

# **Computer Network and Internet Access Policy**

## **Jaipur Rugs Company Pvt. Ltd.**



Prepared By:	Mahaveer Prasad Sharma	Page 1 of 4	Approved By:	Mahesh Agarwal

**Disclaimer:**

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the internet do so at their own risk and the Jaipur Rugs is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet at Jaipur Rugs is governed by the following policy:

**Permitted Use of Internet and Company computer network:**

The computer network is the property of “Jaipur Rugs Company” and is to be used for legitimate business purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, certain employees may also be provided with access to the Internet through the computer network. All Users have a responsibility to use Company's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, including possible termination, and civil and/or criminal liability.

**Computer Network Use Limitations:****PROHIBITED ACTIVITIES**

Without prior written permission from Company, the Company's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, trojan horse programs, etc.) or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the user's or any other employee's job performance; b) have an undue effect on the computer or company network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of the Company. Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.

**ILLEGAL COPYING**

Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the company.

**COMMUNICATION OF TRADE SECRETS**

Unless expressly authorized to do so, User is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to

Prepared By:	Mahaveer Prasad Sharma	Page 2 of 4	Approved By:	Mahesh Agarwal

Company. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal Economic Espionage laws.

**Duty not to Waste or Damage Computer Resources:**

**ACCESSING THE INTERNET**

To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to Company's network must do so through an approved Internet firewall or other security device. Bypassing Company's computer network security by accessing the Internet directly by modem or other means is strictly prohibited unless the computer you are using is not connected to the Company's network.

**FRIVOLOUS USE**

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

**VIRUS DETECTION**

Files obtained from sources outside the company, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the company's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with Company-approved virus checking software. If you suspect that a virus has been introduced into the Company's network, notify Company immediately.

**No Expectation of Privacy:**

Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send or receive using the company's computer equipment. The computer network is the property of the Company and may be used only for Company purposes.

**WAIVER OF PRIVACY PLIGHTS**

User expressly waives any right of privacy in anything they create, store, send or receive using the company's computer equipment or Internet access. User consents to allow company personnel access to and review of all materials created, stored, sent or received by User through any Company network or Internet connection.

Prepared By:	Mahaveer Prasad Sharma	Page 3 of 4	Approved By:	Mahesh Agarwal
--------------	------------------------	-------------	--------------	----------------

**MONITORING OF COMPUTER AND INTERNET USAGE**

The Company has the right to monitor and log any and all aspects of its Computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

**Password Policy:**

This policy establishes a standard for creation of strong passwords and protection of those passwords within the Microsoft Active Directory and email systems. This policy applies to all persons who have, or are responsible for, an account on any system accessed on the Jaipur Rugs Company network or computer systems.

**PASSWORD CREATION RULES**

Passwords are initially assigned when a new user account is created. Users have the right and the ability to change passwords on their Active Directory/System accounts at any time.

- o All passwords are required to meet the “strong password” definition.
  - o Passwords must be at least six characters in length.
  - o Passwords cannot contain all or part of user’s login id.
  - o Passwords cannot match any of your four previous passwords.

**PASSWORD EXPIRATION:**

Passwords will expire on a 90-days cycle. Advance warnings of upcoming password expiration will be sent to the designated account beginning 5 days prior to expiration, with repeated reminders every times when users login on the their systems thereafter until the expiration date.

Any account holder may change his or her password at any time through their Active Directory Account.

Passwords should be changed immediately and the Office of Information Technology notified whenever there is a belief that the password has been compromised.

**Blocking Sites With Inappropriate Content:**

The Company has the right to utilize software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

**Employee Termination from an IT Perspective:**

In the case of a terminated employee, IT team immediately revoke all computer, network, emails access and data access the former employee has. Remote access should also be removed, and the former employee should be dispossessed of all company-owned property, including technological resources like a notebook computer and intellectual property like corporate files containing customer, sales, and marketing information.

However, in the case of an employee whose end of employment is only imminent, IT should consult with the employee's manager, HR, and other key decision-makers to determine the appropriate manner in which to stagger the revocation of access over the person's remaining days of employment.

Prepared By:	Mahaveer Prasad Sharma	Page 4 of 4	Approved By:	Mahesh Agarwal