Security Policy

APEM takes the security of its activities, its property, its data, the data of its stakeholders, but most of all, the security of its employees extremely seriously. APEM requires and requests the support of all personnel to preserve security in these areas, report potential loopholes or breaches in security and suggest where applicable, improvements or enhancements.

Personal Security
APEM will endeavour to discover security issues at the planning stage and address security both within documented methods and safety risk assessments. Personnel should not tolerate situations where their security is in doubt and report any shortcomings to their line managers so that matters can be resolved.

Personnel should not work alone in situations which can put their security and safety in doubt. Where lone working is requested, a risk assessment should be undertaken, and lone working is not permitted unless security can be assured. Personnel shall follow the lone working protocol when they are working in the office or the field.

Building Security
Personnel are expected to ensure the workplaces are safe and secure. The following practices should be followed:

- Do not leave doors to the outside open and unattended;
- Do not leave hazards unreported – such as fire risks;
- Do not leave windows open when leaving for the day;
- Ensure alarm systems are armed before locking up premises;
- Ensure the outside environment is safe and secure before leaving the safety of a building, especially if you are locking up.

Company Property – Vehicles and Equipment
Personnel should ensure that property, vehicles and equipment are safe and secure from damage and theft and secure from causing harm to others. The following practices should be followed:

- Do not leave equipment unattended, without securing it, e.g. locking or tethering it;
- Do not leave vehicles parked with expensive equipment and valuables inside;
- Do not leave vehicles unattended with doors and windows open;
- Do not place or position vehicles or equipment where they could cause a hazard to others;
- Do not leave hazardous substances unattended or unsecured.

Data Security
APEM ensures security of data complies to the Government backed Cyber Essentials Scheme. APEM's data is hosted within Microsoft Azure which is a cloud-based server solution that complies with key industry standards for security and reliability.

Personnel should not send or provide access to anyone outside the Company to personal data, company data or data from partners and stakeholders. If you become aware of a loophole or potential breach in data security, report it to your line manager. Please refer to APEM's data policy for more information.

Signed

Adrian Williams (Managing Director) **Reviewed: 22/04/2020**

Revision	Date	Approved by	Comments
4	12/04/2019	Adrian Williams	Next Review: 12/04/2020
5	22/04/2020	Adrian Williams	Next Review: April 2021