NAM:TECH
We Inspire Humane Capital

DATA PROTECTION POLICY

Version Number: 1.0

Date: 09-10-25

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Data Protection Policy **("Policy")** is to outline the conduct expected of employees, vendors, clients, customers of New Age Education and Skills Foundation ("NAMTECH"), a not-for-profit company established under Section 8 of the Companies Act, 2013 by ArcelorMittal Nippon Steel India Private Limited (AMNS) which has established an institute as New Age Makers' Institute of Technology, who collect, use, protect, Process and store Personal Data. It addresses how NAMTECH and any third party acting on its behalf will collect, use, protect, Process and store Personal Data.

2. SCOPE

This Policy applies to all directors, officers and employees of NAMTECH and to any third party acting on their behalf and to all Processing of Personal Data.

This policy would apply to NAMTECH and all its Data Subjects. The primary sources of NAMTECH India's obligation in connection with data protection are:

- Information Technology Act, 2000 read with applicable rules/regulations thereunder including the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011;
- GDPR

NAMTECH may from time to time have other policies, procedures, forms -- notices and consents etc. which may deal with data protection, primarily in connection with specific functions or business activities. This Policy has to be read in sync with other policies in terms of data protection requirements in NAMTECH's other policies to the extent this Policy imposes additional requirements or requires a higher standard of protection of Personal Data including any inconsistency in the GDPR regulations, policy and procedures would also be overridden by this Policy, to the extent necessary by law.

3. DEFINITION

- **"Binding corporate rules"** are the Personal Data protection policies and applicable regulations which are adhered to by a controller or processor established in the territory of a Member State and as communicated to NAMTECH for transfers or a set of transfers of Personal Data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

- **"Consent"** means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data.

- **"Control"** means the possession, direct or indirect, through one or more intermediaries of the power The term to direct or cause the direction of the management and policies of a company or legal entity, whether through the ownership of voting securities, by contract or otherwise.

- **"Data Controller" or "Controller"** means the natural or legal person which alone or jointly with others determines the purposes and means of Processing of Personal Data.

- **"Data Subject"** means any natural person whose Personal Data are processed in the context of a process falling in the scope of this Policy.

- **"EEA"** means European Economic Area, consists of the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway; excluding Switzerland).

- **"GDPR"** means General Data Protection Regulation', Regulation 2016/679 of the European Parliament;

- **"Personal Data"** means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

- **"Personal Data Breach"** refers to any actual or suspected breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

- **"Processing"** in relation to Personal Data means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection,

[1] *The provisions relating to GDPR would cover the aspects of dealing with EU customers/suppliers, if any.*

recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

- **"Processor"** means a legal entity which processes Personal Data on behalf of the Data Controller. The word "Processor" has the same meaning as "Service Provider" as commonly used within NAMTECH.

- **"Recipient"** means a natural or legal person, public authority, agency or any other body to whom Personal Data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

- **"Sensitive Personal Data"** means such Personal Data or information of person which consists of information relating to password; financial information such as bank accounts or credit card or debit card or other payment instrument details; physical, physiological or mental health condition; sexual orientation; medical records and history; biometric information; any details relating to the points mentioned before as provided to body corporate for providing services; and any details relating to the points mentioned before as provided by body corporate for processing, stored or processed under lawful contract or otherwise; provided that any information that is freely available or accessible in public domain under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information.

- **"Vendor"** referred herein would mean any individual, second/third party or entity that has entered into a business, function, activities or contractual relationship with NAMTECH in relation to any sale of product or services, either for NAMTECH's own use or as part of an item or service that NAMTECH intends to resell or render over the short or long term.

4. ROLES AND RESPONSIBILITIES

The Head of IT will have overall responsibility for the implementation of this Policy , as well as related privacy and data protection policies. NAMTECH including their directors, officers and employees, that process Personal Data must comply with this Policy as well as related privacy and data protection policies.

IT team shall define, implement and monitor deployment of an internal control system with NAMTECH, required to achieve its objectives in the field of compliance and security.

