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 the 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 l 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.

Nandita Mishra

CHETANA INSTITUTE OF MANAGEMENT AND RESEARCH
BANDRA (E), MUMBAI-51. (INDIA)

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 l 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.

An employee should not misuse a password, access a file or retrieve a stored communication that is not normally accessible to that employee.

Access may be provided to employees for subscribed online software and resources. All data contained therein is property of the Institute and therefore may not be misused communicated, handed over or passed on in any format and form.

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, ICT enabled teaching learning.

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

1. Internet connectivity has been upgraded from 300 Mbps to 500 Mbps from Tata Tele Services Pvt Ltd.

2. Students and faculty members get maximum benefits to access the internet through Wi-Fi routers, which are installed and maintained regularly.

3. Firewall has been upgraded from Sophos XG to FortiGate FG200G
5. The 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 the 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, Backup of staff data is stored on the File Server on Google Drive and NAS.
- Google Backup has been installed on the desktops.

IT Policy for all the users including IT Staff

The IT policies are applicable to all the Staff members including IT 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.

CHETANA INSTITUTE OF MANAGEMENT AND RESEARCH
BANDRA (E). MUMBAI-51. (INDIA)

Email Account Usage Policy

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

In an effort to increase the efficient distribution of l 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.

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

An employee should not misuse a password, access a file or retrieve a stored communication that is not normally accessible to that employee.

Access may be provided to employees for subscribed online software and resources. All data contained therein is property of the Institute and therefore may not be misused communicated, handed over or passed on in any format and form.

Chetana's
Institute of Management & Research
AICTE New Delhi Approved & ISO 21001 : 2018 Certified

CIMR Data Backup Policy and Internet Connectivity

We have upgraded to Sophos from Cyberoam Firewall Policy	Application of FortiGate FG200G firewall at the Institute All incoming connections are blocked at this device. The Internet connection is shared with the users through this firewall. Internet Access Restrictions are applied as per the group of users.
Wi-fi details	The campus is Wi-Fi
Internet Speed	500 Mbps from Tata Tele business services
DATA Backup policy	As per the notices in the Lab, the users are responsible for their own data. Still, we take backup of staff's data stored on our File Server on Google Drive, and NAS. Google Backup has been installed on most of the staff's desktops and trained them on how it works.

CHETANA INSTITUTE OF MANAGEMENT AND RESEARCH
BANDRA (E). MUMBAI-51. (INDIA)

Information on the upgradation

Sl No.	Particulars	Previous Status	Present Status
1.	Bandwidth	300 MBPS	500 MBPS
2.	Wi-Fi Access Point	18	21
3.	Firewall	Sophos XG	Upgraded to FortiGate FG200G
4.	Laptops	i3 Processor, with 16 GB RAM & 128 GB SSD + 500 GB HDD	Intel Core i5-13420H Processor 2.1 GHz, 12 MB Cache, 8 GB DDR5, 512 GB SSD
	Desktops	Core i3, 16 GB RAM and 256 GB SSD for ACER Desktops	ASUS Expertcentre Desktop D500MD 16 GB/256 GB SSD
5.	CCTV		Yes

Computer Lab Rules and Regulations

- Students are not allowed to enter the Lab without an 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 the 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 / any carry any eatables in the lab.
- No user will be allowed to download software/songs/videos / and/or any non-academic material.
- 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 on the server.
- Failure to adhere to the above would result in the usage defaulting. Defaulter's account will be blocked immediately, and a fine of Rs. 100/- will be imposed.

IT Department is not responsible for items left in the 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.

CHETANA INSTITUTE OF MANAGEMENT AND RESEARCH
BANDRA (E), MUMBAI-51. (INDIA)