HARN ENGINEERING SOLUTIONS PUBLIC COMPANY LIMITED

PERSONAL DATA PROTECTION POLICY

1. Objective

To ensure that the Company, herein referred to as Harn Engineering Solutions Public Company Limited, has proper practices regarding the personal data of customers, business partners, visitors, employees, or any persons related to the Company's business operations. The Company shall establish a system for the collection, use, disclosure, or transfer of personal data, including measures for the management and security of personal data, in compliance with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws and regulations. The Company also adopts appropriate technologies in alignment with its business operations to prevent any damage to data subjects.

2. Definitions

2.1 Personal Data means any information relating to an individual person that enables the identification of such person, whether directly or indirectly, which the Company has collected as specified in this Policy, such as first name, last name, nickname, identification card number, address, date of birth, telephone number, email address, and other related information.

2.2 Sensitive Personal Data means personal data relating to genetics, health, disability, race, ethnicity, religious or philosophical beliefs, political opinions, sexual behavior, criminal records, labor union information, or biometric data, such as facial recognition data and fingerprint recognition data, including any other information which may similarly affect the data subject.

2.3 Processing means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, alteration or modification, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.4 Data Subject (DS) means a natural person who is the owner of the personal data collected, used, or disclosed by the Company. Hereinafter, such person shall be referred to as the "Data Subject."

2.5 Data Controller (DC) means the Chief Executive Officer or any authorized management personnel at all levels who have the authority and responsibility to make decisions regarding the collection, use, and disclosure of personal data, as well as to monitor the use of personal data within their respective departments or areas of responsibility for the Company's activities in good faith.

2.6 Data Processor (DP) means employees, management personnel, or external parties who perform any operations on personal data, including the collection, use, or disclosure of personal data, in accordance with the instructions of the Data Controller.

2.6.1 Internal Data Processor means employees or management personnel authorized by the Company to collect, use, or disclose personal data in the performance of their assigned duties and responsibilities.

2.6.2 External Data Processor means an external individual or juristic person who collects, uses, or discloses personal data in accordance with the instructions or agreements made with the Company.

2.7 Data Protection Officer (DPO) means an employee, management personnel, or external person appointed by the Company to provide advice to the Data Controller, monitor operations relating to the processing of personal data to ensure compliance with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws, report the Company's compliance performance to the Chief Executive Officer, and coordinate and cooperate with the Office of the Personal Data Protection Committee.

3. Personal Data Collected

The personal data collected, used, or disclosed by the Company under this Personal Data Protection Policy belongs to the Data Subjects, whether such personal data is obtained directly or indirectly, as follows:

3.1 Customers include executives, employees, officers of customers, directors, authorized persons, representatives, and other persons acting on behalf of juristic persons or government agencies that are customers of the Company.

3.2 Business Partners or Business Alliances include individuals, directors, authorized persons, representatives, and other persons acting on behalf of juristic persons who are the Company's business partners, service providers, or consultants.

3.3 Shareholders, investors, securities companies, including any persons who contact the Company to request information, website visitors, and participants in activities relating to investment interests in the Company.

3.4 Visitors and external persons entering the Company's responsible areas, for whom the collection of personal data is necessary to maintain security within the Company's premises and areas of responsibility.

3.5 Company Personnel include employees at all levels, directors, advisors, specialists, and persons receiving salaries, wages, benefits, or any other compensation from the Company, including family members or reference persons referred to by the Company's employees.

3.6 Job Applicants include individuals who have submitted job applications or provided personal profile information to the Company, or whose information has been obtained from job application websites for the purpose of applying for employment or internship positions and who have not yet been selected. This also includes family members and reference persons referred to by the job applicants.

4. Duties and Responsibilities

4.1 Board of Directors

4.1.1 Oversee the establishment of policies and practices relating to personal data protection and privacy.

4.1.2 Supervise and ensure that the policy is implemented effectively and concretely.

4.2 Authorized Management Personnel at All Levels

4.2.1 Establish procedures for the collection and storage of personal data within their areas of responsibility in compliance with the policy, guidelines, applicable laws, and the consent of the Data Subject (if any).

4.2.2 Assign responsible persons to carry out operations relating to personal data processing in accordance with the established procedures.

4.2.3 In the event that the Company engages external individuals or juristic persons to perform operations relating to personal data, there must be a selection process ensuring that such parties have standardized personal data protection systems in place.

4.2.4 Supervise compliance with the policy, guidelines, and procedures, including promoting continuous improvement to ensure effective implementation, as well as reporting the results of operations in accordance with the policy and guidelines.

4.3 Departments or Employees Assigned as Data Collectors / Data Processors

4.3.1 Carry out and control operations relating to data processing, including notification, obtaining consent, collection, use, or disclosure of personal data, in compliance with the personal data protection procedures and applicable laws.

