IT POLICY

Objective:
The IT policy intends to:

a. Regulate the use of all electronic systems, including computers, printers, fax machines, and all forms of Inter net/intranet access. They are all for company business and for authorized purposes only.
b. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the Company or otherwise violate this policy.

Effective:
The Policy will be in force with effect from January 1st, 2016

Applicability:

- The employees (Regular, Probationers and Interns) of the organization.
- All people associated with Gozoop including vendors, freelancers, clients & consultants.

Regulations:

- Use of Company computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

a. Engaging in private or personal business activities, including excessive use of personal emails and internet.
b. Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant
c. Making unauthorized copies of Company files or other Company data
d. Downloading or transferring material of personal nature via emails, pen-drives, hard-disks or any other devices.
e. Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems;
f. Misrepresenting oneself or the Company
g. Violating the laws and regulations of India or any other nation or any state, city, province, or other local jurisdiction in any way.
h. Engaging in unlawful or malicious activities
i. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity
j. Sending, receiving, or accessing pornographic materials
k. Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems
l. Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended.
m. Use of company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. n. Unless specifically granted in this policy, any non-business use of the Company's electronic systems is expressly forbidden.
o. If you violate these policies, you could be subject to disciplinary action, up to and including dismissal & legal recourse.

- The Company has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal. No employee must down load any unlicensed commercial software without written permission of the IT Team. In case of breaching this clause, the penalty or any legal action will be the liability of the individual employee and not the company.
- For any offcial or personal requirement, employees are not permitted to talk, in person or on email, to any software application vendor like Microsoft, Adobe, Shut terstock, etc. on behalf or representing the company. In case this clause is breached, the employee will be solely responsible to bear any penalty or expenses related to this activity.
- Every employee must change the password of their corporate email ID every 3 months to ensure safety of the account as well as all the confidential information shared on the email account. If you notice any suspicious activity with your offcial email ID or realize that your email ID I hacked, you must immediately inform the IT Team to take preventive measures.
- In case of any hardware damage caused by the employee to the computer, laptop, internet dongle, mobile phone or other electronic equipment given by the company, 50% of the present cost of the damaged product will be borne by the particular employee and will be deducted from the salary of the consequent month.
- Due to the significant risk of harm to the company's electronic resources, or loss of data, from any unauthorized access that causes data loss or disruption, employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, USB / flash drives, "smart" phones, iPods/iPads/i Touch or similar devices, laptops or other mobile computing devices, or other data storage media) to the workplace and connect them to Company electronic systems unless expressly permitted to do so by the Company. To minimize the risk of unau thorized copying of confidential company business records and proprietary information that is not available to the general public, any employee connecting a personal computing device, data storage device, or image-recording device to Company networks or information systems thereby gives permission to the Company to inspect the personal computer, data storage device, or image-recording device at any time with personnel and/or electronic resources of the Company's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the data-storage device in question in order to ensure that confidential company business records and proprietary information have not been taken without authorization. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not connect them to Company computers or networks.
- In case an employee brings his/her personal laptop or computer to offce, he/she is solely responsible for any breach of licenses relating to authorized or unauthorized software on the system.
- Violation of this policy, or failure to permit an inspection of any device under the circumstances covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the se verity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from the Company, from law enforcement officials, or from indi viduals whose rights are harmed by the violation.