Contents

1. Scope and Objective

1.1. Scope

Data protection and privacy policy is applicable to all information, IT and OT assets of AEPL. Further this policy is also applicable to all users such as employees, contractors and all third-party vendors creating, using, storing, and processing AEPL's data.

1.2. Objective

The objective of the policy is to establish guidelines and procedures to ensure the protection, confidentiality, and appropriate use of data collected, processed, and stored by the AEPL. It aims to comply with relevant data protection laws and regulations and protect against unauthorized access or disclosure.

2. Policy Statement

1. AEPL shall ensure that all its data, IT and OT assets are protected from unauthorized or accidental access, modification, destruction, or disclosure, as well as from misuse and abuse.
2. While conducting business activities which involve the processing and usage of AEPL data, AEPL shall ensure that all the confidentiality, integrity and availability of data is maintained.
3. AEPL shall ensure that all personal data processing and handling is done in accordance with AEPL's Data Privacy Policy and other application local regulations.
4. Users shall be educated on their roles and responsibilities and made aware of the impact of their actions on data security.
5. Awareness of data protection shall be promoted throughout the organization.
6. Access to sensitive data must be authorized by the supervisor.
7. Data should not be shared informally. When access to sensitive information is required, personnel can request access from the supervisor and should take all necessary steps to prevent unauthorized access.
8. The supervisor must immediately be notified in the event a device is lost containing sensitive data (e.g., laptops, USB devices).
9. Furthermore, the following sections shall be referred by AEPL while implementing its data protection program.

2.1. Data Creation and Classification

1. Data shall be classified at the creation stage based on the categories and data types listed in Annexure A and B of this document.
2. Information owner shall be responsible to upgrade and downgrade the classification category as per the business needs.
3. The assigned classification categories shall be used to determine the necessary data protection controls that need to be leveraged to secure AEPL data.

2.2. Data at rest/storage

1. AEPL shall ensure that the data at rest is protected by implementation of necessary access control and authentication measures.
2. AEPL shall ensure that the data is encrypted and masked as per section 3 (i.e., Cryptography Policy) of this document.
3. Data shall only be stored on AEPL approved information storage systems. Furthermore, AEPL should have a well-maintained asset inventory of all its information systems which are used for storage of critical data.
4. Data stored and processed by cloud services, shall be protected by encrypting sensitive and confidential data using the default encryption solution provided by the cloud service provider.
5. Portable or removable storage devices should be protected by using encrypting techniques (e.g., using encryption software installed on the device, or using file-encryption software on the computing device to which the portable storage device connects).
6. AEPL shall ensure that the physical copies of data should be stored in a secure location when not in use.

7. Personnel should ensure physical copies of sensitive data are not left unattended (e.g., on a printer or a desk).

2.3. Data in transit

1. AEPL shall ensure that information transmitted outside of AEPL networks, including the internet shall be encrypted or sent via secured channels.
2. AEPL shall identify and document appropriate security standards to be followed for transit confidentiality protection based on the communication protocol used in their system.
3. AEPL shall ensure that data shared in a physical format is appropriately labelled (as per Annexure A), sealed and protected while in transit.

2.4. Data Security Solutions

1. Data Security Solution (e.g., Data Loss Prevention (DLP), Information Rights Management (IRM), etc.) should be used to identify specific types of sensitive data, monitor channels of data leakage, and take actions accordingly to prevent any data loss.
2. Data Security Solution should be configured to monitor and control the flow of sensitive data using the in-built technical policies, defining:

- what data can and cannot be sent, posted, uploaded, moved, or copied and pasted
- where the data can be transmitted
- who can send and receive data (such as email) o how can data be shared

3. A register of keywords, electronic document characteristic and specific types of sensitive information shall be identified, and the data security solution shall be configured against the same.
4. Data security solution should be configured to monitor data leakage channels where sensitive data is in motion (e.g., data traversing a network such as internet), in use (e.g., data processed on endpoints) or at rest (e.g., data stored in file systems, databases, cloud or endpoints).

