VivaJiva

VivaJiva Policy Manual

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or firm 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 softwareproducts that are not appropriately licensed for use by VivaJiva .

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographsfrom magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted softwarefor which VivaJiva or the end user does not have an active license is strictly prohibited.

3. Use of any kind of external storage (Pen Drive, External HDD) in floor is strictly prohibited. For emergency purposes permission must be taken from system's team via mail.

4. Exporting software, technical information, encryption software or technology, in violation of international or regionalexport control laws, is illegal. The appropriate management should be consulted prior to export of any material that is inquestion.

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

6. Revealing your account password to others or allowing use of your account by others. This includes family and otherhousehold members when work is being done at home.

7. Using a VivaJiva computing asset to actively engage in procuring or transmitting material that is in violation of sexualharassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any VivaJiva account. Making statements aboutwarranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to,accessing data of which the employee is not an intended recipient or logging

E-261, Basement floor
Industrial area Phase 8b
Mohali- 160071
Contact # - 0172-401-3837

into a server or account that the employee isnot expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section,"disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forgedrouting information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.

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

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, auser's computing resources, data, or programs, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, VivaJiva employees to parties outside VivaJiva.

16. Only urgent telephone calls to be attended through personal Mobiles while in the floor. Please try to keep them as short as possible.

17. **GitHub Repository –**

 *Make sure employee always commit the source codes before logging off. Incase of any mishappen in office, GitHub should always have the latest code.

 * GitHub should not be accessed outside of the office, if required permission must be taken from systems team through mail.

* As we can't have back up of every system, therefore it's advisable to use GitHub on regularly basis so that data can be found in any case of emergency. System team is not responsible for employee's data backup.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

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

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within VivaJiva 's networks of other Internet/Intranet/Extranet serviceproviders on behalf of, or to advertise, any service hosted by VivaJiva or connected via VivaJiva 's network.

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

8. **LAN Messenger** – LAN messenger is an internal messenger communication portal. All communication through LAN messenger will be limited to work/work place related.

Social Media & Blogging

Blogging and Social Media participation by employees, whether using the Firm's property and systems or personal computersystems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Firm systems to engagein blogging and Social Media is acceptable, provided that it is done in a professional and responsible manner, does not otherwiseviolate VivaJiva policy, is not detrimental to the Firm's best interests, does not expose client or proprietary information, and doesnot interfere with an employee's regular work duties. Blogging and Social Media from VivaJiva 's systems is also subject tomonitoring.

Definitions

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

Social Media :Social media are computer-mediated tools that allow people to create, share or exchange information, ideas, and pictures/videos in virtual communities and networks. Social media is defined as "a group ofInternet-based applications that build on the ideological andtechnological foundations of Web 2.0, and that allow the creation andexchange of user-generated content.

Spam: Unauthorized and/or unsolicited electronic mass mailings.

Email: The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.

Forwarded email: Email resent from an internal network to an outside point.

Chain email or letter: Email sent to successive people. Typically, the body of the note has direction to send outmultiple copies of the note and promises good luck or money if the direction is followed.

Sensitive information: Information is considered sensitive if it can be damaging to VivaJiva or its customers'reputation or market standing.

Virus warning: Email containing warnings about virus or malware. The overwhelming majority of theseemails turn out to be a hoax and contain bogus information usually intent only onfrightening or misleading users.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people, bothinside and outside VivaJiva, who do not have a need to know that information.

HIPAA Privacy

Privacy is an individual's right to keep certain information to himself or herself, with the understanding that their protected health information (PHI) will only be used or disclosed with their permission or as permitted by law. The HIPAA PrivacyRule states that PHI may be used and disclosed to facilitate treatment, payment, and healthcare operations. TPO: Treatment,Payment and Healthcare Operations:

● PHI may be disclosed to other providers for treatment.

● PHI may be disclosed to other covered entities for payment.

● PHI may be disclosed for certain approved health care activities (health care operations), such as qualityassessment, credentialing, and compliance.

● PHI may be disclosed to individuals involved in a patient's care or payment for care unless the patient objects.

Benefits

- Tea/Coffee is provided by office without any cost.

Leave Policy

Meaning/Purpose

This policy encourages its employees to take a break from work as this provides healthy, stress free and more productive staff. The leave policy sets out the various types of leaves that an employee is eligible for and outlines the procedure for taking leave.

Scope & Eligibility

¤ Leave- 14 days

Leave Available		
April-July	**August-November**	**December-March**
5 leaves + any pending leave from previous	5 leaves+ any pending leave from previous	4-5leaves (Depends on previous leave balance and proper approval.)

*The policy is applicable for all permanent employees of VivaJiva Pvt. Ltd. and not for Contract employees.

*Maximum 2 leaves can be availed in a month. 5 leaves can be taken at a stretch once a year subject to leave availability and leave application at least 15 days prior and approval from immediate Lead/Manager.

*For Contract employees, the leave will be in accordance to the individual contract signed with the company.

*During the probation no leave will be credited to employees. (First 3 months)

*All leaves should be approved by the manager on mail and HR should be copied in every leave application/approval mail.

- Short Day Leave (SDL)- Attendance after 10mins of scheduled shift timings will be consider as short day leave. Short Day Leave will be deducted from the leave balance of the employee. 1 short leave carries .25 of leave balance. (1 SDL=0.25 Leave, 4 SDL= 1 Leave)

- Floor timing should be maintained as minimum 8 hrs./day, as per the delivery schedule of the project employee may be asked to spend extra hours.

- If an employee needs to come in weekends for the requirement of project, he/she will be eligible for compensatory day off.