IT ASSETS POLICY

IT Assets Management Policy

Objective

Employees at JAIPUR RUGS are responsible for protecting the information to which they have access and to be alert to any instances of an unsolicited approach or misuse. This policy provides guidelines to employees on the IT assets allotted to them and protection of JAIPUR RUGS data.

Scope

IT assets and information security policy apply to all employees. This policy considers the approach required to protect JAIPUR RUGS's information in a consistent and appropriate manner, therefore it is important to classify and have clear guidelines so that employees are aware of its importance.

1) Laptop

All employees will be provided with either desktop or laptop with charger. The HR team will make a request to the IT team for issuing of a system at least 1 week before the employee is joining. The Standard laptop models will be issued by the IT team, who will also maintain the assets register as per protocol. Employee has to sign a "Laptop Undertaking Form" before taking over the laptop. This form includes acceptance of IT clauses as laid down by JAIPUR RUGS. Technology Department will maintain the inventory of all Laptops whether issued or in stock.

Rules pertaining to the Use of Laptop:

- No personal Laptops should be used in the office premises unless it has been approved by the Chief Technology Officer in writing.
- Employee provided with a Laptop will be responsible for its safe-keeping. In case of loss of a Laptop, the concerned employee will:
  - Intimate the Technology and Administration Department through his/her Functional Head of the loss of the same immediately.
  - Employee to lodge a FIR in the nearest Police station, complete the necessary formalities and submit documentation as required.
  - A copy of the police FIR will be handed over to the Accounts Department / Administration Department, for follow up for insurance.
  - The internal IT team will process the insurance formalities
- Laptops are covered under a warranty clause. In case a Laptop is damaged, the employee will hand over the same to the Technology Department, which will make the necessary arrangement to get the same repaired. The Technology Department will handle all annual maintenance contracts for laptops.
- Any damage to the laptop, software or any other accessories due to mis-handling (not covered under warranty) will be the user's responsibility and financial impact shall be borne by the user. A warning letter can be issued to the employee under Disciplinary Action for damage of company asset.
- There is a likelihood that in extreme cases of damage, the cost of repair may be higher than the cost of a replacement, and hence a new Laptop will need to be purchased. In such cases asset will be written off under approval

2) Printers

- Employees have been given access to the common printer. In work from home situations, employees can be issued individual printer.
- Documents once printed, need to be collected from the printer immediately and should not be left unattended.
- Any breakdown or maintenance of printers will be handled by the technology team.

- In line with the code of conduct, no document shall be printed unless explicitly required. Due care shall be taken by the employee that protocol is followed to print documents outside the premises

3) Wireless Network and Internet Access Services

JAIPUR RUGS reserve the right to monitor the activities and if need be access information such as e-mail, message, content and data relating to the use of Internet facilities. Employees should not engage in any activity which:

- Disrupts the intended use of the resources.
- Wastes resources (people, capacity, computer, network, data etc.)
- Compromises the legal rights of others
- Modifies, damages or destroys computing resources or the data on them.
- Jeopardize, in any way, the integrity, performance or reliability of JAIPUR RUGS's computing resources by indulging in circumvent data protection schemes, to uncover security loopholes, to "hack" into systems or to interfere with the intended operation of the computer resources.

Data Protection

- Any entry or exit of sensitive information from the office premises or while working from home, either physically or electronically has to have prior approval from IT Head.
- All information handled within the company should be adequately labelled, sorted, and stored up to defined expiration date.
- All documents, files, records, customer details, project plans, strategies, developments, execution process, quality metrics, etc., relating to business of JAIPUR RUGS, its clients and customers, that is proprietary to JAIPUR RUGS or its clients shall be deemed to be "Confidential Information".
- Confidential Information is to be strictly confidential and no employee shall, directly or indirectly, make known such Confidential Information to any person or entity or permit such Confidential Information to be disclosed or made known to any person or entity, in each case either inside JAIPUR RUGS or otherwise.
- Every employee should faithfully and diligently protect such confidential information from being disclosed to unauthorized persons. Such persons include, but are not necessarily limited to,
    - Persons who are not JAIPUR RUGS employees.
    - Persons who are JAIPUR RUGS employees but who do not have a need to know the confidential information in order to perform their duties.
    - Persons not under a written confidentiality agreement with JAIPUR RUGS in regard to the confidential information, and persons not directly aware of the proprietary and trade secret nature of the confidential information.
- All documents, files, records, project plans, strategies, customer details and items of information or equipment relating to JAIPUR RUGS's business are and shall remain the property of JAIPUR RUGS, including notes, documents, and files created in the performance of employee's duties of employment.
- All documents, files, records, and items of information relating to JAIPUR RUGS's business, clients and customers shall not be altered, modified, or deleted unless authorized by the respective Head of Department.
- In case of any violation or breach of the aforesaid guidelines, whether intentional or inadvertent, the same should be immediately reported to HR and IT team.

