GALADA FINANCE LIMITED

SYSTEM AND CONTROL

27.05.2025

SYSTEM AND CONTROL

Adequate security of information and information systems is a fundamental management responsibility. Nearly all applications that deal with financial, privacy, safety, or defense include some form of access (authorization) control. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system.

From the beginning of the F.Y. 2023-24 the company had upgraded its Software to HYBRID Mode, which is also called double encrypted. Also to ensure Data Protection the company had opted for remote data base commonly termed Cloud based on VPN IP address. All the data are stored both in the external HDD maintained in-house & in the remote data base. In line with the recent amendments on Audit Edit Log the users are classified into hands-on users who are engaged in data entry work and generation of routine documents/reports and supervisory users who are responsible for review of the data generated and adding / editing / deleting data in line with statutory requirements / guidelines.

Currently the company has multiuser platform for data entry with a network of 3 systems including the server for data entry / generation purpose and 3 remote access points for review of the data by supervisory / KMPs / TOP Management / Board of Directors. All the data are stored at one single point the server which takes automatic backup after every entry. Also the software is equipped with multi level access / authentication strategy. The hands-on users are provided with Unique ID with personalized password to entry of data & related activities. They are authorized to enter / edit. The Audit Edit Log provides the details of data generation with respect to ID of the creator / date and time of creation and permitted edit (corrections) including deletion of entries.

The supervisor level user is given complete access to include entry, edit, delete even though their primary task is restricted to review of the entries made / data generated. Separate Audit Edit Log is generated for the supervisory functionaries for review by internal / statutory Audit personals. The supervisor level user ensures regular backup of data in the external HDD maintained in-house & in the remote data base hereafter termed Cloud.

To ensure complete protection of data the company has NPAV-NET PROTECTOR ANTI-VIRUS which comprises of :

1. Anti Virus Malware Rescue Tool;
2. Firewall Protection-Browse Block Virus and Bugs;
3. Latest Virus – Rescue & Recovery

The Company granted Complete access after a successful authentication of the user, but most systems require more sophisticated and complex control. In addition to the authentication mechanism (such as a password), access control is concerned with how authorizations are structured. In some cases, authorization may mirror the structure of the organization, while in others it may be based on the sensitivity level of various documents and the clearance level of the user accessing those documents.

The Company's internal audit is conducted as per the Annual Audit Plan approved by the Audit Committee. The scope of internal audit covers all aspects of business including regular front-end and back-end operations and internal compliances. It lays emphasis to check on process controls, measures undertaken by the Company to monitor risk and to check on leakages or frauds. The Company has invested in ensuring that its internal audit and control systems are adequate and commensurate with the nature of business, regulatory prescriptions and the size of its operations. The internal control system is supplemented by concurrent and internal audits, as well as special audits and regular reviews by the management. For Company-wide internal audits,

The Company has put in place enhanced Risk Based Supervision Systems / Risk Based Internal Audit and ensures continuous monitoring. The Company has an internal team of audit professionals at its head office.. In addition, the Company complies with several specific audits mandated by regulatory authorities such as SEBI / Exchanges / Depositories, and the reports are periodically submitted to the regulators.

The Board/Audit Committee reviews the overall risk management framework and the adequacy of internal controls instituted by the management team. The Audit Committee reviews major instances of fraud on a quarterly basis and actions are taken on the same. It also focuses on the implementation of the necessary systems and controls to strengthen the system and prevent such recurrence. The internal processes have been designed to ensure adequate checks and balances, regulatory compliances at every stage. Internal audit team carries out a risk-based audit of these processes to provide assurance on the adequacy and effectiveness of internal controls for prevention, detection, reporting and remediation of frauds