Privacy Policy

AES is committed to its obligations and responsibilities in accordance with The Privacy Act 1988 (which includes the 13 Australian Privacy Principles – APPs) when it handles personal information.

1. Personal and commercial data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal and commercial data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal or commercial data are processed; and
- processed in a manner that ensures appropriate security of the personal or commercial data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General Provisions

- This policy applies to all personal or commercial data processed by Access Engineering Systems and its related entities and Service Partners (AES).
- The Managing Director shall take responsibility for the AES' ongoing compliance with this policy.
- This policy shall be reviewed at annually and modified if required.
- Employees have the right to access their personal data and any such requests made to AES shall be dealt with in a timely manner.

3. Lawful purposes

- All data processed by AES must be done on one of the following lawful bases: consent, contract, legal obligation, or legitimate interests.

4. Data minimisation

- AES shall ensure that personal or commercial data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5. Accuracy

- AES shall take reasonable steps to ensure personal or commercial data is accurate.
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal or commercial data is kept up to date.

6. Archiving / removal

- To ensure that personal or commercial data is kept for no longer than necessary, AES shall put in place an archiving policy in which personal or commercial data is processed.
- The archiving policy shall consider what data should/must be retained, for how long, and why.

7. Security

- AES shall ensure that personal or commercial data is stored securely using modern software that is kept-up-to-date.
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal or commercial data is deleted this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

8. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, AES shall promptly assess the risk and if appropriate report this breach (personal data) to the Office of the Australian Information Commissioner (OIAC). https://www.oaic.gov.au/