Vakrangee

सशक्त परिवर्तन

ACCEPTABLE USE POLICY

Contents

1. Introduction

An Access Policy or acceptable use policy is a set of rules applied by the owner/manager/user of a computer system that restrict the ways in which the system or network site may be used.

Acceptable Use Policies are an integral part of the framework of information security policies; it is often common practice to ask new members of an organization to sign an acceptable use policy (AUP) before they are given access to its information systems. For this reason, an AUP must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the IT systems of an organization. It should refer users to the more comprehensive security policy where relevant. It should also, and very notably, define what sanctions will be applied if a user breaks the AUP. Compliance with this policy should, as usual, be measured by regular audits.

2. Document Concerns users

All Users of Information Technology Systems and Infrastructure (Computers, Network and IT Devices) at Vakrangee Limited.

3. Reason for Policy

This policy outlines the responsible and legitimate use of the Information Technology Infrastructure in the organization. These rules are in place to protect the employee and the organization. Inappropriate use exposes the organization to risks including virus attacks, compromise of network systems and services, and legal issues.

4. Statement of Policy

All users of the Organization are required to adhere to the Acceptable Use Policy.

4.1 General Use and Ownership

- Our proprietary information stored on electronic and computing devices whether owned or leased by Us, the employee or a third party, remains the sole property of the organization.
- He/she must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
- Employee/user have a responsibility to promptly report the theft, loss or unauthorized disclosure of Our proprietary information.
- Employee may access, use or share Our proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.
- We reserve the right to audit systems and networks on a periodic basis to ensure compliance with this policy.
- Users shall be responsible for all use of his/her systems and network. In case he/she has a laptop and connects to Our network, he/she will be responsible for all the content on it, especially if he/she – makes the content available to other users. (This provision will also apply to any computer or device for which he/she responsible and is included in the meaning of "my device" or any

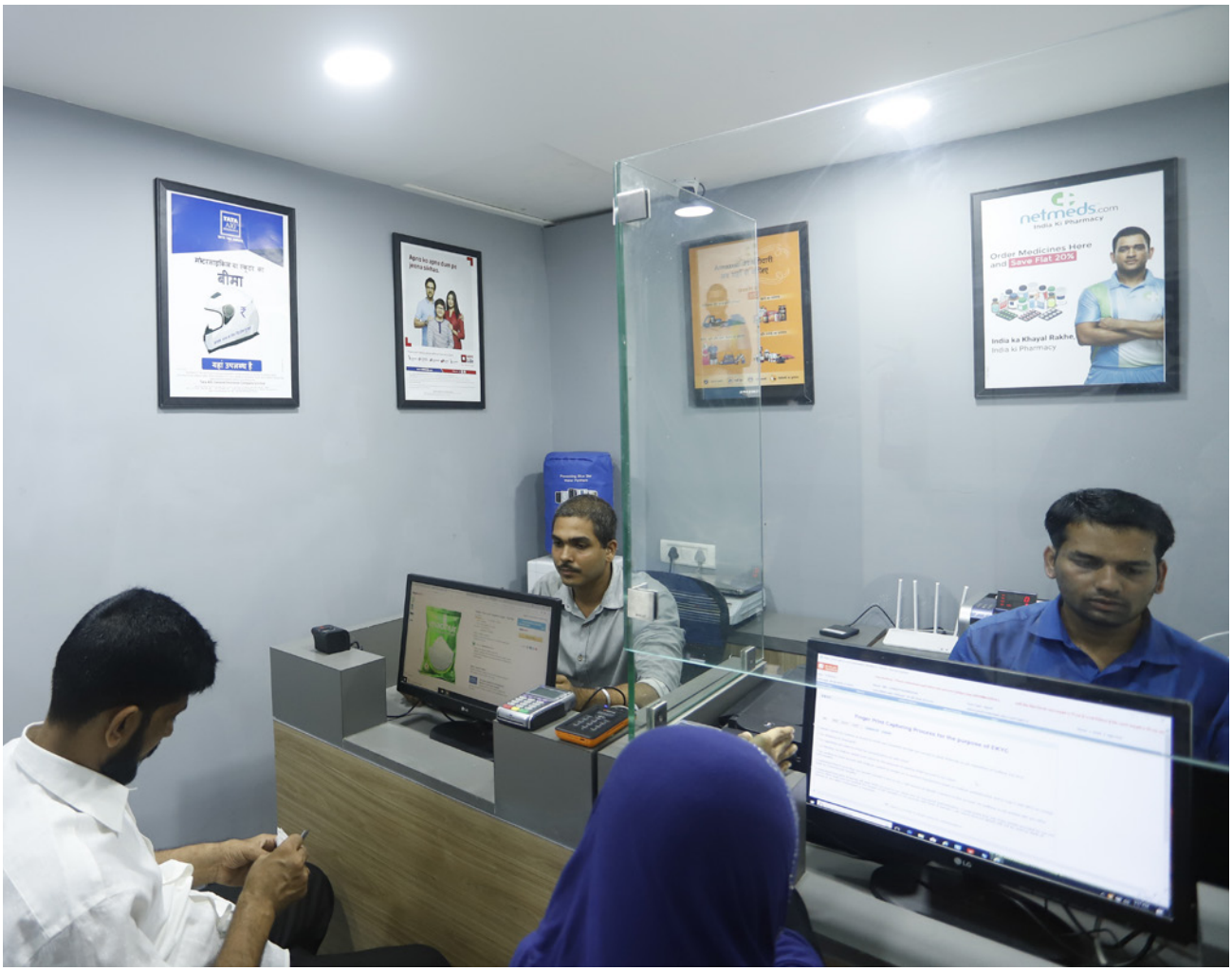
shared device.) In case he/she do not own a laptop but provided with workstation (desktop) or other IT resource, he/she will be held responsible for the content stored in the designated workspace allotted to him/her (examples: file storage area, web pages, stored/ archived emails, on Computer Centre or Department machines).

