JMJ FINANCE LIMITED

Company Information Technology and Data Protection Policy ("IT policy")

Approved by Board of Directors in meeting held on 11.02.2020

I. Purpose

The Company is growing day by day and the need for proper maintenance of data and protection of data and processing systems is increasing on a daily basis. Based on the recommendation made by experts in the field of Information Technology and cyber laws, the Board decided to place an IT policy which will be the guiding point in maintenance of IT systems, software's, data processing systems and all electronic gadgets in the office premises of HO and Branches. All the staff members and Key Managerial Personnel's using IT related systems/resources (of the Company) in the course of work, irrespective of the location of work, shall be bound to follow this policy.

II. Implementation Of Policy

This policy shall be known as "IT policy" of the Company.

The IT department of the Company shall be under duty to ensure implementation of IT policy. Any suggestions made by IT department shall be duly considered by the Board in the interest of stakeholders of the Company.

However, head of all departments or branches or any place of business of the Company shall be under duty to ensure that IT policy is properly communicated to subordinates/staff or any person covered by the word "User".

III. Definition

Following definitions are for the purpose of understanding and interpreting this policy,

i. IT Resources

Information Technology Resources ("IT Resources") for purposes of this Policy include, but are not limited to, JMJ Finance Limited owned or those used under license or contract or those devices not owned by "JMJ Finance Limited but connected or linked to JMJ Finance Limited -owned Information Technology Resources such as computer hardware, printers, fax machines, scanners, voice-mail, software, e-mail, Internet, intranet or any other electronic gadgets.

ii. User

Any person or group of persons who has access to IT resources of JMJ Finance Limited, including but not limited to, all employees, (whether full time or part time or probationers or trainees or by whatever name they are known in the official records of the Company),vendors, contractors, consultants, and suppliers, unless otherwise excluded expressly by a document/executive order or is a person(s) who cannot be reasonably considered to be "user" by nature of activity undertaken by him or by nature of relationship with company.

iii. Key Managerial Personnel

Key managerial Personnel means and includes Managing Director, CEO, Company Secretary and CFO in the Company, for the time being.

iv. Virus or Malware

Virus or Malware means any programme or software or application or code loaded into the user's computer or IT resources/systems of the Company, directly or indirectly, by mail or pen drive or CD or through any other possible means, with an intention to perform malicious actions or to cause damage/loss to the user/Company or its associate or related parties.

v. Data

Data means the quantities, characters, or symbols in the form of video, audio, text or code on which operations are performed by a computer or any computer operated device or electronic gadgets or IT resources owned by the Company, which is capable of being stored and transmitted in the form of electrical signals or any other available technology and capable of recorded on magnetic, optical, or mechanical or any type of recording media.

Any usages or words not defined here shall be interpreted and understood as per globally accepted practices and laws prevailing in the country.

IV. Scope

The policy covers Company's IT Resources, whether they are owned or leased by the Company or are under the Company's possession, control or custody, directly or indirectly, including but not limited to –

- All computer-related and/or electronic equipment's, including desktop personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, attendance punching devices, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected with the help of any technology.

- All electronic communications equipment or gadgets including telephones, pagers, radio communicators, mobile phones, cameras and surveillance devices, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services.

- All software including purchased or own developed in-house software or licensed business software applications, JMJ Finance Limited's own in-house applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on JMJ Finance Limited's -owned equipment/gadgets.

- All intellectual property and other data stored on JMJ Finance Limited's Information Technology equipment.

The policy also apply to all users, whether on Company property or otherwise, connected from remote connections via any networked connection, or using Company equipment.

V. Sub-policies of IT policy

For more understanding and ease of implementing the policy, the policy is classified into following-

A. General usage policy
B. Internet usage policy and prohibitions
C. Email usage policy
D. Software policy
E. Data backup policy
F. Custody of IT resources policy
G. IT redressal procedure.

A. General Usage Policy

(i) (a)Guiding Principles

All the users shall follow the general principles given below –

- Positive and responsible attitude and behaviour to the implementation of IT policy
- Willingness to comply with all applicable laws, regulations and Company's IT policy.
- Respect for rights and property of others in the IT environment.
- Responsible behaviour consistent with privacy and integrity of electronic networks, electronic data and information and electronic infrastructure and systems.

