

Maintenance Policy

The Maintenance Policy for CMR University outlines the guidelines and procedures for construction of new infrastructure, maintenance and utilization of the present infrastructural assets of the University, the facilities, and equipment. The document covers the objectives, strategies and procedures for maintenance and utilization planning and execution, and the roles and responsibilities of the maintenance team.

1. Objective:

The primary objective of repair and maintenance is to ensure that all the assets of the University (eg., buildings, classrooms, laboratories), facilities (hostels, library, sports fields, gymnasium etc.), and equipment are kept in good condition and are operational at all times through regular and timely maintenance. This would provide a safe, functional and comfortable atmosphere for the students, faculty, and staff of the University.

The policy document establishes clear guidelines and procedures for maintaining and utilizing equipment, facilities and other assets.

2. Scope:

The policy shall include the following:

- a) Campus development and construction of new buildings and infrastructure
- b) Maintenance, repair and utilization of existing classrooms, furniture and laboratories
- c) Maintenance & utilization of other physical facilities
- d) Maintenance & utilization of sports facilities and equipment
- e) Maintenance & utilization of library and library resources
- f) Maintenance & utilization of hostels
- g) Housekeeping and Maintenance of campus cleanliness
- h) Allied and incidental maintenance

3. Strategies for Maintenance & Utilization

All maintenance work is categorized into annual maintenance, routine maintenance, preventive maintenance and complaints/requests from departments, hostels, offices etc.

- (a) Annual maintenance: Annual maintenance refers to scheduled maintenance activities that are performed once a year to ensure the proper functioning and longevity of equipment, machinery, or systems. Such activities should be funded through the annual budget. Equipment such as generators, air conditioners, firefighting equipment, water purification RO equipment, vehicles all come under the category where annual maintenance is required.
- (b) Routine maintenance: Routine maintenance refers to cleaning of assets, repair or replacement of components of equipment performed on a regular/periodic basis (intervals shorter than a year) to ensure systems operate at peak efficiency and prevent its failure. Routine maintenance includes daily cleaning jobs, periodic maintenance of equipment etc.
- (c) Preventive maintenance: Preventive maintenance refers to periodic inspection, replacement of components and cleaning done to keep equipment and assets operating at desired level and reduce occurrence of breakdowns.
- (d) Complaints received from stakeholders: Corrective action is to be taken in case of complaints are received from departments, hostels, offices and other units.

4. Roles and responsibilities

The following are the roles and responsibilities of the personnel involved in the maintenance process:

- (a) The Campus Managers of the university shall have the overall responsibility of ensuring the compliance of the Maintenance Policy. The Campus Manager shall be in-charge of coordinating all building, renovation, and maintenance related activities. The responsibility of overseeing and monitoring the maintenance of academic buildings, offices, classrooms, laboratories, and all other physical and infrastructural facilities shall lie with the Campus Manager.
- (b) The maintenance work will be carried out under the direct supervision of Engineering Department of the University.
- (c) The maintenance section of the university will have dedicated support staff for civil, mechanical and electrical maintenance.

- (d) All proposals for construction and maintenance of assets in the departments/facilities/hostels shall be the responsibility of Heads of Department, Lab In- charges, Coordinators/In-charges of the facilities and Hostel Wardens.

5. Construction and Maintenance of Assets

a) Campus development and construction of new buildings and infrastructure

All proposals for construction of new buildings, extensions and renovations of existing buildings shall be initiated by the concerned heads of the Departments after providing suitable justification. This may then be placed before the Chancellor / Pro Chancellor through Registrar and Vice Chancellor for approvals. The sanction for new construction and renovation of university infrastructure shall be given by the Board of Governors of the University.

b) Maintenance, repair and utilization of existing classrooms, furniture, and laboratories

- All the departments of the University have classrooms with interactive panels and LCD projectors, along with green/white boards and adequate furniture as per student capacity.
- The classrooms in the academic buildings have furniture, and teaching aids and electrical fixtures. The laboratories have state of the art equipment for curriculum-based laboratory courses and research. The classrooms shall be used for lectures and tutorial classes and for holding examinations.
- The Campus Manager shall have a Central Stock Register for maintaining the stock of all items purchased in the University (furniture, laboratory equipment etc.) and then the items shall be issued to the departments. Stock registers are to be maintained in each department for keeping a record of all non-consumable and consumable items issued to the department.
- The Heads of Departments shall ensure proper maintenance and utilization of classrooms, seminar halls, equipment and furniture.
- The classrooms shall be optimally utilized according to the timetable prepared by the Heads of Department and uploaded on the Academic Monitoring Services Portal. The requests for maintenance of furniture and electrical repairs shall be made by the Heads of Department to the Campus Managers, who shall undertake the maintenance process.

- The laboratories shall be maintained by the respective department laboratory assistants and technical staff and supervised by the respective Head of the Department. They shall also monitor effective utilization of the laboratories. The laboratories with state-of-the-art equipment shall be used for conducting lab sessions, practical exams, and research under the supervision of faculty members and lab assistants.
- Breakage and need for repair shall be reported to the Heads of Department and suitable measures shall be taken for speedy functioning of the equipment. Minor repairs required for laboratory equipment shall be undertaken on priority basis by the department using funds issued as impress money. For major repair works, the Heads of Departments shall report to the Campus Manager who will carry out the repair from competent agencies after proper permission from authorities.
- The general cleanliness of the classrooms and office rooms shall be carried out by a housekeeping team appointed by the University.

c) Maintenance and utilization of other physical facilities

- The overall maintenance of physical facilities such as the auditorium, multi-purpose hall, administrative buildings, stadiums, playgrounds, guest houses, roads, gardens etc shall be the responsibility of the Campus Managers and carried out under his supervision.
- All civil and electrical repair/service/works shall be carried out under the overall supervision of Engineering Department of the University and other technical staff.
- Periodical preventive measures for the maintenance of the buildings, painting, and white- washing of buildings, rectifying leakages and blockages in pipe lines to provide uninterrupted water supply to the entire campus, maintenance of generator and other electrical works such as frayed wiring and overloaded circuits, cleaning of roof top water tanks, replacing fire- extinguishers, and ensuring a clean environment in the whole campus shall be carried out with the support of technical and housekeeping staff.
- Regular monitoring of fire safety measures, water purifying RO units and provisions for physically challenged shall be undertaken.
- Annual maintenance of air-conditioning units in administrative office buildings, auditorium, and seminar halls shall be undertaken to ensure effective and efficient service.

