USER MANAGEMENT POLICY

Introduction
This Policy governs:

- The creation, management and deletion of user accounts.
- The granting and revocation of authorized privileges associated with a user-account.
- The authentication (usually a secret password) by which the user establishes their right to use the account.

Scope
This policy applies to all accounts on computer systems directly connected to RELITRADE Network. This includes operating system (Windows, Linux, etc.). This document includes statements on:

- Access Control;
- Managing Privileges; and
- Authentication/Password Management.

Access Control

- The creation, deletion and changes of user accounts and privileges must be carried out by trained and authorized staff.
- The person enacting any change in a user account must be different from the one authorizing/requesting the change.
- An unalterable log will be kept of all account creation/deletion/changes.
- A review period will be established, at an appropriate level for each system, which minimizes information security risks yet allow the Relitrade's business activities to be carried out.

Managing Privileges

- A user account should have the least privilege which is sufficient for the user to perform their role within Network.
- Changes in the privilege of an account must be authorized by a nominated "owner" of the system to which the account affects.
- Procedures shall be established to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the Relitrade.
- User 's privilege rights will be periodically reviewed.

Authentication/Password Management

- All users will have a unique identifier for any Relitrade system.
- The user responsible for their account will keep the accounts authentication details secret and will not divulge it to any other person for any reason.
- The account must not be used by the user where there is a possibility that the account details may be revealed.
- Passwords can only be changed by the user or suitably trained and authorized staff.
- If a user suspects their password is no longer secret it must be changed immediately and the system "owner" notified.
- Forceful change of password at the interval of 15 days is implemented for all users.