(b) The users shall keep the IT resources or systems in clean and tidy manner away from dust, pests, poisonous substances and water. The IT resources or systems shall not be touched with wet hands and shall be kept in place out of reach of unauthorised persons. Every user is under duty to report to IT department, cases of unauthorised persons using the IT resources or IT resources being treated in manner against the spirit of this policy.

(ii) Passwords

Passwords or PIN are an essential component of JMJ Finance Limited's computer and network security systems. The following shall be complied with by the "User"-

a) ***Confidentiality of Passwords shall be individual responsibility of the user***. The IT department or concerned official, as the case may be, shall always ensure the passwords allotted to or selected by a user are difficult to guess. It is strongly suggested not to use date of birth, wedding date, date of joining, vehicle registration number, employee id, phone number, house location etc as password /PIN, as the same could be easily guessed by a layman or person having contact with the user. It is strongly suggested to use a combination of numbers, symbols and alphabets in all possible cases to protect the data/network. However, this shall depend upon the understanding of user about his surroundings and people he deal with. Where the user feels that the password is compromised (leaked), he shall inform the IT head immediately and cause to change the password immediately to prevent/limit data loss or data misuse. It is strongly suggested to change the passwords at least once in 60 days in case of systems involving substantial data transmission likely to affect financial position/ operations of the Company. The frequency of changing passwords shall increase depending upon the size and relevance of data transmitted over the device, software or network or any IT resource.

b) The users shall not write or store the passwords in readable format whether in physical form or electronic form in any documentation/ equipment's/ systems or files or folders or in any other locations, where unauthorised persons might discover them. Make sure no one is observing while you are typing in your password/PIN.

c) Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information. Also ensure that old passwords are not re-used again.

d) ***Users shall not use another User's account or password without proper authorization.*** Similarly**,** ***the user shall not share his password(s) with other user(s), unless the said user has obtained from the IT Head, the necessary approval in this regard***. In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared. Where such prior approval is not obtained by such user, such user shall be completely responsible for all consequences that shall follow in respect of breach of this para of this Policy.

e) The head of IT department shall have administrator (admin) rights to revive the password or data, in case of emergency (for eg. On user leaving the organisation without prior notice or without proper handing over of duty or any other emergencies which is likely to affect the financial/ legal/ operational aspects of Company).

f) Where due to carelessness or negligence or irresponsible behaviour of user, a third party (outsider) is found to have accessed the password leading the company to financial loss/operational difficulties/legal problems, then the management may take appropriate action against him after ordering a preliminary investigation into the incident. Where the user is covered under HR policy of the Company, then the management may initiate action under "misconduct" in the course of duty. The word "appropriate action" or "action" may include administrative action, legal suit, compensation for loss suffered by company etc against the user, subject to applicable policies and applicable laws of the Country.

g) In case of software/devices managed by vendors/consultants on behalf of the Company, the vendors may have access rights to passwords and other software/device settings, subject to the agreement between Company and software vendors/consultants. The IT department shall have proper track of the controls applied by software vendor on data or access of network or IT resources by virtue of his/their rights under the agreement.

(iii) Access controls & Security

- All JMJ Finance Limited's computers/laptops/equipment's that are either permanently or temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems. The Computers/laptops of Key Managerial Personnel and Directors involved in operations shall have a password –based access to laptop/computers/IT resources as they are believed to store confidential information in the course of work. However, they may prefer not to have password protection if they themselves and the management are of the view that they are not actively using the laptops/computers/IT systems to deal with/access confidential information.

- Network Modems connected to continuous surveillance systems including CC TV camera or surveillance software shall not be turned off as the same is essential for 24*7 security of the Company. However, the same may be turned off by IT head himself in unavoidable circumstances to ensure data protection (eg. Hacking / cracking by unauthorised persons) or avoid damage to systems during natural calamities/unexpected events. In his absence from H.O, his sub-ordinates or any other officer of the Company may turn off the systems/ resources on direction of Managing Director or any Key Managerial Personnel. In such cases, the IT department shall make a formal report containing reasons for the same and put the same in records after obtaining signature of Managing Director/ Key Managerial Personnel who gave such instruction/direction. This shall be a major record and shall be preserved in the Company for at least 8 years from date of signing. Any unusual events in the IT resources/ systems which affect the normal operations of the Company shall be reported to the IT head who shall investigate into the matter and submit formal report to the Managing Director.

