Rushil Décor Limited

Information Technology Policy and Procedure

Version no 1

September 2022

About the Information Technology Policy

RDL IT Dept. provides and maintains technological products, services and facilities like Laptops/ Desktops, Tablets, Cell Phones, servers, telephones, Printers, Internet and application software to employees for official use. The Information Technology (IT) Policy of the organization defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the employees pertaining to technological assets and services used for office work.

Purchase

IT Dept. will assist the Purchase Dept. while evaluating best and most cost-effective hardware or software to be purchased for a particular dept./project/purpose based on the requirement. The IT Dept. will also make sure all hardware/software standards defined in the IT Policy are enforced during such purchases.

Compliance

1. All employees are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the organization.
2. Any employee who notices misuse or improper use of equipment or software within the organization must inform his/her Dept. Head immediately.
3. Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the Management of the organization.

Employee Training

1. Basic IT training and guidance is provided to all new employees about using and maintaining their Laptop/ Desktop, peripheral devices and equipment in the organization, accessing the organization network and using application software.
2. Employees can request and/or the Management can decide to conduct an IT training on a regular or requirement basis.

IT Support

1. Employees may need hardware/software installations or may face technological issues which cannot be resolved on their own. Employees are expected to get help from the IT Dept.
2. For the sake of quick understanding, employees are expected to provide details of their issue or help required by Email or via phone.
3. For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all employees to inform the IT Dept.
4. For any damage to Laptop/ Computers, Cell Phone or other asset approval from Head of Dept. would be required for any replacements.

5. After reporting issue via email or phone, employees should expect a reply from the IT Dept. as early as possible. The IT Dept. may ask the employee to deposit the problematic equipment to the IT Dept. for checking and will inform the timeline for repair/maintenance/troubleshooting/installations or the required work.
6. If there is no response, then the IT Dept. Designated Staff should be asked for an explanation for the delay. If no response is obtained in 1 working day, a complaint can be raised through an email to the employee's Head of Dept. and IT Dept. Designated Staff.
7. Issues will be resolved on a First-Come-First-Served basis. However, the priority can be changed on request at the sole discretion of the designated team in IT Dept.
8. Issues will be prioritized on the basis of high, medium and low category.

Equipment Usage Policy

Equipment Purchase

The following equipment is purchased by the organization and provided to individual employees, departments or projects for their official use.

a. Personal Computing Devices (Desktop, Laptop, Tablet)
b. Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker etc.)
c. Networking Equipment & Supplies (Router, Switch, Antenna, Wiring, etc.)
d. Cell phones
e. Biometric Devices

Equipment Allocation, De-allocation & Relocation

Allocation of Assets:

a. New Employees may be allocated a personal computer (desktop or laptop) for office work on the Day of Joining, as per work requirement.
b. If required, employees can request their Head of Dept. for additional equipment or supplies like external keyboard, mouse etc.
c. Allocation of additional assets to an employee is at the sole discretion of the Head of Dept.
d. No employee is allowed to carry official electronic devices out of office without permission from Head of Dept. In such case a written communication should be sent to IT department.

De-allocation of Assets:

a. It is the Head of Dept.'s responsibility to collect all allocated organizational equipment & other assets from an employee who is leaving the organization.
b. The received assets must be returned back to the IT. Dept.
c. In such case a No-Objection/ No Due Certificate shall be issued by respective HODs and HR Department notifying the IT department.

Equipment Usage, Maintenance and Security

1. It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.
2. Proper guidelines or safety information must be obtained from designated staff in the IT Dept. before operating any equipment for the first time.
3. Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the designated staff in IT Dept.
4. Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.
5. If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from your Head of Dept. is required for the same. The malfunctioning device needs to be submitted to the IT Dept. for checking, maintenance or repair. The IT Dept. staff person will give a time estimate for repair/maintenance.
6. The Head of Dept. can be informed about excessive delay or dissatisfaction about the repair or maintenance performed by the IT Dept. The issue will then be resolved by the Head of Dept in consultation with the IT Head. The Management can be consulted in terms of serious disputes or unresolved issues.