5. DATA PROTECTION OFFICER/ GRIEVANCE OFFICER

- NAMTECH shall appoint a designated Data Protection Officer/s to address any discrepancies and grievances of Data Subjects with respect to Processing of data in a time bound manner.
- Under GDPR, when Processing EEA personal data in the circumstances referred to in Articles 37(1)(b) and (c) of the GDPR, have a Data Protection Officer and meet the requirements of Articles 38 and 39 of the GDPR with respect to the Data Protection Officer's position and tasks.
- Under the Clause 5 (9) of IT Rules, 2011, **NAMTECH** shall appoint a Grievance Officer, if applicable, and meet the requirements of the specified with respect to the Grievance Officer's position and responsibility.

6. BUSINESS BENEFITS

The Processing of Personal Data is regulated in many of the countries where NAMTECH is present and does business. NAMTECH recognizes that Personal Data must be treated with caution, whether it concerns employees' or business partners' Personal Data. NAMTECH hence wishes to adopt practical and legal measures to protect Personal Data handled under its responsibility.

Within the EU, on May 25th, 2018, the GDPR replaced the 1995 EU Data Protection Directive and superseded the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. The purpose of the GDPR is to protect the "rights and freedoms" of living individuals, and to ensure that Personal Data is not Processed without their knowledge, and, wherever necessary, that it is Processed with their consent.

Similar legislation to protect the "rights and freedoms" of living individuals, and to ensure that Personal Data is processed respecting these rights and freedoms may exist in countries where NAMTECH does business or has a presence.

This Policy serves to lay down uniform, adequate and global data protection standards while Processing Personal Data within NAMTECH.

NAMTECH recognizes that laws in certain countries where NAMTECH does business or has a presence may require stricter standards than those described in this Policy. In that case, NAMTECH shall handle Personal Data in accordance with local law applicable in the countries where the Personal Data are Processed.

7. DATA PROTECTION AT NAMTECH

- The Board of Directors and management of NAMTECH are committed to comply with all relevant local and global laws relating to Personal Data, and to protecting the rights and freedoms of individuals whose Personal Data NAMTECH collects, uses, processes and stores.

- NAMTECH's may have a privacy management framework in future which shall be in consonance with the applicable law and which may *inter a/ia* (i) meet its own requirements for the management of personal information; (ii) support organizational objectives and obligations; (iii) impose controls in line with NAMTECH's acceptable level of risk; (iv) ensure that it meets applicable statutory, regulatory, contractual and/or professional duties; and (v) protect the interests of individuals and other key stakeholders.

8. LEGAL BASIS OR GROUNDS FOR PROCESSING OF PERSONAL DATA

NAMTECH shall not Process Personal Data unless it has a legal basis or ground for so doing. Before undertaking any Processing activity, the right legal ground needs to be identified and recorded. If NAMTECH India Processes Personal Data without any legal basis or grounds as provided below, then such Processing should be immediately rectified to the extent possible and adequate measures should be taken to remedy any breach of Processing norms.

The basis or grounds for Processing may vary depending upon the jurisdictions and applicable law, including GDPR and IT Act, 2000, NAMTECH India would exercise discretion to examine such grounds.

As per GDPR, a legal basis or ground is the legal justification for a Personal Data Processing activity.

In terms of GDPR, the Processing of Personal Data shall always be based on one or more of the six legal basis or grounds set out below:

Performance of a contract;

- Compliance with a legal obligation;

Protection of the vital interest of the Data Subject;

- Performance of a task carried out in the public interest or in the exercise of official authority;
- Legitimate interest of NAMTECH or a third party;
- Prior consent of the Data Subject.

If NAMTECH chooses to process Personal Data based on the Consent of Data Subjects, the Consent shall comply with the following requirements:

- be unambiguous;
- be freely given;
- be specific; and
- be informed.

A process for the withdrawal of consent shall be established.

