Data Privacy Policy

Confidentiality: *This document is solely for the information of Adani Power Limited and should not be used, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.*

1. Introduction

In 2023, the Government of India introduced the 'Digital Personal Data Protection Act of India 2023 to regulate the collection, processing, and storage of personal data by Indian private organizations. In accordance with this legislation, associated rules, notifications, etc. and the controls outlined in ISO27001:2022 for safeguarding personal data, this policy is being formulated to achieve privacy compliance across Adani Power Limited (APL).

2. Purpose and Objective

The purpose of this policy is to establish the privacy related requirements in APL to protect the personal data of its employees, customers, users, and vendors.

The Objectives of this policy are:

- Ensure secure handling and protection of personal data such as health, financial information through robust technical and organisational measures to maintain its Confidentiality, Integrity, and Availability.
- Foster a culture of data privacy awareness across APL.
- To limit the use of personal data to the identified business purposes only for which it is collected.
- To ensure that APL employees are fully aware of the contractual, statutory and/or regulatory implications of any privacy breaches.
- To create an awareness of privacy requirements to be an integral part of the day-to-day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy.
- To make all the employees aware of the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal data.
- To ensure that all third parties collecting, storing and processing personal data on behalf of APL provide adequate data protection.

- To ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross-border transfer of personal data are adhered to.

3. Applicability and Scope

The policy shall be applicable to all locations and departments of APL as a Data Fiduciary (controller), their projects, product or services restricted to Indian territory only, that collect, process, transfer and/or store personal data of any individual/data principal (e.g., such as employees, customers, users, visitors, and vendors), whether gathered offline, digitised subsequently or collected electronically.

4. Policy Statement:

APL shall adhere to the data privacy baseline compliance principles, as outlined below:

a) **Data Privacy Steering Committee:** A steering committee shall be formed to drive data privacy across the organization.

b) **Data Protection Officer:** The Head of Cyber Security will function as the Data Protection Officer (DPO) for the organization.

c) **Data Protection Impact Assessment:** Data Privacy impact assessment (DPIA) for critical applications /systems that include collection/processing of personal data shall be carried out to identify privacy related risks.

d) **Applicable Legal, statutory, regulatory and contractual requirements:** A list of applicable and relevant privacy laws and regulations shall be prepared and updated on a periodic basis.

e) **Privacy Policy & Notice:** All digital data collection points of APL, where personal data is processed shall provide adequate notice to the data principals, whose data is being collected.

f) **Consent:** Consent shall be obtained from data principals at the time of collection of personal data or as per the timeline prescribed by the DPBI (Data Protection Board of India).

g) **Purpose of Personal Data Collection:** Personal data shall be collected for specified, explicit, lawful, and legitimate purposes only and shall not be further processed for purposes which are incompatible with the original purpose(s).

h) **Collection of Personal Data:** Methods of collecting personal data shall ensure that personal data is obtained.

i) **Data Minimization:** Collection of personal data shall be minimized to only adequate, relevant personal data which is necessary for the purpose of processing.

j) **Limited Use, and Disclosure:** Personal data shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

k) **Retention:** Personal data shall be retained only for the duration necessary to fulfil the identified lawful business purposes or as prescribed by law.

l) **Processing of Personal Data:** Personal data shall be processed in lawful, fair and in a transparent manner so that the data principals understand the means and purposes for data processing in a clear and concise manner.

m) **Cookie Handling:** All digital data collection points, where personal data is collected / processed shall implement appropriate cookie management capabilities, setting up customized banners to choose the type of cookies, activate explicit consent capability and to deploy cookie banner on the applications.

n) **Cyber Security Practices for Privacy:** Appropriate physical, technical, and security measures shall be taken to maintain the confidentiality, integrity, and availability of an individual's personal or sensitive personal data. Appropriate Technological controls (Access controls, Data Encryption/ Masking/ scrambling/ Anonymization etc.) shall be implemented to protect personal data as per the relevant internal policies and applicable compliance requirements.

o) **Quality of Personal Data:** Additional validation can be performed to ensure that personal data collected is accurate and complete for the business purposes for which it is to be used.

p) **Contractual Obligations:** Existing contracts, which include processing of personal data shall be reviewed from the data privacy perspective to include applicable data privacy requirements.

q) **Disclosure to Third Parties and Outward Transfers:** Personal data shall be disclosed to third parties only for identified lawful business purposes and after obtaining appropriate consent from the data principals, unless a law or regulation allows or requires otherwise. Privacy related requirements shall be incorporated in contractual agreements with all such third parties.

r) **Cross Border Transfer of Personal Data:** In case of requirement of sharing / processing of personal data outside India, Consent shall be obtained from the respective data principals. It shall be ensured that the recipient country should not be blacklisted by the Indian Government for such activities.

s) **Data breach incident response plan:** A data breach incident management plan shall be prepared to handle any privacy related data breaches. This plan shall also include the internal and external communication plan.

t) **Handling appeals and resolution of disputes of Data Principal (Access, review, Update and deletion of Personal data):** Process for providing access to data updates and redressal mechanism for data principals shall be implemented to address data quality related issues and to address grievances.

u) **Application inventory**: A Centralized repository of applications shall be maintained across all business units which clearly identifies if the application collects, process Personal data.

v) **Integrated Security & Privacy Third-party Risk Management:** A framework should be developed to assess security and privacy risks related to third-party engagements. All collection and processing of personal data by vendors must comply with APL's Information and Cyber Security Policy and adhere to

other relevant standards for data security and protection of personal data, in accordance with applicable laws/regulations.

5. Review

This policy shall be reviewed annually to check for its effectiveness, changes in technology /amendments in DPDP Act 2023, and/or changes in risk levels that may impact privacy, legal & contractual requirements, and business efficiency.

----------**END OF DOCUMENT**----------