaint, the data subject must submit a complaint form as prescribed by law, clearly stating the complainant's information and the content of the complaint. [201]

Article 31: Implementation Effectiveness

1. This Policy shall take effect from **July 25, 2024** and last modified on **October 10, 2025.**
2. Any amendments/supplements/replacements to this Policy shall be issued in writing and publicly updated by AIRCLOSET ENGINEERING COMPANY LIMITED. [204]