9. PRINCIPLES OF PERSONAL DATA PROCESSING

In the Processing of Personal Data, NAMTECH shall take into account and comply with the legal principles of Processing of Personal Data, set out below, as and when applicable.

10. LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal Data shall be **processed lawfully, fairly** and in a **transparent manner** in relation to the Data Subjects.

11. LAWFULNESS OF PROCESSING

Processing or handling of Personal Data is considered lawful, if it is based *on* at least one of *the legal* grounds set out in Article 7 *above.*

12. FAIRNESS

NAMTECH must process Personal Data in a fair way. This means that:

- NAMTECH should handle Personal Data in a way that Data Subjects expect the company to Process it (transparency and reasonable expectations);
- NAMTECH should not use Personal Data in a way that it has adverse effects on the Data Subject.

13. TRANSPARENCY

Data Subjects shall be informed of how their Personal Data is being handled. In general, Personal Data must be collected directly from the individual concerned. When Personal Data is collected, the Data Subject must either be aware of, or informed of

- The identity of the Data Controller;
- The categories of Personal Data being collected and the manner of such collection;
- The purpose of data Processing;
- Third parties or categories of third parties to whom the Personal Data might be transmitted;
- the right of Data Subject to seek remedy against NAMTECH for breach of fundamental right to privacy & security breach;
- any other information as may be specified under the applicable law.

14. PURPOSE LIMITATION

Personal Data shall be **collected for specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes.

15. PURPOSE LIMITATION

The specific purposes for which Personal Data is Processed should be explicit and legitimate and determined at the time of collection of the Personal Data. Hence, before collecting Personal Data, NAMTECH will carefully consider in sufficient detail, the purposes the Processing is intended for.

Data obtained for a specified purpose shall not be used for a purpose that is incompatible with the identified purpose.

16. LEGITIMATE PURPOSE

- Personal Data shall be collected for legitimate purposes. This requirement goes beyond the legal grounds for Processing Personal Data listed above to include purposes in accordance with applicable law in the broadest sense. As such, the purposes shall be in accordance with all provisions of applicable data protection law, as well as other applicable laws such as employment law, contract law, consumer protection law etc.

- Furthermore, a legitimate purpose does not only have to be legal, but also reasonable, and the purpose shall be within the reasonable expectations of the Data Subject.

17. DATA MINIMIZATION

Personal Data shall be ***adequate, relevant and limited*** to what is necessary in relation to the purposes for which they are processed.

The principle of data minimization is closely linked to the purpose of the Processing of Persona Data: no more Personal Data can be processed that those needed to fulfil the purpose for which it is collected. The Personal Data that are being processed need to be:

- Adequate (enough Data);
- Relevant (necessary to fulfill the purpose);
- Limited to and not more that needed to fulfill the purpose.

18. ACCURACY

Personal Data shall be **accurate** and, where necessary, **kept up to date;** every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The Personal Data processed within NAMTECH needs to be accurate and up to date. NAMTECH does not keep any data unless it is reasonable to assume that it is accurate. In order tc achieve optimal accuracy (quality) of the Personal Data, NAMTECH tries, as far as possible, tc obtain Personal Data from the Data Subject directly.

19. RETENTION LIMITATION

Personal Data shall be kept in a form which permits identification of Data Subjects for **no longer than is necessary** for the purposes for which the Personal Data are processed.

Personal Data must not be retained any longer than is necessary for the purposes for which they are processed and in compliance with applicable legal requirements with respect to document retention. The Personal Data must be destroyed, or archived after the retention period and in accordance with the applicable laws, when they are no longer necessary for the Processing activity.

The Personal Data maybe retained for a longer period if consented by the Data Principal or necessary to comply with any obligation under the law. NAMTECH shall undertake periodic review to determine whether it is necessary to retain Personal Data in its possession.