DOS AND DON'TS

Network Security

√ Login password is required to be changed every thirty days.
√ If any user has forgotten the password, they should approach the IT department for resetting of password.
√ Employees should not reveal their username or password to other employees / outside vendors /guests.
√ Should never leave their system unattended with data left open to view by others

Device & Information Security

√ All laptops will have authorized and licensed software. Downloading illegal software is prohibited. Installation of software will be done by IT Department
√ Users must lock their system when they leave their workstation for any length of time.
√ All unused devices must be switched off outside working hours by the end user.
√ Employees must ensure the physical security of the device. Also ensure protection is taken for data or information stored on the device. Employees must inform IT team for any data backup that might be required.
√ Employees are required to ensure that the sticker for MS Office or Operating system on the Laptop needs to be kept in proper condition for any external audit and is not removed or scratched as original license key information is stored on the sticker.
√ Employees are required to fill suitable IT Equipment forms while joining/exiting which is available with IT Department
√ Company's confidential data/ information must not be copied on any device or shared with anyone outside of the Company like vendors/guests, without authorization, at any time.

Information Technology Services

JAIPUR RUGS IT Unit will provide any IT related services including the following:

- Software & Hardware issues
- PC/Laptop installation, configuration and maintenance
- Printer support
- Internet related issues
- Connectivity issues
- Intranet portal support
- Phone related issues
- Network configuration and management

General Guidelines

- It is the responsibility of the users to comply with all policies and procedures, set in relation to the use of IT assets.
- When traveling, laptop/notebooks or smart phone must be stored securely and should be carried as hand luggage. Ensure they are not left unattended in public places
- If the laptop is lost or stolen it must be reported to the IT Department immediately. Theft or loss off such company property should also be reported to local police & a copy of FIR must be shared with I.T. department.
- If laptop is provided, employee will not be entitled to Desk top
- It is the responsibility of the IT department to take back up of the data on periodic intervals
- The IT assets may be used for processing and storing personal data with approval of reporting manager. The company accepts no responsibility if personal data is deleted or corrupted while the laptop/notebook is being repaired or serviced by the I.T. Department.

- Issue of Accessories- Accessories like carry bag, Monitor and external mouse may be issued based upon requirement.

I.T. Department

- It is the responsibility of I.T. Department to decide on the configuration/version of the IT assets based on the job requirement in consultation with Functional Head.
- The serviceability and shelf life of the asset will be determined by IT department and its decision will be final.
- IT Department will allocate IT assets to users based on need assessments and criticality of the job role, guided by its own Asset allocation policy.

Company's right to Inspect Data

All data and software held by the company in any of the IT assets including company mobile phones may be inspected by authorized staff at any time, without prior notice. Users will be asked to remove software and/or data which are found to be inappropriate by the CTO.

Returning of IT assets

- On resigning, it is the responsibility of employee to return the IT asset to IT department at corporate office/authorized representative of IT department in Branch/regional offices.
- IT department will make the necessary changes in asset register
- HR Department shall inform IT department of all exiting employees well in advance so that IT department can either decide for collect the asset or reallocate the asset to another employee. Disposal of IT asset will solely be at the discretion of IT department.
- Exiting employee shall take clearance from IT department before full and final settlement can be processed
- HR department will not process Full and final settlement of the exiting employee till the time clearance is received by IT department. In case of inordinate delay in returning the asset, company has the right to recover full purchase price of the IT asset from the employee's full and final settlement.
- Standard life of laptop would be 4 years. After 4 years, it can be replaced with new laptop and the old laptop can be transferred to employee if he wished to buy the same at 15% of the original purchase price. However, this is subject to approval of Head IT.

Help Desk Assistance

In case an employee requires any IT end-user support, problem solving, training or assistance and follow-up of ANY KIND and at ANY POINT they are required to contact the IT Support by email on itsupport@jaipurrugs.com