4.3.2 Implement and monitor appropriate security measures to prevent loss, unauthorized access, use, alteration, modification, or unlawful disclosure of personal data, including notifying the management personnel acting as the Data Controller within the department of any data breach incidents that occur.

4.3.3 Carry out and control the deletion or destruction of personal data when the retention period has expired, or when such data is no longer relevant or necessary for the purposes of collection, or upon request of the Data Subject.

4.3.4 Review, monitor, and update personal data to ensure its accuracy and that it remains current.

4.3.5 In the event of a personal data leak or breach, the Data Controller and the Data Protection Officer shall be notified immediately.

4.3.6 Assess risks relating to the personal data under their responsibility, and manage and implement measures to mitigate such risks.

4.4 All Employees

4.4.1 Comply with the Company's Personal Data Protection Policy, guidelines, operating procedures, and other documents relating to personal data protection.

4.4.2 Report any abnormal incidents relating to personal data protection, as well as any non-compliance with applicable laws and the Company's Personal Data Protection Policy, to their supervisors.

5. Personal Data Protection Operational Guidelines

5.1 The Company shall establish measures and guidelines in compliance with applicable laws, regulations, rules, and this Personal Data Protection Policy for the Company's employees and other related persons.

5.2 The Company shall support and encourage employees to have knowledge and awareness of their duties and responsibilities regarding the collection, use, and disclosure of personal data of Data Subjects, and to be prepared to protect the personal data of related persons as if it were their own personal data. Employees must comply with the Personal Data Protection Policy and guidelines established by the Company.

6. Collection of Personal Data

In collecting personal data, the Company's Data Controllers shall consider collecting only the data necessary for lawful purposes and in accordance with the policies or guidelines established by the Company. Consent shall be obtained from the "Data Subject" prior to the collection of personal data, and the Data Subject shall be informed, either before or at the time of collection, of the following details:

6.1 The purpose of the collection for use or disclosure of personal data.

6.2 The types of personal data being collected and the retention period for such data.

6.3 Inform the Data Subject of cases where the provision of personal data is required for compliance with the law, contractual obligations, or for entering into a contract, including notifying the possible consequences of failure to provide such personal data.

6.4 The categories of persons or entities to whom the collected personal data may be disclosed, as specified in Clause 7.

6.5 The rights of the Data Subject.

7. Use or Disclosure of Personal Data

7.1 The Company shall use or disclose personal data only for the specified purposes and in accordance with the criteria prescribed by law to the following entities and persons:

7.1.1 The Company, including its employees, staff, directors, and management personnel involved in the processing of personal data.

7.1.2 Government authorities or regulatory agencies empowered by law, or agencies requesting disclosure of information by virtue of legal authority, such as the Department of Provincial Administration, the Royal Thai Police, the Office of the Attorney General, the Courts of Justice, the Social Security Office, the Revenue Department, the Department of Business Development, and the Office of the Securities and Exchange Commission, etc.

7.1.3 Service recipients and data processors appointed by the Company to be responsible for providing services or managing personal data, such as system development and improvement, maintenance of information system security standards, payment processing, accounting audits, human resource management, or any other services that are beneficial to the Data Subject.

7.2 The Company shall obtain consent from the Data Subject prior to carrying out actions under Clauses 7.1–7.3 and shall not disclose collected personal data to third parties, except in the following cases where consent from the Data Subject is not required.

7.2.1 For the benefit of life, health, or safety (Vital Interest).

7.2.2 For the performance of a contract to which the Data Subject is a party (Contract).

7.2.3 For compliance with legal obligations, court orders, or orders from competent authorities, or any other similar circumstances (Official Authority).

7.2.4 For legitimate interests (Legitimate Interest) or for compliance with legal obligations (Legal Obligation).

7.3 The Company has no policy to transfer personal data outside the country, except where required by a court order or where the Company is legally obligated to do so.

8. Storage, Retention Period, and Security Measures

8.1 The Company shall retain personal data only for as long as necessary to achieve the purposes stated in this Policy. The retention period shall be determined based on the duration of contractual relationships, applicable legal prescription periods, and the necessity to retain personal data for compliance with legal obligations, internal and external audits, and the establishment or exercise of legal claims.

8.2 The Company shall appropriately store and maintain personal data, whether in document form, computer systems, or electronic systems, including tools used by the Company to ensure personal data security. The Company shall ensure that its personal data security measures are appropriate and in accordance with international standards to prevent loss, unauthorized access, use, alteration, modification, or unlawful disclosure of personal data.

8.3 The Company shall restrict access rights and apply technology to safeguard personal data security in order to prevent unauthorized access to computer systems or electronic systems.

9. Rights of the Data Subject

The rights under applicable personal data protection laws that you may exercise in relation to your personal data, which you may request from the Company subject to the conditions prescribed by law and the Company's rights management procedures.

