

CIMR has an IT policy covering Wi-Fi, Firewall etc. and allocated budget for updating its IT facilities for the users.

The IT policies are applicable to Staff, Students, Faculty members and Visitors. Institute have framed various policies like Installation of Hardware, Network and software.

### Objective

The objective of this policy is to ensure proper access to and usage of CIMR's IT resources and prevent their misuse by the users. Use of resources provided by CIMR implies the user's agreement to be governed by this policy.

- This IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the institute on the campus.
- This policy establishes rules and responsibilities for protecting the Confidentiality, Integrity, and availability of the information assets that are accessed, created, managed, and/or controlled by the institute.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents.

### Scope

Policy covers areas like Wi-Fi access, Internet access policy, Cyber security etc. which is updated or amended whenever required as per the need of the institute.

### Email Account Usage Policy

CIMR provides official email access privileges to its Students, faculty members and all Admin staff members. In an effort to handle the efficient information dissemination among the administration, faculty members, staffs and students, it is recommended to avail official email with CIMR domain

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

User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.



Impersonating email account of others will be taken as a serious offence under the IT security policy.

Certain violations of IT policy by any member may even result in disciplinary action against the offender by institute authorities.

### IT facilities upgradation

Institute upgrade its IT facilities as per the requirements. Institute's regularly upgrading its infrastructure covering Wi-Fi, cyber security, software upgradation, ERP system, ICT enabled teaching learning.

CIMR has the annual budget for upgradation of IT facilities and Infrastructure maintenance:

1. Internet connectivity has been upgraded from 200 Mbps to 300 Mbps from Tata Tele services pvt ltd.
2. Students and faculty members get maximum benefits to access internet through Wi-Fi routers which are installed and maintained on regular basis.
3. Firewall has been upgraded from Cyberoam 300ing to high end features firewall Upgraded to Sophos XG
5. Institute has installed CCTV across the campus covering all areas of the institute.

### Security and DATA Backup policy

- User shall take prior approval from the IT team to connect any access device to the CIMR network.
- User shall keep their passwords secure and not share their account details.
- User shall report any loss of data or accessories to the IT Team and authority of CIMR
- User shall obtain authorization from the competent authority before taking any CIMR issued desktop outside the premises of the institute.
- Users shall properly shut down the systems before leaving the office/ department.
- Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.
- Though students are responsible for their own data as per the notices displayed in the department, Back up of staff data is stored on the File Server on Google Drive and NAS.
- Google Backup has been installed on the desktops.



*Nandita Mishra*  
7/2/2022

Information of the upgradation

Sl No.	Particulars	Previous Status	Present Status
1.	Bandwidth	200 MBPS	300 MBPS
2.	Wi-Fi Router	16	6
3.	Firewall	Cyberoam	Upgraded to Sophos XG
4.	Laptops	Classroom Laptops i3 Processor, with 4 GB RAM 500 GB HDD	i3 Processor, with 16 GB RAM & 128 GB SSD + 500 GB HDD
5	Desktops	I3, 4GB RAM, 500 GB HDD	Core i3, 16 GB RAM and 256 GB SSD for ACER Desktops
6.	CCTV		Yes

## IT Policy for Students

### Computer Lab

CIMR boasts of an excellent IT infrastructure that supports its pedagogy of out-of-class learning. The Computer Lab services the IT needs of the Institute and is equipped with state of the art networking peripherals

### Computer Lab Rules & Regulations

- Students are not allowed to enter in the Lab without ID-Card around the neck.
- Students are required to register their name, time in and time out.
- No discussion is allowed in the Lab. Students are to maintain silence in the Lab.
- No cell phone calls are allowed in computer lab at any time.
- Students must step outside the computer lab to attend/make a phone call.
- Students are required to put their mobile phones on silent mode before entering into the lab.
- Students are not allowed to eat / carry any eatables in the lab.
- No user will be allowed to download software / songs / videos And / or any non-academic material.
- No user will be allowed to use computer system for any non-academic use.
- While leaving the Lab, users are required to arrange the chairs properly, if disarranged during usage.
- Users are not allowed to save their work on any of the local hard drives. The computers are automatically cleaned and unauthorized files, directories and programs are routinely deleted. Users must save on their space provided in the server.
- Failure to adhere to the above would result in usage defaulting. Defaulter's account will be blocked immediately and a fine Rs. 100/-will be imposed

*IT Department is not responsible for items left in computer labs or the loss of documents / files due to power failures, Computer hardware / software failures, network difficulties, and / or users not periodically saving their work.*



*Nandkishor*  
*8/2/2022*