RELITRADE STOCK BROKING PVT. LTD.

ACCESS CONTROL POLICY

Introduction

Relitrade Stock Broking Private Limited implements Access Control across all its IT systems and services in order to provide authorized, granular and appropriate user access and to ensure appropriate preservation of data Confidentiality, Integrity and Availability in accordance with the Information Security Management Policy.

Access Control systems are in place to protect the interests of all users of Relitrade computer systems by providing a safe, secure and readily accessible environment to work.

Scope

This policy applies to all Relitrade networks, IT systems and authorized users.

Access Control Principles

Relitrade will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.

The allocation of privileged rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privileged rights to entire team to prevent loss of confidentiality.

Access rights will be accorded following the principles of need to know.

Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.

Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification, and are consequently responsible.

Access Control Methods

Access to data is variously and appropriately controlled according to the data classification levels.

Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.

Access Control Review

A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.