20. INTEGRITY AND CONFIDENTIALITY

Personal Data shall be processed in a manner that ensures appropriate **security** of the Personal Data; including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- Personal data must be processed in a manner that ensures its integrity. Data needs to be secured in order to achieve and maintain its integrity. Integrity of Personal Data should be considered for the entire lifecycle of a project or process.
- Confidentiality of the Personal Data: NAMTECH shall ensure confidentiality of the Personal Data by restricting the access to such data and only processed by authorised personnel, on authorised equipment.

21. ACCOUNTABILITY

NAMTECH Controllers shall be responsible for, and be able to **demonstrate compliance with the principles set out in Article 8 and 9 above.**

NAMTECH is not only responsible for ensuring compliance but for demonstrating that each Processing operation complies with the requirements set out in this Policy.

NAMTECH is required to:

i. establish clear documentation, procedures and guidelines supplemental to this Policy as well as related privacy and data protection related policies as required under the applicable law;
ii. maintain a record of Processing activities involving Personal Data;
iii. ensure quality in Processing of Personal Data - *For E.g. The quality of processing means that the risk and exposure of data leakage should be curtailed/ minimum. Also, the data should only be processed for specified purpose and not otherwise -- this would determine the quality ofprocessing;*
iv. implement appropriate security measures to ensure the security of Personal Data and establish as well as maintain a Process to discover and report in the event of a breach;

v. perform Data Protection Impact Assessment if applicable;

vi. establish and maintain a mechanism to comply with Data Principals' Rights,

vii. in the event that Personal Data is Processed based on consent, ensure that consent is validly obtained and records of such consent and protocols for withdrawal of consent are maintained.

22. PROCESSING OF SENSITIVE PERSONAL DATA

NAMTECH shall obtain explicit consent of the Data Principal in respect of Processing of any Sensitive Personal Data:

after informing the purpose of collection to the Data Subject;

in clear terms without recourse to inference from conduct in a context; and

- the collection of such sensitive personal data is necessary for the purpose.

23. DATA SUBJECT RIGHTS

Data Subjects have the following rights relating to their Personal Data that is processed by NAMTECH:

- Right to access details of the nature of Personal Data held by NAMTECH and to whom it has been disclosed or transferred;
- Right to object, restrict, stop or prevent Processing and storage;
- Right to rectify any error in their Personal Data;
- Right to erasure of the Personal Data;
- Right to receive their Personal Data in a structured, commonly used and machine-readable format, and the right to have that Personal Data transmitted to another controller;
- Right to object to any automated decision-making, incl. profiling without consent.

Data Subjects may submit data access requests as described in the relevant policies and procedure.

The above detailed Data Subject rights are not absolute. NAMTECH is subject to legal obligations which may prevent it from giving effect to certain Data Subject Rights requests.

24. SECURITY OF PERSONAL DATA

- NAMTECH shall implement all technical and organizational measures as required under the applicable law to ensure adequate security of Personal Data.

- All employees are responsible for ensuring that Personal Data which **NAMTECH** holds and for which they are responsible, are kept securely and are not under any conditions disclosed to any third party unless that third party has been specifically authorized by **NAMTECH** to receive that information and has entered into a data Processing agreement and/or confidentiality agreement in accordance with the guidelines and compliances on third party data transfers as provided under the applicable law.

- Personal Data should be accessible only to those who need to use it, and access may only be granted in line with the relevant Company policies or procedures. Manual records may not be left where they can be accessed by unauthorized personnel and may not be removed from business premises without explicit written authorization. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the internal Company policies.

- Personal Data may only be deleted or disposed of in line with the applicable law and other relevant Company policies. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by the applicable procedure relating to secure disposal of storage media.

- During the employment and/or service (as applicable) with NAMTECH, the employee or service provider shall comply with all NAMTECH procedures, policies and rules (as *amended from time to time)* for the protection of NAMTECH' s information and/or other confidential information which is valuable and not publicly known or available to the public and kept confidential through considerable efforts including but not limited to production methods, sales methods and other technical and management information.