- Access to the server room is restricted and only recognised IT staff, Key Managerial Personnel or any one authorised by the IT head shall be permitted to enter the room.

- Users are prohibited from taking copies of system configuration files (e.g. Passwords, etc) for their own, unauthorized personal use or to provide to other users for unauthorized uses.

- Users shall not be allowed to connect or pair or use their personal pen drives or electronic device/gadgets with IT resources (containing valuable confidential data) of the Company. The IT head may grant approval to officials in case of emergency to use the pen drive/disk/gadget/device in his presence or after thoroughly checking the pen drive/ disk/ electronic gadget/device for virus and malware.

(iv) Security measures

- The users shall not use the wi-fi passwords or networks or devices for personal mobiles or devices. IT head may permit the same in case of emergencies.

- User shall not try to circumvent the security measures/devices.

- Users shall ensure that their laptop, computer or IT resources allotted to them are secure in their absence from office.

- User shall not carry any IT resources out of office while leaving the office after work. However, the IT head may permit users to carry laptop/computers/pen drives or accessories depending upon the nature of work/circumstances. The IT department shall track the status/working condition of such IT resources/systems without fail.

- Unauthorized persons shall not be given access to IT resources, without permission of IT head/department.

- Any attempt by user to copy data from IT resources and systems of the Company using any device or technology available in India or abroad, online or offline shall be regarded as data theft and shall be subject to disciplinary action under Company policies and applicable laws in the country.

- Any voluntary attempt from side of user to hack or misuse the IT resources or crack the passwords/pin or copying files/software, without approval of IT head shall be considered very seriously and action shall be initiated against him/her for breach of this policy.

- Users shall not use the mobile phones, SIM cards, pagers, telephones, internet dongle/modem or similar gadgets of Company for personal purpose (except in emergency cases).

- Users shall not use the IT resources for sending emails or processing or storing files containing obscene matter/defamation material/visuals, statements or audio likely to cause harm to the reputation or mental or physical or financial position of a person/group of persons/organisation or religious sentiments or containing any matter punishable under criminal laws of the country.

(v) Changes to existing system

- No user shall connect or disconnect any equipment to or from the JMJ Finance Limited networks. Where the user notices any change in the connection of networks or equipments, which he has all reason to believe, has been done by another person (without knowledge of IT department), he shall immediately intimate the same to IT head/Department.

- Any repairs/disconnection/modification of IT resources, wirings/cabling etc shall be undertaken in the presence of senior officer in IT department or with knowledge and guidance of IT department head, based on the level of work involved.

- Whereby unintentional mistake any equipment or main cable or accessory is disconnected, the user shall seek the immediate assistance of IT department.

- The IT head shall document all changes to the IT resources and networks on an up-to-date basis including emergency changes.

- Emergency changes could be made only by a person authorised by IT head.

(vi) Privileges and facilities

- Users may request new user ID, facilities or privileges in IT resources. Such requests shall be made by sending a formal request by email/written letter with justification for requesting such privileges.

- The IT department shall maintain adequate MIS (Management Information System) for generating reports that are used for decision making purposes by board of Directors/Committee of Directors and Key Managerial Personnel.

- The IT department shall ensure required software/applications and IT resources are provided to Key Managerial Personnel's and their department staff to ensure filing of forms/reports with statutory authorities in compliance with applicable laws. However, the concerned departments shall communicate such requirements to IT department formally from time to time.

- In case of loans disbursement and banking transactions and transactions involving transfer of money or money equivalents, the Company shall have initiator-maker-checker mechanism to ensure safety of funds and to mitigate risks associated with such transactions. IT head shall ensure the same is followed. Where banks, financial institutions or third parties involved conditions laid down by them shall also be complied, without compromising on security aspects.

- After receiving information from HR / Admin department all system access privileges will be terminated within 24 hours when an employee/staff leaves the Company by resignation or by dismissal or transfer to another branch or on termination of contract, if any, with him.

- The IT head shall withdraw privileges or facilities provided to an officer on a direction issued by Managing Director/HR Department. In cases where major breach of policy is detected by IT head, he can himself temporarily withdraw IT privileges/facilities enjoyed by the official till pendency of official proceedings.

