TAZIKER INDUSTRIAL

# Integrated Management System
# Section 2.1.15.3

## IT Access Control Policy

Taziker Industrial Ltd implements Access Controls applicable to the business IT systems and mobile devices in order to maintain an adequate level of security, and to provide authorised, granular and appropriate user access; to ensure the preservation of data, confidentiality, integrity and availability.

**Scope**
This Policy applies to all employees, contractual third parties and sub-contractors who work on our behalf, and who have access to information systems used for our purposes.

**Principles**
Only authorised users are granted access to information systems, and users are limited to specific defined applications and levels of access rights on a need to know basis. Computer system access control is achieved through the allocation of user ID's and passwords that are unique to each individual user, to manage security measures.

Generic IDs are not permitted to be allocated, and the allocation of privilege rights (e.g.to Laptops, SharePoint, mobile devices and other platforms) shall be restricted and controlled.

Privilege rights will be granted to employees when they are first employed through setting security templates within the company information systems, and will be reviewed as and when new functionality is provided.

Password-enabled screen-savers with a time-out-after-no-activity setting, and a power on password for the CPU and BIOs must be enabled at all times.

Active workstations and laptops are not to be left unattended unless locked. When a user leaves a workstation or laptop at the close of business each day, they must log out of all applications and networks.

Users will be held responsible for all computer activity under their signed in ID. Inactive workstations and laptops will automatically default to the screen saver status after a period of inactivity (typically 30 minutes). Users will then be required to re-log on to the system again for continued usage. This minimises the opportunity for unauthorised users to assume the privileges of the intended user during the user's absence.

User access is to be immediately revoked where an individual's employment ceases. Where user privileges are changed in connection with an alternative job role, privileges must be reviewed, and any changes required must be applied with immediate effect.

Password lists must not be stored in readable form without access control. All such passwords are to be strictly controlled using either physical security or computer security controls. Where any password is suspected of being disclosed, this must be changed by the systems administrator with immediate effect.

The display and printing of passwords must be masked suppressed, or otherwise obscured so that unauthorised parties will not be able to observe or subsequently recover them. After three unsuccessful attempts to enter a password into any workstation or laptop, the involved user-ID must be suspended until reset by a systems administrator.

**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 & Systems Administrator |
| **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;
- Information Security Policy;
- IMS 3.3.1 Data Handling & Security Procedure.

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

**Paolo Benedetto**
Group Managing Director
7th January 2020