25. DISCLOSURE AND TRANSFER OF PERSONAL DATA TO THIRD PARTY

NAMTECH shall ensure that Personal Data is not disclosed to unauthorized third parties. All employees should exercise caution when asked to disclose Personal Data held on another individual to a third party and will be required to attend specific training from time to time that

enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of NAMTECH's business.

NAMTECH shall adhere to the cross-border data transfer norms in terms of the applicable laws of India.

Under the GDPR, Disclosure without consent are only permitted in the following circumstances:

- To safeguard national security;
- To prevent or detect crime including the apprehension or prosecution of offenders;
- To assess or to collect tax duty;
- To discharge regulatory functions (including health, safety and welfare of persons at work);
- To prevent serious harm to a third party;
- To protect the vital interests of the individual (in life and death situations).

Under the IT Act & Rules, Disclosure without consent of Sensitive Personal Data are only permitted in the following circumstances:

Government agency mandated under the law

Order under the law

26. DATA TRANSFER MECHANISM

NAMTECH must ensure that the level of protection of Personal Data contained in this Policy and the Binding Corporate Rules is guaranteed when transferring Personal Data internationally. The rules protecting Personal Data continue to apply regardless of where the Personal Data lands.

However, where Personal Data is transferred outside India (i.e. to a third country), NAMTECH must review whether the necessary protection, data transfer mechanism, is in place in order to ensure an adequate level of legal protection in the third country. NAMTECH shall only transfer Personal Data to a third country when this country ensures an adequate level of protection of the rights and freedoms of the Data Subject in relation to the Processing of their Personal Data.

Data transfer mechanisms protection for cross border exchanges include, but are not limited to:

- Adequacy Decision;

- Standard Contractual Clauses;
- Binding Corporate Rules (intra-group transfers only)

When choosing a Personal Data transfer mechanism, always involve the legal department.

27. DATA BREACH NOTIFICATION

In case of breach related to any privacy aspects, NAMTECH inform the appropriate authority as required under the applicable law, in the form of a notice, about the breach of any Personal Data Processed by NAMTECH where such breach is likely to cause harm to any Data Principal.

The said notice shall include the following particulars:

- nature of Personal Data which is the subject-matter of the breach;
- number of Data Principals affected by the breach;
- possible consequences of the breach; and
- action being taken by NAMTECH to remedy the breach.

The said notice shall be made by NAMTECH to the appropriate authority as soon as possible and without undue delay, following the breach, after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm. Where it is not possible to provide all the information at the same time, NAMTECH shall provide such information to the Authority in phases without undue delay.

28. FOLLOW-UP, MONITORING AND EVALUATION

As a practice, each Head of Function must certify compliance with this Policy and report any possible exceptions. Each Function should regularly review its internal controls and proceed with a risk assessment in order to assess its risk profile with respect to Personal Data Protection and adapt its internal controls and procedures accordingly.

This Policy shall be subject to development, review, evaluation and continuous improvement.

Different tools can be used to follow up and monitor risks related to Personal Data protection in addition to the tools and processes set out in this Policy. NAMTECH shall perform management reviews through its Data Protection Officer to follow up on risks relating to protection of Personal Data on a regular basis and shall consider the following:

a) Status of actions from previous reviews;
b) Changes in internal and external issues relevant to the Personal Data Protection;
c) Information on Personal Data Protection performance including trends in;
   - Non-conformities and corrective actions;
   - Measurement evaluation results;
   - Internal and external audit reports;
   - Results and/or trends from the measurement of progress towards the protection of information security and Personal Data.
d) Continuous improvement opportunities including the following:
   - Need for changes including its policies and procedures
   - Results of audits and reviews and recommendations
   - Results of audits and reviews of key suppliers and partners and recommendations
   - Techniques, products or services which could be used to improve compliance
   - Results of exercises and tests
   - Risks or issues not adequately addressed
   - Changes (internal or external) that could affect compliance (post-incident reports)
   - Emerging good practice and guidance

Data Protection Officer & Grievance Officer is _____

Email ID:

Approved by: Mr. Arunkumar Pillai, CEO