Phone Usage Policy

1. Landline phone systems are installed in the organization's offices to communicate internally with other employees and make external calls.
2. The landline phones should be strictly used to conduct official work only. As far as possible, no personal calls should be made using landline phones owned by the organization.
3. Long distance and ISD calls should be made after careful consideration since they incur significant costs to the organization.
4. The IT Dept. is responsible for maintaining telephone connections in offices. For any problems related to telephones, they should be contacted.
5. Employees should remember to follow telephone etiquette and be courteous while representing themselves and the organization using the organization's phone services.

Laptop/ Desktop Standards

Objective

The main aim of this policy is to maintain standard configurations of laptop/ desktop hardware and software purchased by the organization and provided to employees for official work. The hardware standards will help maintain optimum work productivity, computer health & security and provide timely and effective support in troubleshooting laptop/ desktop problems. The software standards will ensure better system administration, effective tracking of software licenses and efficient technical support.

General Guidelines

1. It is the responsibility of the IT Dept. to establish and maintain standard configurations of hardware and software for laptops/ desktops owned by the organization. The standard, can however, be modified at any point in time as required by the IT Dept. Head in consultation with the Management.
2. Multiple configurations are maintained as per the different requirements of various departments and projects in the organization, in consultation with the Dept.

Network Access

1. All laptops/ desktops being used in the organization are enabled to connect to the organization's Local Area Network as well as the Internet.
2. Network security is enabled in all laptops/ desktops through Firewall.
3. Employees are expected to undertake appropriate security measures as enlisted in the IT Policy.

Data Storage Procedure

Data Storage is setup during installation of Operating System in a Laptop/ Desktop. As an additional security measure, it is advised that employees keep important official data in network drive only. We have a file server for backing up data of all employees. All employees are expected to keep official data on the file system.

Employee's Head of Dept., the Management and IT Dept. will have access to that data in file server.

All employees will login to the file server through given user ID and password.

Server Data backup:

IT Dept. is maintaining an incremental backup of file server with at least 3 copies a day and ERP &Tally servers one day backup it's available till past 3 months.

Antivirus Software

1. Approved licensed antivirus software is installed on all laptops/ desktops owned by the organization.
2. Employees are expected to make sure their Antivirus is updated regularly. The IT Dept. should be informed if the Antivirus related issues if not updated or not working.
3. Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.
4. As per policy IT Dept. has blocked pen drive or USB hard disk access in some users.

Internet Usage Policy

Objective

The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the employees.

General Guidelines

1. Internet is a paid resource and therefore shall be used only for office work.
2. The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
3. The IT dept. has systems in place to monitor each email sent or received.
4. The organization has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.
5. Organization provided mobiles and SIM cards having data plans. Kindly use it for official purpose only. Total GB usage intimation provided via SMS at the usage of 80% by the mobile company. Over usage of Internet may be cause to high billing and it will be bared by user. If you have requirement of more GB data plan other than your current plan, you have to inform your Head of Dept. for increase it via Email only.

Internet Usage Guidelines

1. All employees' laptops/ desktop provided with internet connection for official usage.
2. An employee can also get a local static IP address for internet and intranet use. All employees will be responsible for the internet usage through this local static IP.
3. A visitor or guest user who wants to use the office Internet will be given by IT Dept. with the permission of Dept. head.

Password Guidelines

The following password guidelines can be followed to ensure maximum password safety.

Select a Good Password:

a. Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.).
b. Use 8 or more characters.
c. Use at least one numeric and one special character apart from letters.
d. Combine multiple unrelated words to make a password.

Keep your Password Safe:

a) Do not share your password with anyone.
b) Make sure no one is observing you while you enter your password.
c) As far as possible, do not write down your password. If you want to write it down, do no display it in a publicly visible area.

Other Security Measures:

a. Ensure your computer is reasonably secure in your absence.
b. Lock your monitor screen, log out or turn off your laptop/ desktop when not at desk.
c. In Employees absence Laptop/ Desktop password must be share with Head of Dept.

