IT ACCEPTABLE USE POLICY

1. OVERVIEW

Zoho Corporation IT Service's Acceptable Use Policy aims at protecting Zoho Corporation employees, partners, and the company from illegal actions of individuals. The Acceptable Use Policy is intended to provide a framework governing the use of all IT resources provided by the company.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Zoho Corporation. These systems are used for business purposes in serving the interests of the company, and of clients and customers in course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate of Zoho Corporation who deals with information and/or information systems. It is the responsibility of the employees and affiliates to read and understand these guidelines, and conduct their activities accordingly.

2. PURPOSE

This policy outlines the acceptable use of computers, mobile phones, software, and network systems provided by Zoho Corporation to its employees, contractors, consultants, temporary workers, and other workers employed. These rules are in place to protect employees and the company from risks including virus attacks, compromise of network systems and services, and legal issues due to inappropriate use.

3. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Zoho Corporation's business or to interact with internal networks and business systems that are owned or leased by Zoho Corporation. All employees, contractors, consultants, temporary workers, and other workers employed with Zoho Corporation and its subsidiaries are responsible for appropriate use of information, electronic devices, and network resources according to Zoho Corporation's policy and standards, and local laws and regulations. Zoho Corporation denotes all the entities of Zoho.

4. POLICY

A. GENERAL USE AND OWNERSHIP

i. Zoho Corporation's proprietary information stored on electronic and computing devices, whether owned or leased by Zoho Corporation or the employee is the sole property of Zoho Corporation. You must ensure through legal or technical means that proprietary information is protected.
ii. It is your responsibility to report the theft, loss or unauthorized disclosure of Zoho Corporation's proprietary information promptly.
iii. You may access, use, or share Zoho Corporation's proprietary information within the authorized extent only if it is necessary to fulfill your assigned job duties.
iv. Employees must exercise good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by organization-wide policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
v. Authorized individuals within Zoho Corporation have the authority to view and monitor equipment, systems, and network traffic for security and network maintenance.
vi. Zoho Corporation reserves the right to audit networks and systems periodically to ensure compliance with this policy.

B. SECURITY AND PROPRIETARY INFORMATION

i. All mobile and computing devices that connect to Zoho Corporation's internal network must comply with the Access Control Policy.
ii. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
iii. Allowing other users to use your Zoho account, laptops and other gadgets provided by Zoho Corporation is prohibited. This includes friends, family, and members of the household when employees work from home.
iv. All computing devices must be secured with a password-protected screensaver that must be activated within 10 minutes of inactivity or less. Users must lock the screen or log off when the device is unattended.
v. Employees posting to newsgroups and forums using the official Zoho email address must post a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless they represent the company's views for business purposes.


ZOHO

vi. Employees must be wary while opening email attachments received from unknown senders as it may contain malware.

vii. Employees are not allowed to use unsecured or open wifi for official purposes. Employees are also advised to secure their wifi router connections with enabling WPA2 + AES security.

viii. Employees are advised not to skip security updates in their official devices and ensure that VPN and other software are fully patched.

ix. Employees should ensure that their laptops and gadgets are virus-scanned periodically.

x. Employees are not advised to install pirated / third party software in official devices provided by Zoho Corporation. To install software on company-provided devices, employees are requested to contact the Zoho Corporation IT services team.

xi. Employees are prohibited from providing information/PII of employees working in Zoho Corporation to parties outside the company, knowingly or unknowingly.

5. UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Zoho Corporation authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing resources owned by Zoho Corporation.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

6. SYSTEM AND NETWORK ACTIVITIES

The following activities are strictly prohibited, with no exceptions:

i. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Zoho Corporation.

ii. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted

music, and the installation of any copyrighted software for which Zoho Corporation or the end user does not have an active license is strictly prohibited.

iii. Accessing data, a server or an account for any purpose other than conducting Zoho Corporation's business, even if you have authorized access, is prohibited.

iv. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Employees must consult the management before exporting any material that is in question.

v. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

vi. Revealing your account password to others or allowing use of your account by others. This includes friends, family, and members of the household when employees work from home.

vii. Using computing assets owned by Zoho Corporation to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

viii. Making fraudulent offers of products, items, or services owned by Zoho Corporation.

ix. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

x. Effecting security breaches including, but not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

xi. Effecting disruptions including, but not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

xii. Port scanning or security scanning is prohibited unless Zoho Corporation IT Services approves it after a prior notification is made.

xiii. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

xiv. By-passing user authentication or security of any host, network or account.

xv. Introducing honeypots, honey nets, or similar technology on Zoho Corporation's network.

xvi. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

xvii. Using any program/script/command, or sending messages of any kind, with the intent to

interfere or disable a user's terminal session via any means, locally or via the Internet/Intranet/Extranet.

7. EMAIL AND COMMUNICATION ACTIVITIES

When using the company's resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are mine and not necessarily those of the company". Questions may be addressed to the IT Department.

i. Sending unsolicited emails, including but not limited to advertising material to individuals who did not specifically request such material (email spam).

ii. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

iii. Unauthorized use, or forging, of Zoho Corporation's email header information.

iv. Solicitation of email to any other email address other than the intended recipient, with the intent to harass or collect replies.

v. Creating or forwarding "Chain letters", "Ponzi" or "Pyramid schemes" of any type.

vi. Use of unsolicited email originating from within Zoho Corporation networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Zoho Corporation or connected to Zoho Corporation's network.

vii. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

8. BLOGGING AND SOCIAL MEDIA

i. Blogging by employees, whether using Zoho Corporation’s property and systems or personal computer systems, is also subject to the terms and restrictions in this policy. Limited and occasional use of Zoho Corporation’s systems to engage in blogging is acceptable, provided it is done in a professional and responsible manner, does not violate Social Media policy of Zoho, is not detrimental to Zoho Corporation’s best interests, and does not interfere with an employee's regular work duties. Blogging from Zoho Corporation's systems is also subject to monitoring.


ZOHO

ii. Zoho Corporation's Confidential Information policy also applies to blogging. As such, employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered under Zoho Corporation's Confidential Information policy when engaging in blogging.

iii. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and goodwill of Zoho Corporation and any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.

iv. Employees may also not attribute personal statements, opinions or beliefs to Zoho Corporation, the company, when engaged in blogging. If an employee is expressing his or her beliefs and opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the company. Employees assume any risk associated with blogging.

Apart from following all laws pertaining on the handling and disclosure of copyrighted or export controlled materials, trademarks, logos and any other intellectual property of Zoho Corporation may also not be used in blogging activity.

9. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

Zoho Corporation IT Services team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B. EXCEPTIONS

Any exception to the policy must be approved by Zoho Corporation IT Services team in advance.

C. NON-COMPLIANCE

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10. DEFINITIONS

Term Definition

A. BLOGGING :

Writing a blog. A blog (short or weblog) is a personal online journal that is frequently updated and intended for public consumption.

B. SPAM :

Spam includes but not limited to unauthorized and unsolicited electronic mass mailings.

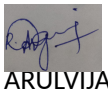
C. IT INFRASTRUCTURE :

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP.

11. RELATED STANDARDS, POLICIES AND PROCESSES

- Social Media Policy
- Access Control Policy
- Password Policy

I hereby certify that I have read and understood the terms and conditions specified above.

Signature:		Date:	08 Aug 2022
Name :	ARULVIJAY P	Place :	SURANDAI