- The IT head shall suo motu withdraw partially or fully, access to IT resources or any privileges/facilities granted to a user where he is found to have engaged in acts via (Company's IT systems/resources)likely to cause harm to the reputation or mental or physical or financial position of a person/group of persons/organisation or religious sentiments or containing any matter punishable under criminal laws of the country, under HR policy or Prevention of Sexual Harassment (POSH) Policy or under applicable laws. However, the IT head shall hold substantial evidence to prove the same.

B. Internet & intranet usage and prohibitions

- All employees (depending upon designation/nature of job) may be provided with a Username and Password to login to the Internet network in the office and to monitor their individual usage.

- The IT department reserves the right to block access to any Internet resource without any prior notice, in case anyone required access to restricted site, the same may be dealt as special case provided the same is identified as use strictly for official purpose and conducting "K" Line business. The approval for the same needs to be obtained by the Department Head / Branch Manager from the IT Head.

- Internet software may only be installed / used by or with the approval of the IT Head.

- Username and password for a new employee must be requested by the HR Dept.

- Sharing the Username and Password with another employee, visitor or guest user is prohibited.

- The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.

- A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.

- The IT Dept will define guidelines for issuing new passwords or allowing employees to modify their own passwords.

- Any password security breach must be notified to the IT Dept. immediately.

- Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization.

Prohibitions

Any disciplinary action considered appropriate by the Management (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

1) Playing online games, downloading and/or watching games, movies, videos or entertainment software, gambling, betting, lottery, video or audio chatting or engaging in any online activity which is personal purpose and/or compromises the network speed and consumes unnecessary Internet bandwidth.

2) Downloading images, videos, audio files and documents unless required for official work.

3) The employees are prohibited from accessing news, social media and other websites online, unless explicitly required for office work.

4) Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work.

5) Accessing pirated software, tools or data using the official network or systems.

6) Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the IT head.

7) Engaging in any criminal or illegal activity or violating law.

8) Invading privacy of co-workers.

9) Using the Internet for personal financial gain or for conducting personal business.

10) Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.

11) Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation.

12) Sharing the confidential data of the Company online.

13) Posting own photos/videos of or photos/videos of employees or guests in facebook, watsapp or social media websites or Apps during working hours. No prohibition in case of celebrations or events during office hours.

14) Causing damage to IT resources or systems by irresponsible and careless/rough usage.

15) re-positioning or disconnecting internet/intranet devices or systems from their normal position or location without necessary approval from IT department.

16) Uploading virus/malicious software or codes into IT resources or networks with or without intention to cause damage to Company.

Irresponsible behaviour & Show cause notice

In case of branches the branch manager shall have right to oversee the functioning of IT resources (non-technical matters) on daily basis. Any irregularities shall be reported to IT department/IT head by email. In all above cases the Company shall issue "show cause notice" to the user/employee within 7 working days asking him to show reason why disciplinary action be intiated against his behaviour in breach of the policy. Before issuing notice, a preliminary report shall be prepared by IT department regarding the breach of policy and the same shall be placed before the authorised officer issuing show cause notice. The employee/user shall give reply to notice within 5 working days or a shorter period as may be communicated by the management in the notice. Non-response to notice within prescribed time limits shall be considered as "misconduct" and the Company may proceed with further disciplinary action as per HR policy of the Company.

On receipt of reply, the IT head and the management shall go through the same and may take action depending upon the facts.

C. E-mail Usage policy

Email Etiquette

1. All official mails shall be responded in a timely manner. (Within 24 hrs). However important mails need to be attended at the earliest.
2. Use professional salutation. Dear Sir, Hi sir etc. Avoid "hey" "yo" or freaky terms. Salutation shall be used according to recipient's designation and position.
3. Avoid highly emotional/ funny/humorous messages in official communication
4. Signature (which contains your name, designation, dept, phone number and Company logo)
5. Give priority to mails from Government /Statutory authorities. No excuse in case of missing the same. Reply to such mails shall be based on the direction from concerned senior officers in HO or concerned department heads or branch heads.
6. In case of confidential data ensure the data is dealt in confidential manner.
7. In case you understand that a mail has been sent wrongly to a person or there is error in what you typed, then send another mail asking apologies and requesting to ignore the same.
8. In case of continuous email conversations always use "reply all" option. However, this shall be the discretion of the user or based on the instruction received by the user from his senior officer or management.
9. All mails from Company head office (including mails from KMP like MD, CS, CEO, COO and CFO) shall be dealt with priority.