Online Content Usage Guidelines

1. Employees are solely responsible for the content accessed and downloaded using Internet facility in the office
2. During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.
3. Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.
4. Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

Inappropriate Use

The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the Management as deemed fit.

Any disciplinary action considered appropriate by the Management (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

1. Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
2. Downloading images, videos and documents unless required to official work
3. Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work
4. Accessing pirated software, tools or data using the official network or systems
5. Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee
6. Engaging in any criminal or illegal activity or violating law
7. Invading privacy of coworkers
8. Using the Internet for personal financial gain or for conducting personal business
9. Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
10. Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation.

Email Policy

Objective

This policy provides information about acceptable usage, ownership, confidentiality and security while using electronic messaging systems platforms provided or approved by the organization. The policy applies to all electronic messages sent or received via the above mentioned messaging systems platforms by all official employees of the organization.

General Guidelines

1. The organization reserves the right to approve or disapprove which electronic messaging systems platforms would be used for official purposes. It is strictly advised to use the pre-approved messaging systems and platforms for office use only.
2. An employee who, upon joining the organization, is provided with an official email address should use it for official purposes only.
3. Any email security breach must be notified to the IT Dept. immediately.
4. Upon termination, resignation or retirement from the organization, the organization will deny all access to electronic messaging platforms owned/provided by the organization.
5. All messages composed and/or sent using the pre-approved messaging systems and platforms need to comply with the company policies of acceptable communication.
6. Electronic mails should be sent after careful consideration since they are inadequate in conveying the mood and context of the situation or sender and might be interpreted wrongly.
7. All email signatures must have appropriate designations of employees and must be in the format approved by the Management.
8. Email Password are not shared with any employees.
9. Whenever a new employee has joined the designated email will be configured in their respective desktops or laptops.
10. In special cases if an employee requires their email to be configured on their mobile phone special approval from the top management shall be require in writing.

Ownership

1. The official electronic messaging system used by the organization is the property of the organization and not the employee. All emails and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the organization
2. IT Dept. can change the email system password and monitor email usage of any employee for security purposes as per instruction by Management.

Confidentiality

1. Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the Head of Dept. and/or the Management.
2. Caution and proper judgment should be used to decide whether to deliver a message in person, on phone or via email/electronic messaging systems.

3. Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

Email Security

Anti-Virus:

a. Anti-virus software pre-approved by the IT Dept. is installed in the laptop/desktop provided to a new employee after joining the organization.
b. All employees in the organization are expected to make sure they have anti-virus software installed in their laptops/desktops (personal or official) used for office work.
c. IT Dept. bear responsibility for providing, installing, updating and maintaining records for one anti-virus per employee at a time for the official laptop/ desktop provided by the organization.
d. Employees are prohibited from disabling the anti-virus software on organization- provided laptops/desktops.
e. Employees should make sure their anti-virus is regularly updated and not out of date.

Safe Email Usage: Following precautions must be taken to maintain email security:

a) Do not to open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
b) In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.

Inappropriate Use

1. Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.
2. Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views.
3. Spam/ bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

Software Usage Policy

Objective

The Software Usage Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization-owned computers.

General Guidelines

1. Third-party software (free as well as purchased) required for day-to-day work will be pre- installed onto all company systems before handing them over to employees. A designated person in the IT Dept. can be contacted to add to/delete from the list of pre-installed software on organizational computers.
2. No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Dept.
3. To request installation of software onto a laptop/ desktop, an employee needs to send a written request via email to IT Dept.
4. Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

Compliance

1. No employee is allowed to install pirated software on official computing systems.
2. Software purchased by the organization or installed on organizational computer systems must be used within the terms of its license agreement.
3. Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the organization is strictly prohibited. Any such act will be subject to strict disciplinary action.
4. Any employee who notices misuse or improper use of software within the organization must inform his/her Head of the Dept.

Software Registration

1. Software licensed or purchased by the organization must be registered in the name of the organization with the Job Role or Department in which it will be used and not in the name of an individual.
2. After proper registration, the software may be installed as per the Software Usage Policy of the organization.
3. After installation, all original installation media (CDs, DVDs, and Pen Drive etc.) must be safely stored in a designated location at the IT Dept.

