

**Bhilai Institute of Technology,  
Durg CG  
(An Autonomous Institute)**



**IT Policies and Guidelines**

## **TABLE OF CONTENTS**

<b>S.No</b>	<b>Chapter</b>	<b>Page No.</b>
1	Need for IT Policy	3
2	IT Hardware Installation Policy	4
3	Software Installation and Licensing Policy	5
4	Network Use Policy	5
5	Email Account Use Policy	6
6	Website Hosting Policy	6
7	Responsibilities of Central Computing Facility (CCF)	6
8	Video Surveillance Policy	7
9	Firewall Policy	7

## **IT POLICY 2022-23**

### **Need for IT Policy**

IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, faculty, Staff, Management and visiting Guests and Research Fellowship Members.

The IT policy of Bhilai Institute of Technology, Durg (BIT) is formulated-

- To maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established on the campus and provide guidelines on acceptable and unacceptable use of IT resources of the college.
- To establish strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, created, managed, and/or controlled by BIT.
- To support effective organizational security and protect users and IT resources from, but not limited to cyber criminals, bullying, misuse of accounts and assets as well as the spread of malicious software.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information. Due to the policy initiative and academic drives, IT resource utilization in the Campus has grown by leaps and bounds during the last decade.

Further, the policies will be applicable at two levels:

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

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**

BIT 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.

#### **A. 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.

#### **B. What are End User Computer Systems**

Apart from the client PCs used by the users, computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet will be considered as "end-users" computers.

#### **C. Warranty & Annual Maintenance Contract**

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site 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.

#### **D. 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.

#### **E. 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.

#### **F. 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.

### **G. Shifting Computer from One Location to another**

Computer system may be moved from one location to another with prior written intimation to the Central Computing Facility (CCF), as CCF maintains a record of computer identification names and corresponding IP address.

### **H. Noncompliance**

BIT 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.

### **I. Central Computing Facility (CCF)**

CCF upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance.

### **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, BIT IT policy does not allow any pirated/unauthorized software installation in the college campus network. In case of any such instances, BIT will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms. Software installation policy will include-

- A. Operating System and its Updating
- B. Antivirus Software and its updating
- C. Backups of Data

### **Network Use Policy**

Network connectivity provided either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the BIT IT Policy. The CCF is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the college network should be reported to CCF. Network Use Policy will include:

- IP Address Allocation
- DHCP and Proxy Configuration by Individual Departments /Sections/ Users
- Running Network Services on the Servers
- Dial-up/Broadband Connections
- Wireless Local Area Networks

### **Email Account Use Policy**

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and BIT administrators, it is recommended to utilize the organization's e-mail services, for formal organization 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. For obtaining the institution's email account, user may contact Head of Department for email account and default password by submitting an application in a prescribed proforma.

### **Website Hosting Policy**

Departments, Cells, central facilities may have pages on BIT's official Web Site. As on date, the IT cell is responsible for maintaining the official web site of the institute viz., <http://bitdur.ac.in>. IT cell is responsible to send updated information time to time about their Web pages.

### **Responsibilities of CCF**

The campus network backbone and its active components are administered, maintained and controlled by CCF. CCF operates the campus network backbone such that service levels are maintained as required by the departments and divisions served by the campus network backbone within the constraints of operational best practices. The responsibilities and authorization of the CCF are as follows:

- Physical connectivity of campus buildings already connected to the campus network and newly constructed buildings to the "backbone" is the responsibility of CCF.
- CCF will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone. Major network expansion is also the responsibility of CCF.
- Where access through Fiber Optic/UTP cables is not feasible, in such locations CCF considers providing network connection through wireless connectivity.
- CCF is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.
- CCF provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the college upon receiving the requests from the individuals on prescribed proforma. The campus network and Internet facilities are available 24 hours a day, 7 days a week.
- All network failures and excess utilization are reported to the CCF technical staff for problem resolution. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, CCF will analyze the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a report will be sent to higher authorities in case the offences are of very serious nature.

- CCF is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.
- CCF may receive complaints of the network related problems. Such complaints should be by email/phone.
- CCF will be responsible only for solving the network related problems or services related to the network.
- CCF will be constrained to disconnect any Section, department, or division from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy.

### **Video Surveillance Policy**

- The system comprises: Fixed position cameras; Monitors; digital video recorders; Storage; Public information signs.
- Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings.
- No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
- Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera installation is in use.
- Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

### **Firewall Policy**

A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies. This section provides details on what types of traffic should be blocked.

#### **Policies Based on IP Addresses and Protocols**

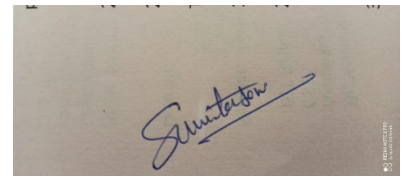
Firewall policies should only allow necessary IP protocols through. Examples of commonly used IP protocols, with their IP protocol numbers,<sup>17</sup> are ICMP (1), TCP (6), and UDP (17). Other IP protocols, such as IPsec components Encapsulating Security Payload (ESP) (50) and authentication Header (AH)(51) and routing protocols, may also need to pass through firewalls. These necessary protocols should be restricted whenever possible to the specific hosts and networks within the organization with a need to use them. By permitting only necessary protocols, all unnecessary IP protocols are denied by default.

## **Policies Based on Applications**

The application-based approach provides an additional layer of security for incoming traffic by validating some of the traffic before it reaches the desired server. An application firewall or proxy also prevents the server from having direct access to the outside network.

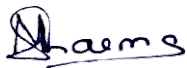
## **Disclaimer –**

**The entire IT infrastructure of BIT, Durg is for ethical use and solely for Academic. For anykind of misuse in unethical manner by any user, neither the Internet Service provider nor the BIT management will be responsible and only the concern user will be solely responsible and liable to punished under Indian IT Act.**



**DrSunitaSoni**

**Dean( ITDeveloment)**



**Dr. Manisha Sharma**  
Vice Principal



**Dr. M.K. Gupta**  
Principal



**Dr. Arun Arora**  
Director