TAZIKER INDUSTRIAL

Integrated Management System
Section 2.1.15.2

Information Security Policy

Taziker Industrial Ltd will ensure the protection of all information assets within the custody of the Business. High standards of confidentiality, integrity and availability of information will be maintained at all times.

Purpose
Information is a major asset that we as a business have a legislative responsibility and requirement to protect. Protecting information assets is not simply limited to covering information (electronic data or paper records) that the business maintains. It also addresses the people that use them, the processes they follow, and the physical computer or portable device equipment used to access them.

Scope
This Policy applies to all the systems, people and business processes that make up the business's information systems. This includes all employees, contractual third parties and sub-contractors who work on our behalf, and who have access to information systems or information used for our purposes.

Application
Application of this policy is mandated to be applied whenever business information systems are used. As a general guide, information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper;
- Data stored electronically;
- Communications sent by post / courier or using electronic means;
- Stored tape or CCTV video.

Risks
The business recognises that there are risks associated with users accessing and handling information in-order to conduct our day to day activities.

This policy aims to mitigate the following risks:

- An unauthorised or accidental disclosure of, or access to, personal data;
- An accidental or unauthorised loss of access to, or destruction of, personal data;
- An unauthorised or accidental alteration of personal data;
- The non-reporting of information security incidents;
- Inadequate destruction of data;
- The loss of direct control of user access to information systems and facilities.

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

Policy Compliance
If any user is found to have breached this policy, they may be subject to the disciplinary action. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Policy Governance
The following table identifies who within Taziker Industrial Ltd is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Anthony Brooke - Data Privacy Officer – Andy Gill IT Manager
Accountable	Paolo Benedetto – Group Managing Director
Consulted	Rob usher – Head of Group HSQE
Informed	All Directors, Managers and Administrative Staff within the business

References

The following policies and procedures are directly relevant to this policy, and are referenced as follows:

- Data Protection Policy;
- Data Handling & Security Policy;
- IT Access Control Policy;
- IT Data Backup Policy;
- IMS 3.3.1 Data Handling & Security Procedure;
- IMS 3.3.2 Subject Access Request Management;
- IMS 3.3.3 Personal Data Breach Management.

Information Assets

Important information assets will include (but not limited to) the following:

- Filing cabinets and stores containing paper records;
- Computer databases;
- Data files and folders;
- Software licenses;
- Physical assets (computer equipment and accessories, PDAs, mobile phones).

Taziker Industrial Ltd maintain inventories of all important information assets that it relies upon. These identify each asset and associated data required for risk assessment, information/records management and disaster recovery. As a minimum, it includes the following:

- Type;
- Location;
- Designated owner;
- Security classification;
- Format.;
- Backup;
- Licensing information.

Information Storage

All electronic information will be stored on centralised facilities, with regular backups taking place. Records management and retention guidance will be followed, and databases holding personal information must have defined user-access controls applied.

Any sharing or transfer of information with other organisations must comply with all Legal, Regulatory and Policy requirements.

This Policy will be reviewed annually to ensure that it reflects current legislation and regulations.

Paolo Benedetto
Group Managing Director
7th January 2020