Software Audit

1. The IT Dept. will conduct periodic audit of software installed in all company-owned systems to make sure all compliances are being met.
2. Prior notice may or may not be provided by the IT Dept. before conducting the Software Audit.

3. During this audit, the IT Dept. will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes or personal data.
4. The full cooperation of all employees is required during such audits.

Printer Usage Policy

1) Think before you print: It is simply too easy to push the print-button. For example, much paper is wasted by printing out single line emails or printing out unnecessary copies of documents.
2) Printers are for official usage only. Do not take personal print outs from organization printer.
3) Think twice if you really need to print – if it is necessary to print make sure you print on both sides (duplex). This is a really easy way to reduce paper consumption by half.

Work from Home Policy

1) This is the most basic, but by no means the only step should you take to secure our company's files. Your laptop must be having Antivirus with latest update patch. You can check it at the right side bottom of the screen.
2) Don't allow family members to use your work devices. Treat your work-issued laptop, mobile device and sensitive data as if you were sitting in a physical office location. This will help you continuously associate your actions with a security-first and data-aware mentality in mind. If you think of your laptop and mobile devices as work-only assets, it makes it far easier to control access to sensitive data.
3) Keep your physical workspace secure. While virtual security is important, it's equally important to make sure that your home working space is physically secure. Like: Use laptops on proper table and chair like our office environment. Do not use laptops on Dining table, sofas and on the floor. Its help us it from physical damage of devices with water, food and dust. Lock or shutdown laptop while not using or at the time of taking break.
4) Follow company policies and as per IT guidelines we have to follow rules and safety tips working remotely. Report any suspicious behavior to IT team immediately. Scan your laptop with antivirus regularly.
5) Use a centralized, company-approved storage for our all files. Make sure you are using and saving your files on our server only. It helps us to backup and secure your work. Do not use personal pen drives as it may contains virus and malwares. As per IP policy IT Dept. have blocked usage of pen drive for most of the laptops for security reason but please avoid personal or non-official pen drives and UBS Hard drives.
6) Any IT assets damages or misplace; user is responsible for it. Please Take care of Laptop, Cellphone or chargers while working from Home.
7) If user is bringing any physical office files at home for working; it is users responsibility to take care of it and after completion of work put it back to office at proper place.

Cyber Security

The purpose of this policy is to establish the guidelines and standards for ensuring the security and confidentiality of the data and systems of our organization. This policy applies to all employees, consultants, auditors and guests who access, use, or handle the data and systems of our organization.

Our organization is committed to protecting its data and systems from cyber-attacks by using hardware firewall and antivirus endpoint security solutions. These solutions are designed to prevent unauthorized access, detect malicious activities, and respond to incidents in a timely manner.

Hardware firewall is a device that filters the network traffic between our organization's internal network and the internet. It blocks or allows traffic based on predefined rules and policies. Hardware firewall helps us to protect our network from external threats such as hackers, malware, or denial-of-service attacks (DOS attacks).

Antivirus endpoint security is a software that scans the device for viruses, worms, trojans, ransomware, spyware, or other malware. It also updates itself regularly with the latest virus definitions and patches. Antivirus endpoint security helps us to protect our devices from internal threats such as infected files, phishing emails, or removable media.

All employees, consultants, auditors and guests who access, use, or handle the data and systems of our organization must comply with the following rules and responsibilities:

- Do not disable or tamper with antivirus endpoint security solutions.
- Do not install or use any unauthorized software or hardware on the devices connected to our network.
- Do not share or disclose your login credentials or passwords with anyone.
- Do not access or download any suspicious or inappropriate content from the internet or email.
- If they are using their own device, then it is a must that antivirus software is installed.
- Report any security incidents or breaches to the IT department immediately.

The IT department will review this policy periodically and update it as needed to reflect the changes in technology, regulations, or business needs.

By following this policy, we aim to ensure the security and confidentiality of our data and systems and protect our organization from cyber attacks.