9.1 Right of Access: The Data Subject has the right to access their personal data and request that the Company provide a copy of such personal data, or request disclosure of the source of the personal data collected, used, and disclosed by the Company, to the extent permitted under applicable personal data protection laws.

9.2 Right to Data Portability: The Data Subject has the right to obtain their personal data in a structured, commonly used, and machine-readable format for their own use, and has the right to request that such personal data be transmitted or transferred to another data controller, subject to applicable legal requirements.

9.3 Right to Object to Processing: The Data Subject has the right to object to the collection, use, or disclosure of personal data if the Company does not comply with the purposes stated in Clause 4.

9.4 Right to Erasure or Anonymization: The Data Subject has the right to request the deletion, destruction, or anonymization of their personal data so that it can no longer identify the Data Subject, when such data is no longer necessary for the stated purposes or when the Data Subject withdraws consent.

9.5 Right to Rectification: The Data Subject has the right to request that the Company correct their personal data to ensure that it is accurate, up to date, complete, and not misleading.

9.6 Right to Restriction of Processing: The Data Subject has the right to request the restriction of the use of personal data where the Company is in the process of reviewing a request for rectification or objection to the processing of personal data, or in any other cases where the Data Subject requests the Company to temporarily suspend the use of personal data instead.

9.7 Right to Withdraw Consent: The Data Subject has the right to withdraw consent given to the Company for the processing of personal data at any time while the personal data is held by the Company, unless otherwise restricted by law or a contract that benefits the Data Subject. However, such withdrawal of consent may affect the Data Subject; therefore, the Data Subject is advised to review or inquire about the potential impacts before withdrawing consent for their own benefit.

The exercise of your rights may be restricted under applicable laws, or in certain necessary circumstances, the Company may refuse or be unable to act upon your request to exercise the above rights, such as where it is required to comply with legal obligations or court orders, or where the processing of personal data is necessary for the performance of a contract.

10. Exercise of Data Subject Rights

The Company, in its capacity as the Data Controller (DC), has communicated the procedures for exercising data subject rights under the Personal Data Protection Act B.E. 2562 ("Personal Data Protection Law") through the Company's internal electronic communication channel (Intranet) and via the Company's website at www.harn.co.th. If the Data Subject wishes to exercise any of the rights under Clause 9, the Data Subject must clearly state the purpose of the request in good faith, without bias, and within the scope permitted by applicable personal data protection laws, so that the Company can properly and accurately proceed in accordance with the Data Subject's intention, in accordance with the following procedures:

Procedure for Exercising Data Subject Rights

10.1 Submit a request to exercise rights under the Personal Data Protection Law through the following channels:

1. Email to dpo@harn.co.th, or
2. Through the Company's website at www.harn.co.th under the section "Exercise of Data Subject Rights"

10.2 Provide personal information including first name–last name, national identification number, telephone number, email address, relationship with the Company, period of interaction with the Company, and other relevant details (if any). In this regard, the Data Subject shall consent to the Company collecting, using, processing, or disclosing such personal data for the purpose of exercising data subject rights.

10.3 Select and specify the type of rights to be exercised and review the details of each legal right before submitting the request for the Company to proceed accordingly.

10.4 Supporting documents may be attached, such as JPG or PDF files, to assist the Company in processing the request more efficiently.

10.5 Upon receipt of the request to exercise rights, the Company shall send an automatic email or system-generated message to the Data Subject to confirm that the request has been duly received.

10.6 The Company shall process the Data Subject's request in accordance with the Personal Data Protection Law within 30 days from the date of receipt of a complete request. The Company shall notify the Data Subject of the result via email, including details of whether the request has been fulfilled or not, together with the reasons. In the event that the Company does not proceed in accordance with the request, the Company shall record the details of the request, the reasons, and the applicable legal basis in its database as evidence.

If it is clearly evident that the Data Subject intentionally exercises their rights in bad faith, with bias, or not in accordance with the Personal Data Protection Law, through the Company's established procedures for exercising

data subject rights, or files a complaint to the Personal Data Protection Committee, the Company may consider taking legal action against such Data Subject.

11. Contact Channels of the Company and the Data Protection Officer

If the Data Subject has any concerns or questions regarding the collection, use, processing, or storage of personal data, they may contact the Company through the channels specified by the Company. The Company will make its best efforts to facilitate such requests, except where the requested action would impose an unreasonable burden on the Company, risk infringing the personal data protection rights of others, be contrary to applicable laws, or be impossible to implement as requested.

