TAZIKER INDUSTRIAL

Integrated Management System
Section 2.1.15.4

IT Data Backup Policy

This Backup and Recovery Policy is intended to ensure that portable computers are regularly backed up to prevent loss of data. All information stored in electronic form on Lap-tops and stand-alone PC's are required to be backed up to ensure data integrity in the event of system failure, disaster, or cyber-attack.

Purpose
This Policy is designed to protect data in the organisation to ensure that it is not lost; and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Scope
This Policy applies to all equipment owned or leased and operated by the users within the business.

Application
Personal data is not to be kept on individual user Laptops. Site and office-based laptops user data shall be backed up to the associated user profile on the company IT Azure server no later than on the last day of each calendar month.

Data files stored on the company IT Azure server is automatically backed up on a daily basis.

Restoration
The restoration of user data will be managed by the company IT manager.

Policy Compliance
If any user is found to have breached this policy, they may be subject to the disciplinary action.

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	Andy Gill - IT Manager
Accountable	Paolo Benedetto – Group Managing Director
Consulted	Rob usher – Head of Group HSQE
Informed	All Directors, Managers, Site based 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;
- Personal Data Records Retention 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 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 2019