2.5. Data retention and disposal

1. Data retention period shall be defined, and records shall be retained for the defined period. Retention periods shall define and reviewed at least once in a year based on the following:
    - AEPL's business requirement
    - Legal or regulatory compliances
    - Contractual obligations
2. Records shall be maintained in a safe and secure environment to prevent unauthorized access and tampering.
3. Storage media like floppy disk, hard drives, Compact Disks (CDs), tapes, etc. shall be erased using a degaussing device or "disk-wiping" software before being discarded.
4. If the data cannot be erased, then media shall be physically destroyed in such a way that data should be beyond retrieval.
5. Physical copies of sensitive data should be shredded or disposed in a secure manner when no longer required. Please refer AEPL's IT Asset Disposal Policy for more details.

3. Cryptography

3.1. Use of Cryptography

1. AEPL shall implement approved and secure encryption algorithms for encryption of information at rest and information in transit, depending on the classification, sensitivity of information.
2. Legal and regulatory requirements of cryptographic controls shall be complied with by only using standard publicly released and tested algorithms.

3.2. Key Management

1. AEPL shall ensure security of encryption keys and their backup by implementing access restriction and secure storage mechanisms.
2. AEPL shall ensure that secure mechanisms are implemented for key generation, issuance, access, distribution, storage, processing, and destruction.

4. Legal and Compliance

1. AEPL shall identify and document all applicable legal, statutory, regulatory, and contractual requirements pertaining to cyber security.
2. AEPL shall perform technical compliance review periodically on its information systems to check compliance with its defined Cyber Security Policy and procedures.
3. AEPL shall define and conduct internal and external audit plan for performing information security audits on its information systems.
4. AEPL shall ensure protection and retention of all legal compliance documents as per legal, regulatory, and contractual requirements in accordance with this document.
5. With respect to protection of Personally Identifiable Information (PII), AEPL shall implement adequate security controls in accordance with its Data Privacy Policy to be compliant with applicable local regulatory requirements.
6. AEPL shall incorporate procedure for identifying and reporting of sabotage.
7. AEPL shall prepare a detailed report on disturbances or unusual occurrences, identified, suspected, or determined to be caused by sabotage in the Critical System of AEPL, and shall submit the report to the respective regulatory bodies.

5. Policy Compliance

5.1. Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the IT HOD in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Annexure A – Data Classification Categories

Classification Level	Definition
Public	Data that is not sensitive in nature; can be posted to public facing websites, discussed openly with anyone and has no existing national, international, or legal restrictions on access or usage.
Internal	Data that is not sensitive in nature and has no existing national, international, or legal restrictions. However, use of this data externally could have a low negative impact if disclosed.
Sensitive	Data that is collected through normal business activities or generated through the management of the same. Its use is restricted to smaller teams within the organization who have a legitimate business reason to access it. Compromise of this data could have a moderate negative impact with threats or legal implications on stakeholders.
Confidential	Data that is collected through business transactions or generated through the strategic execution of business activities. Its use is intended for an exclusive group or team of personnel. Compromise of this information could have a significant negative impact on stakeholders with critical threats or legal implications.

Annexure B – Types of data handled at AEPL

Type of Data	Definition
Personally identifiable information (PII)	Personally identifiable information (PII) is information that, when used alone or with other relevant data, can identify an individual. This data type refers to customer PII and Vendor PII. It includes personal information that is collected, managed, or stored by service providers. This includes customer personal information including contact details, background check information, customer personal financial information (credit scores, account numbers etc.), vendor data (contact information and banking details) and leaseholder data
Human Resource Information	Any data stored, managed and/ or handled by the HR including personal data that relates to an employee, consultant, or a contractor (current or past).
Legal Information	Any data created or handled by the legal department. This data includes and not limited to legal contracts, records, audit information, court documents, attorney's information, litigation history.
Operational Data (OT)	Information stored and/ or utilized for operations including critical asset data and SCADA systems data.
Financial Information	Data related to the financial health of a business or customer related data including balance sheet, invoice, treasury, costing, and pricing information. This also includes the data used by internal management to analyze business performance and determine whether tactics and strategies must be altered.