Security Policy

The AWS Board and Stakeholders take the issue of security for the company, employees, customers, suppliers and members of the public as a high priority. In a society where security is becoming increasingly important AWS will ensure that adequate resources are made available to minimise potential risk.

Employee Security

All employees are key to the success of the company and the Board makes employee security a top priority across all sites, all vehicles and on all third-party locations. The Board have in place various procedures that should be read in conjunction with this policy; namely GP1 Emergency Procedure, GP5 Threats to Safety and Security Procedure, GP6 Travel on Company Business Procedure and GP10 Lone Worker Procedure and GP12 GDPR.

Data Security

The business is dependent upon the security of data. Data security is to protect the business intellectual property, financial information, personnel information, supplier information and customer information. Access to data will be restricted to those who require it to perform their duties and the level of access will be graded by the Directors/Data Process Controllers. In doing so, reference should be made to the Company Handbook, Job Description and Appraisals, Disaster Recovery Plan and GDPR Privacy Statement.

Security of laptops, Mobile Phones, Tablets other IT equipment

All employees who have any official Acumen IT equipment must ensure that the equipment and the information it carries remains secure at all times. In particular, the following are highlighted:

- When carried in a driven vehicle, the laptop is to be secured out of sight in the boot/luggage compartment to deter opportunist theft.
- It is highly recommended that laptop computers should not be left unattended in private residences for more than a few days whilst the premises are unoccupied for example whilst on summer leave. Please securely store the laptop in the office to maintain protection of both the equipment and information asset.
- When any IT equipment is presumed, lost or believed to have been compromised, you must immediately report this to your direct line manager and compliance manager.
- Employees are not to download to external devices without express and written approval for the Data Controller or deputy.

Facilities

The facilities at all permanent locations will be equipped with CCTV, perimeter fencing, external lighting and fire alarms; for the protection of personnel, visitors, suppliers and members of the public at all times. Where third party locations have their own security arrangements it is the duty of AWS personnel to familiarise themselves with all site and safety rules. Whilst on external sites having no or little installed security, the Directors will insist upon the provision of adequate (as far as is reasonably practicable), security arrangements to protect personnel, sub-contractors, suppliers, members of the public and plant and equipment.

Counterfeit, Fraudulent and Suspect Items

The company will always use and purchase genuine goods sourced from original manufacturers or legitimate suppliers of goods. The company will use goods that are intended for purpose and not goods which are sold on a misrepresentative basis for said purpose.

Continuous Improvement

The Board directive is for the continual improvement of security in all areas. This will be addressed through measures including auditing and, as far as is reasonably practical and cost-effective, by providing adequate resources and investment in new security technology and other areas of security to further improve the company's security.

For and on behalf of Acumen Waste Group

Leon Kirk
MD
1st May 2018