Security Group Policy

APEM Group 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 Group 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 Group will endeavour to discover security issues at the planning stage and address security both within documented methods and health and safety risk assessments. Personnel should not tolerate situations where their security is in doubt and report any shortcomings to their line manager or via the event reporting system so that matters can be resolved.

Personnel should not work alone in situations which can put their security and safety in doubt. Lone working will form part of the risk assessment process and will not be permitted where personnel security cannot be assured.

Personnel shall follow the lone working protocol when they are lone working in the office or the field.

Building Security
Personnel are expected to ensure that 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.
- When finishing your work, ensure that all electrical equipment is safe and turned off where possible.
- Follow all lock-up procedures relevant to your facility or office.
- 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, i.e. locking or tethering it.
- Do no leave vehicles parked with expensive equipment or valuable 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 Group ensures security of data complies to the Government backed Cyber Essentials Scheme. APEM Group'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 of the company to personal data, company data or data from partners and stakeholders. If staff become aware of a loophole or potential

breach in data security, it should be reported through the line management chain and the APEM Group event reporting system. Please refer to APEM Group's data policy for more information.

It is the responsibility of all APEM Group employees to comply with this policy and to report concerns. APEM Group prohibits any form of retaliation for the reporting of such matters.

All staff will be made aware of this statement as part of their induction on appointment and subsequent on-going training. This policy is communicated and published on the company website for all interested parties.

Reference	Version	Date released	Approved by
T1-GP-021	2	01/08/2023	Leah McGimpsey, Chief Executive Officer, APEM Group
This policy is communicated and published on the company website for all interested parties.			
This policy is subject to periodic review and change to ensure it remains valid. The review period is annotated within the Version Control section, or the policy may be reviewed prior to this date when prompted by context, such as developments in legislation, industry practice, or the organisation. This Policy has been Equality Impact Assessed and no adverse impact has been identified.			