Rajagiri College of Social Sciences, Kalamassery
IT Policies & Guidelines

Table of Contents

Introduction 3
Terminology 3
IT Hardware Installation Policy 4
Who is Primary User 4
What are End User Computer Systems? 4
Warranty & Annual Maintenance Contract 4
Power Connection to Computers and Peripherals 4
Network Cable Connection 5
File and Print Sharing Facilities 5
Shifting Computer from One Location to another 5
Noncompliance 5
Software Installation and Licensing Policy 6
Operating System and its Updating 6
Antivirus Software and its updating 6
Backups of Data 6
Network (Intranet & Internet) Use Policy 7
IP Address Allocation 7
Internet Bandwidth obtained by Other Departments 7
Email Account Use Policy 7

Introduction

Basically the RCSS IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the Institution on the campus. This policy establishes Institution wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the College. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, RCSS took initiative way back in 1990s and established basic network infrastructure in the academic complex of the College. Over the last ten years, not only active users of the network facilities have increased many folds but also the web-based applications have increased.

When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications. When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems. Hence, in order to securing the network, Internet Unit has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway. However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users.

Terminology

IT policies may be classified into following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Database Use Policy

Further, the policies will be applicable at two levels :

- End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
- Network Administrators

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the RCSS IT policy. Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by Rajagiri College of Social Sciences, Kalamassery by any member may even result in disciplinary action against the offender by the authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

- Stake holders on campus or off campus
- Students: UG, PG, Research
- Employees (Permanent/ Temporary/ Contractual)
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Resources

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

IT Hardware Installation Policy

The network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

Who is Primary User

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

What are End User Computer Systems?

Apart from the client PCs used by the users, the College will consider servers not directly administered by INTERNET UNIT, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the INTERNET UNIT, are still considered under this policy as "end-users" computers.

Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably be under comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS

is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

Network Cable Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written intimation to the Central Lab Administration as they maintain a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified.

Noncompliance

RCSS faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole College. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, RCSS IT policy does not allow any pirated/unautho campus network. In case of any such instances, Rajagiri College of Social Sciences, Kalamassery will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

Operating System and its Updating

Individual users who has the privilege to update the software should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

Antivirus Software and its updating

Computer systems used in the college should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Network (Intranet & Internet) Use Policy

Network connectivity provided through the institution, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the Rcss IT Policy. The Communication & Information Services (INTERNET UNIT) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the college's network should be reported to INTERNET UNIT.

IP Address Allocation

Any computer (PC/Server) that will be connected to the college network, should have an IP address assigned by the Lab Administration department. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any Section, department of the college under any research programme/project should ideally be pooled with the college's Internet bandwidth, and be treated as college's common resource.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the College's administrators, it is recommended to utilize the college's e-mail services, for formal College communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal College communications are official notices from the College to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general College messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Impersonating email account of others will be taken as a serious offence under the college IT security policy.