Quinn (London) Limited
IT Access Control Policy

Version 1.0

CONTENTS

1. Risks Addressed

This document describes the IT Access Control Policy for Quinn London Limited (“Company”).

2. Scope

This control applies to all systems, people and processes that constitute the organisation’s information systems, including board members, directors, employees, suppliers and other third parties who have access to the Company’s systems.

3. Related Documents

The following policies and procedures are relevant to this document:

- Mobile Computing Policy
- Procedure for the Reset of User Passwords
- Acceptable Use Policy

4. User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are allocated and authorised to use
- Have a unique user name that is not shared with or disclosed to any other user
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the allotted rights are appropriate. System administration accounts must only be provided to users that are required to perform system administration tasks.

4.1 User Registration

A request for access to the organisation’s computer systems must first be submitted to the IT Department for approval. Applications for access must only be submitted if approval has been gained from the applicant’s line manager.

When an employee leaves the Company, their access to computer systems and data must be suspended at the close of business on the employee’s last working day. It is the responsibility of the line manager to request the suspension of the access rights from the IT Department.

4.2 User Responsibilities

It is a user’s responsibility to prevent their user name and password being used to gain unauthorised access to organisation systems by:

- Keeping passwords secret
- Using a strong password

- Ensuring that any PC they are using, when left unattended, is locked or logged out
- Leaving nothing on display that may contain access information such as login names and passwords
- Informing the IT Department of any changes to their role and access requirements.

5. Network Access Control

The use of non-organisation owned PC's connected to the organisation's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from the IT Department before connecting any equipment to the organisation's network.

5.1 User Authentication for External Connections

Where remote access to the network is required, an application must be made via the IT Department.

5.2 Supplier's Remote Access to the organisation Network

Partner agencies or 3rd party suppliers must not be given details of how to access the organisation's network without permission from the IT Department. Any changes to supplier's connections must be immediately sent to the IT Department so that access can be updated or ceased. All permissions and access methods must be controlled by the IT Department.

Partners or 3rd party suppliers must contact the IT Department before connecting to the network and a log of activity must be maintained. Remote access software must be disabled when not in use.

6. Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section above must be applied. The login procedure must also be protected by:

- Not displaying multiple previous login information: i.e. more than one user-name
- Limiting the number of unsuccessful attempts and locking the account if exceeded
- The password characters being hidden by symbols
- Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique user name that will be audited and can be traced back to each individual user. The user name must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

7. Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The ‘business owner’ of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section above
- Be separated into clearly defined roles
- Give the appropriate level of access required for the role of the user
- Be unable to be overridden (with the admin settings removed or hidden from the user)
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access
- Be logged and auditable.