4.2 Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
- 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.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set. Employee must lock the screen or log off when the device is unattended.
- Employee/user will be held responsible for all the network traffic generated by "his/her device" dedicated or shared. He/she understand that network capacity is a limited and shared resource. He/she agree that physically tampering with network connections/equipment, sending disruptive signals, or making EXCESSIVE USE of network

resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. He/she shall not share the network connection beyond his/her own use and will not act as a forwarder/ masquerader for anyone else.

- Employee/user understand that our IT infrastructure is for official use and he/she shall not use it for any personal purpose or to host data services for other people or groups. Also, he/she will not host or broadcast information that might harm others or may be otherwise considered objectionable or as per law.
- Employee/user will not attempt to deceive others about his/her identity in electronic communications or network traffic. He/she will also not use our IT resources to threaten, intimidate, or harass others.
- Employee/user will not intrude on privacy of anyone by attempting to harvest, collect, store, or publish private or personally identifiable information, such as passwords, account information, addresses, or other contact information without their knowledge and consent. He/she will not try to access computers (hacking), accounts, files, or information not belonging to him/her without knowledge and explicit consent of the owner.



- Employee/user understand that the IT resources provided to him/her are subject to monitoring, with cause, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. He/she authorize the management to perform network vulnerability and port scans on his/her systems, as needed, for protecting the overall integrity and efficiency of Our network.
- Employee/user shall maintain his/her computer with latest system update, virus detection software and latest updates of his/her operating system, and he/she shall attempt to keep his/her computer free from viruses, worms, trojans, and other similar programs.
- Employee/user will not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material).

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees/ user 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/user of Vakrangee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Our owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

- 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 Our organization .
- Downloading or printing of a confidential or restricted data or a volume of one or more documents (called systematic downloading) is strictly prohibited.
- Use of games, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- 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 Vakrangee Limited or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting Our business, even if you have authorized access, is prohibited.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.
- Revealing account password to others or allowing use of account by others. This includes family and other household members when work is being done at home is prohibited.
- Using Our computing asset 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 is prohibited.
- Making fraudulent offers of products, items, or services originating from any of our accounts is prohibited.
- Electronic resources such as e-journals, e-books, databases, etc. made available by the office library are for official use only.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties is prohibited.
- 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 into a server or account that the employee is not 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 forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to IT department is made.
- 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.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on Our network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack) is prohibited.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet is prohibited
- Illegal activity such Threatening, gambling,stalking, defaming, defrauding, degrading, victimizing or intimidating anyone for any reason is strictly prohibited
- Providing information about, or lists of, Our employees to parties outside the Organization is prohibited.
- Any violation of this policy will result in appropriate penal action as per the rules and regulations of the organization.
- Employee/user understand that he/she will not take any steps that endanger the security of the our systems and network. Specifically,

he/she will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible outside the Organization vicinity. In critical situations, Our authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of organization.

- Employee/user understand that any use of IT infrastructure in the organization that constitutes a violation of Our regulations could result in administrative or disciplinary procedures.
- We reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.4 Email and Communication Activities

- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

- 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) is prohibited.
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is prohibited.
- Unauthorized use, or forging, of email header information is prohibited.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is prohibited.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.
- Use of unsolicited email originating from within Our network or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the organization or connected via Our network is prohibited.

5 Policy Compliance

5.1 Compliance Measurement

Our IT 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.

5.2 Exceptions

Any exception to the policy must be approved by the Management in advance.

5.3 Non-Compliance

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

Vakrangee
सशक्त परिवर्तन

CORPORATE OFFICE:
Vakrangee Corporate House,
Plot No. 93, Road No. 16, M.I.D.C.,
Marol, Andheri (East),
Mumbai – 400093, Maharashtra