If the "Data Subject" has any questions regarding this Personal Data Protection Policy, wishes to exercise their rights as stated in Clause 9, or wishes to file a complaint in the event of any violation of the Personal Data Protection Law, they may contact the Company at:

- Harn Engineering Solutions Public Company Limited,
  No. 559 Soi Soonvijai 4, Rama 9 Road, Bang Kapi Subdistrict, Huai Khwang District, Bangkok 10310, Thailand. Tel: 02 318 9744
- Data Protection Officer (DPO),
  No. 559 Soi Soonvijai 4, Rama 9 Road, Bang Kapi Subdistrict, Huai Khwang District,
  Bangkok 10310, Thailand.
  Tel: 02 318 9744 ext. 4004,
  Email: dpo@harn.co.th

12. Monitoring and Audit

Personal data breaches may occur in both information technology systems and in cases where personal data is stored in paper-based form. The Company hereby defines the following responsibilities:

- Authorized management personnel at all levels or assigned employees, representing various departments, shall be responsible for monitoring compliance with the personal data protection management system and operational procedures within their respective departments.
- The Quality Management Department shall be responsible for verifying compliance with operational procedures related to personal data protection.
- The Chief Financial Officer, acting as the Data Protection Officer, shall oversee compliance with the policy and guidelines, provide training and awareness to employees and data processors regarding the importance of personal data protection, and report results, issues, and opportunities

for improvement of the personal data protection management system to the Chief Executive Officer and management.

12.1 Personal data breach means a breach of personal data security relating to the collection, use, processing, or disclosure of personal data, which results in impacts on the Data Subject, damage, and legal liability, such as:

1. Unauthorized access to personal data
2. Unauthorized alteration of personal data
3. Unauthorized deletion of personal data
4. Loss or theft of personal data
5. Incorrect or inaccurate processing of personal data
6. Processing of personal data beyond the specified purposes

12.2 Monitoring and Audit Channels The Company has established channels for monitoring personal data breach incidents as follows:

1. Authorized management personnel at all levels or assigned employees shall be responsible for reporting incidents.
2. The Information Technology Department shall detect system abnormalities within information systems.
3. The Quality Management Department shall detect abnormalities or non-compliance with the Personal Data Protection Policy that may lead to personal data breaches or data leakage.
4. The Data Protection Officer shall identify personal data breach incidents.
5. Complaints may be received via email at dpo@harn.co.th or through the Company's website at www.harn.co.th under the section "Notification/Complaint of Personal Data Breach and Data Leakage.

12.3 Procedures in the Event of a Personal Data Breach (Data Breach)

1. Upon receiving a notification or identifying a personal data breach incident, the person who receives the report or discovers the incident shall immediately notify the next higher-level management or the assigned employee.
2. Analyze the cause, assess the impact, and contain the personal data breach to the extent possible by the next-level management or assigned employee, and report to the Data Protection Officer as soon as possible. The Data Protection Officer shall be consulted to determine appropriate corrective actions and to eliminate the cause of the breach, as well as to implement preventive measures to avoid recurrence of the personal data breach as soon as possible.

3. Assess the severity level of the personal data breach and record the information in the personal data control system by the Data Protection Officer, and proceed with the following actions:
    3.1 If the severity level is assessed as very low, and the impact of the personal data breach is acceptable, the incident shall be recorded and the process shall be closed.
    3.2 If the severity level is assessed as low, medium, or high, the Company shall notify the Personal Data Protection Committee (PDPC) without delay, and within 72 hours from the time the incident is known, to the extent possible. The Data Subject shall be notified via letter and/or email (where no specific method is prescribed by law). The incident, corrective actions, and related evidence shall also be recorded and retained.

13. Penalties for Violations or Breaches of Personal Data Protection Policy

13.1 Employees who disclose or breach personal data held by the Company, or use such data for personal benefit, or cause damage without authorization from the Data Controller or the Chief Executive Officer, shall be deemed to have committed misconduct and intentional wrongdoing causing damage to the Company. Such actions constitute a serious offense and may result in termination of employment without severance pay.

13.2 Employees assigned by the Company to collect, use, or process personal data who commit misconduct shall be deemed to have committed a serious offense and may be subject to termination of employment without severance pay.

13.3 Employees who request or obtain personal data from Data Subjects for personal use, or use such data for personal gain or in a manner that causes damage to the Data Subject, shall be deemed to have violated this policy. Such conduct constitutes a serious offense and may result in termination of employment without severance pay.

13.4 Employees who fail to comply with this policy or related guidelines shall be personally liable for any resulting damages in accordance with applicable laws and may also be subject to criminal penalties.

14. Personal Data Protection Policy Review

The Company may review and update this Personal Data Protection Policy from time to time to ensure compliance with any changes related to the processing of your personal data and to align with any amendments to personal data protection laws or other relevant laws. In the event of any revision, modification, or amendment, the Company will announce such changes via the website www.harn.co.th and/or other appropriate channels. However, the Company recommends that you review this Policy periodically.