Intellect Money

Intellect Commodities Pvt Ltd

USER MANAGEMENT AND ACCESS CONTROL POLICY

Effective security controls in relation to access to data are an essential component of the effective risk management. Access controls protect information by managing access at all entry and exit points, both logical and physical. These measures ensure that only authorized users have access to specific information, systems and facilities. Therefore, the application of access controls, the management of user accounts and the monitoring of their use plays an extremely important part in the overall security of information resources.

Access controls are established for all major information, information systems and facilities based on their classification and security risk assessment to ensure that the appropriate level of security is implemented.

The company has in place adequate controls for access to server rooms by restricting entry except the directors and compliance officer and proper audit trails are maintained for all unauthorized entry and exit of people for the same.

The persons authorized for Access Control are Mr. Sandeep Jindal and Mr. Ram Ishwar Pandey.

Two factor authentications is not required as the company uses Stan soft software and no facility of IBT, etc is provided by the company.

The access control measures of the company are adequate and commensurate with the size of the organization.

Access to the information assets is based on the User’s roles and responsibilities.

Access to the network, information systems and servers will be achieved by the use of Individual User accounts that will require an appropriate authentication method as outlined in the Password Policy.

All default passwords for accounts must be constructed in accordance with the Company’s Password Policy. All default passwords must be immediately changed by the user immediately after logging into the system.

Users will only be granted access to information and information systems and facilities on a “need-to-know” basis. Users will only be granted the minimum access and privileges required to perform their duties and any changes / modifications required for a particular user will be done only if approval is granted by the Authorised Person for doing the same.

The system requests for identification and new password before login into the system. The system has appropriate authority levels to ensure that the limits can be setup only by persons authorized by the Management.

The organization ensures that access control of internal networks is maintained.

The company maintains the records of all accesses requested, approved, granted, terminated and changed. All accesses granted to User ids are reviewed half yearly.

The company ensures that default system credentials are disabled/ locked.

The Company does not make any In-House Software development. Therefore, Application development, Testing (QA and UAT) and Production environments segregation is not required.