Caution/ Prohibitions

1. Information transmitted over email shall not be violate of Prevention of Sexual Harassment Policy (POSH policy) or any applicable company policies or against spirit of law in the country.
2. The users shall be careful with emails from unknown sources or third parties. Any mails with attachments (which has no connection with official matters or looks absurd/ambiguous) received

from an outside person without any reason shall be reported to IT department. Such attachments shall not be opened by users without guidance of IT department.

3. Caution be exercised while sending huge files during peek working hours as the same may interrupt/affect the recipients email software.
4. Any technical issue to email access or sending shall be communicated to your Senior officer and concerned persons and also to IT dept.

D. Software Usage policy

a. General guidelines

a. No employee is allowed to install pirated software on official computing systems.

b. Third-party software (free as well as purchased) required for day-to-day work will be preinstalled onto all company systems before handing them over to employees.

c. No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept.

d. To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email.

e. Any software developed & copyrighted by the organization belongs to the organization.

f. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

g. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

h. Any employee who notices misuse or improper use of software within the organization must inform IT department.

b. System & Software Audit

a. The IT Dept. will conduct periodic audit of software installed in all company-owned systems/software at least once in two years to make sure all requirements are being met.

b. Prior notice may or may not be issued by the IT Dept. before conducting the Software/system Audit.

c. During this audit, the IT Dept. will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes.

d. The full cooperation of all employees is required during such audits.

E. Data Back up Policy

In order to prevent loss of information by destruction of hard disk/server or related devices in which it is stored, a periodic backup procedure need to be carried out by the Users and IT department.

Generally all critical files shall be back up every week. Whether file is important or not depend on its use. All important files stored in the laptop/computer is the responsibility of the user. The user may keep backup of important files (for eg. filings with statutory authorities/Government) in a separate

hard drive or usb device. The users are advised to give “save” “save as” option while dealing in basic office programmes every 1 hour or less than 1 hour.

The server shall have minimum 32 GB RAM and facility to accommodate extra 10 Hard disks of minimum 1 TB storage space. The specs may vary according to updations in server models and priority shall always be given to servers and devices with maximum RAM and storage space. The IT department shall do backup of its servers every week. The Company may use cloud facility to backup data in software on regular basis. The servers and critical systems shall have UPS/inverter backup to avoid data loss due to power failure. A replica mode of all live running servers may be backed up to data cloud or another server. The servers shall be kept in secure area under surveillance of IT head and only those users permitted by IT head shall enter the server room. Server shall have a lock and key or any password operated system for more safety. Periodic testing shall be conducted on a reasonable time limits.

F. Custody of IT resources

Generally all IT resources are under the control of IT department. However, for convenience in operations, custody of IT resources may be given to authorised officers of the company by an executive order or resolution of Board. Directors and Key Managerial Personnel (KMP) like MD, CS, CFO and CEO may be provided with special rights and privileges for carrying/keeping in custody IT resources like laptops, computers, hard disks, mini internet modems, pen drives, digital signatures or any electronic devices owned by Company. They may also allowed to use the IT resources off-office working hours, in the interest of the Company. However, in such cases the concerned official shall not use the IT resources for his personal benefit or against the interest of the Company. IT head shall keep track of such special cases and conduct proper audit to ensure proper management of IT resources.

G. IT redressal procedure

Any requirements/complaints/grievances/suggestions on IT resources shall be mailed to IT head/IT department. Requests could also be made in written format. The IT head shall respond to emails/requests within a reasonable period of time.

VI. Revision/Amendment of IT policy

Any amendments or revision to IT policy shall be made by resolution of the Board of Directors or a Committee of Board constituted for said purpose, whenever required, from time to time. Where any of the clauses in this policy becomes contrary or inconsistent due to changes or subsequent amendments in any applicable laws/rules/regulations/policies, then the new provisions of the particular laws/new statute shall have overriding effect on such inconsistent /erroneous clauses of this policy, till the policy is revised by the Board of Directors/Committee in a duly constituted meeting.

----------End of document----------