JINDAL CAPITAL LIMITED

Jcap

INFORMATION TECHNOLOGY SYSTEM

&

INFORMATION TECHNOLOGY POLICY

Head Office:

201, Aggarwal Plaza, Sector - 9
Rohini, Delhi - 110085
E-mail: info@jindalcapital.co.in
Website: www.jindalcapital.co.in

JINDAL CAPITAL LIMITED

Information Technology System
&
Information Technology Policy

Our company **Jindal Capital Limited** is a NBFC, Category B, non-deposit NBFC operating mainly in Delhi NCR for on lending to needy beneficiaries for their business development & to develop Socio Economic status.

In this modern era, Information Technology & its adequate policy is very much important for our company for monitoring & observing of our operational area activities. Information technology is one of the most important departments of our company. The I T team members have the most important role in the company as they manage all technologies and systems of the company as well as all electronic information and critical data. It is important that our company **Jindal Capital Limited** must have adequate I T policy & to implement such policy and procedures. In regards to this matter as this will set out rules and regulations to maintain the security and to control lapses concerning information technology.

We adopted 7 important IT policies and procedures for betterment of our company:

1. Acceptable Use Policy

The Acceptable Use Policy is a policy that ensures all our employees knows the acceptable use of technology .This policy covers defining company's resources that has something to do with technology, such as the computers, computer networks, communication and mail servers, and other resources that need technology to run. We cover these important areas under this policy:

- Employees access to computers
- Computer security
- Email and internet usage
- Sharing confidential information

* Use of computer resources

* Password protection

* Data communication

* Using other's access and files

- Installing of any software that may or may not affect the company
- Monitoring of computer resources and computer logs
- Secure remote login
- Storing and back up of files

2. Security Awareness

Security Awareness policy is important for us to inform all users the result of their actions regarding on security and privacy. This policy ensures that all computer security risks is being handled and control. Some of the actions that this policy covers to reduce related risks and cut down the cost of security incidents are:

- Implementing security policies
- Blocking unauthorized access to networks and computers.
- Improving security awareness
- Early detection and mitigation of security risks

3. Information Security

Information Security policies which sets of rules and regulations that lay out the framework for the company's data risk management such as the program, people, process, and the technology.

These aspects include the management, personnel, and the technology. The most important aspect of this policy tells the point of contact that is responsible for information security such as MIS Head, IT manager, IT specialist, technical consultant, or the data analyst. The BOD have the right to assign someone even if he/she is not part of the IT management.

This policy covers the following aspects:

- System access control
- Information access
- User IDs and passwords
- Password policy

- Password policy

4. Backup and Storage

Jindal Capital Limited adopted the backup & storage IT policy and procedure that enforce the backup and storage policy. As the electronic backup is important in our business to enable a recovery of data and application loss in the case of unwanted and events such as natural disasters that can damage the system, system failures, data corruption, faulty data entry, espionage or system operations errors.

This policy set rules and regulations for the backup and secure storage of all critical data and electronic information of our company.

5. Change Management

The change management policy is to ensure that all changes made are managed, verified, approved, and tracked. Since our system and software are being updated and modified as per requirements of our company and for a number of different reasons, it is important that all of these are managed and tracked by the IT team members to ensure that all things are running smoothly and without a problem.

6. BYOD (Bring your own device)

Our company also adopted **"Bring your own device"** policy is a policy that allows all our employees to bring their own devices such as laptops, tablets, and smart phones to the workplace and to use those devices to access privileged company information and applications.

This policy includes the following aspects:

- All devices must use the approved operating system.
- All devices must save passwords in an encrypted password store.
- All devices must be configured with a secure password that complies with company's password policy.
- Outside devices are not allowed to connect directly to the internal company network.

7. DR/BCP (Disaster Recovery, Business Continuity Plan)

The DR/BCP policy helps our company to manage and control the security risk in real-time. This means that the company is ready and has all the right possible solution for any risk that the company may face. This includes everything from computer threats such as denial-of-service attacks, data corruption, software hack, malware attack, etc. to physical threats such as floods, fires, hurricanes or any other potential disruption of service.

Aim of this policy is to keep the business up and running no matter what threats and risk the company may face. Moreover, the Disaster Recovery, Business Continuity Plan must always involve the business units every time the company may conduct planning and testing.

Thus we can say that Our Company is equipped with the servers, firewall, antivirus and switches, which is maintained by the IT team of corporate office, New Delhi. We opted the concept of online connectivity from corporate office to regional offices & its branches. The servers are online and the access given to the regional heads to upload and to view the data as and when required.

The regional heads are receiving the data from the branches through online / offline as the case may be. The regional offices are well connected with the online system for smooth functioning of the data upload and download.

For security purpose, we are taking back up of the data daily and keeping in the server storage and separately to the external storage device to access for future references.

SYSTEM AUDIT POLICY

Jindal Capital Limited introduced the effective System Audit Policy to monitor & recognize the deficiency of our running customized software through our network computer system. The system audit is a very sensitive aspect of any organization & it is important for our company too. The system audit is an examination of information systems which maintain the reliability & validity of prevailing system inputs, outputs, and processing the data accurately. In the process of System Audit, the board instructs the concerned I.T .officials to take care & to maintain the system in place without any deficiency & to store the company's data related to financial and its operational data in server safely & secured. JCL adopted & implemented System Audit policy to protect our MIS from any cyber threat.

Auditing information security is a vital part of our IT audit. We follow a high level of requisite evaluation of the system's internal control design and effectiveness. The broad scope of auditing information security includes such topics as data centers (the physical security of data centers and the logical security of databases, servers and network infrastructure components), networks and application security. As these topics are always evolving, we have professionally equipped professionals who have wide knowledge and understanding of the systems and environment & its pursuit in Company's systems. We follow internal as well as external Audits to review the inputs, processing and outputs of adopted reliable Management Information Systems (MIS). It focuses on issues like operations, data, integrity, software applications, security, privacy, budgets and expenditures, cost control, and productivity. The concerned I.T. authorized officers / outsourced System Audit Agency conducts our system Audit yearly and the company follows the prescribed guidelines of Reserve Bank of India.

For

Jindal Capital Limited

For Jindal Capital Limited

Director / Auth. Signatory

(Sadhu Ram Aggarwal)
Director