- Transport facilities and all vehicles of the University shall be monitored and maintained under the supervision of the Campus Manager.

d) Maintenance and utilization of sports facilities and equipment

- Sports & fitness equipment and other facilities shall be supervised and managed by the Secretary, University Sports Council and Head, Department of Physical Education.
- All the facilities as like Stadium, basketball courts, gymnasium, and playgrounds shall be maintained with the help of multitasking employees on a regular basis with thorough maintenance being carried out during vacations. Expensive fitness equipment in the gymnasium shall be maintained through Annual Maintenance Contract with the manufacturer or suitable service provider. Maintenance of the swimming pool shall be carried out by specialized workers under the supervision of the Physical Education Department.
- The sports facilities including the running track shall be open for use of students, faculty and staff of the University as per the timings decided by the Physical Education Department. Students shall fill out an online registration form for the use of the University play grounds and sports facilities.
- The sports related material shall be issued to students and record of the same shall be maintained in an issue/return register for safekeeping of equipment and optimize the use.

e) Maintenance and utilization of hostels

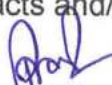
- The hostels provide accommodation to out of station students. The maintenance of the hostels in terms of repair of infrastructural facilities, and regular cleanliness and hygiene is carried out by the Unit Manager in coordination with the wardens of the hostels under the overall supervision of the Hostel Administrator.
- The Wardens of the hostels are responsible for upholding cleanliness and performing minor maintenance tasks within the hostels. They ensure efficient utilization of hostel facilities by students, receiving support from the unit manager and maintenance staff as needed.
- The Warden and Unit Manager of the university will oversee the hostel's overall

functioning and ensure cleanliness, hygiene, and ambiance. It shall be the responsibility of the Warden to look after the general maintenance and cleanliness of the hostel premises including the building, courtyards, and the toilets.

- All hostel maintenance duties shall be handled by the Warden of each hostel, who shall be responsible for collecting all minor maintenance requests and referring them to the Unit Manager.
- Regular cleaning of the hostel premises, washrooms, kitchens, and corridors and rooms shall be undertaken by the housekeeping staff.
- Periodic maintenance of gadgets in the hostel kitchen, overhead water tanks, RO machines etc., shall be carried out by the maintenance staff of the University.
- Request for hostel accommodation may be made through the online portal available on hostel web page. Accommodations shall be provided to eligible students based on the rules as decided by the Wardens of the hostels.

f) Maintenance and utilization of library and library resources

- The library shall remain open from 8:00 AM to 5:00 PM from Monday to Saturday.
- Open bookshelf shelf system, library software system and supporting staff of the library shall help in the search, issue and return of resources for all registered users.
- The Librarian shall be responsible for the overall management and maintenance of the library and the library resources. Library resources shall be used and governed by predefined policies.
- Maintenance of library material involves - stacking, shelf arrangement, cleaning, shelving, stock verification and weeding of unwanted material.
- Records of all library resources shall be maintained by library staff and inventories are to be reviewed annually by a physical review.
- RFID facility is used to register daily physical footfalls and the e- Library app shall be used to record the online footfalls.
- Periodical cleaning and dust removal of the library will be carried out by a cleaning staff dedicated to the library.
- Photocopy machines in the library shall be serviced periodically through Annual Maintenance Contracts and/or call basis.


REGISTRAR
CMR University
2, 3rd 'C' Cross, 6th 'A' Main Road
2nd Block, HRBR Layout
Bangalore - 560 043.

g) Housekeeping, Maintenance of campus cleanliness and Other allied maintenance

- Daily cleaning of the campus premises including roads, sidewalks, parking lots and the academic, and administrative buildings including washrooms shall be carried out by the outsourced housekeeping team.
- In order to ensure proper waste management, adequate number of waste bins shall be placed at strategic locations. Separate bins for dry and wet waste shall be installed.
- The electricity and water supply services shall be maintained by the civil and electrical maintenance staff. They shall carry out periodic maintenance of these facilities in order to ensure uninterrupted supply to the hostels, academic area, and faculty and staff residences.
- Fire-fighting equipment in the academic area, laboratories, offices, and hostels shall be maintained by the Campus Manager.
- Regular pest control and periodic fogging of the campus premises shall be carried out by the Campus Manager.
- To ensure a safe and secure campus, CCTV cameras shall be placed at various places throughout the campus. The surveillance equipment and CCTV cameras shall be monitored by the Security Officer.
- The maintenance of green initiatives such as rainwater harvesting, sewage treatment plants, bio-gas plant, solar panels, plastic free campus and green audits shall be all carried out under the supervision of the Campus Manager.
- Any spare parts or materials required for maintenance will be procured in advance.
- Overall, maintenance of campus cleanliness is essential to create a healthy and welcoming environment for students, faculty, and staff. By implementing a proactive approach to cleaning and waste management, the University shall promote a safe and healthy campus environment


REGISTRAR
CMR University
2, 3rd 'C' Cross, 6th 'A' Main Road
2nd Block, HRBR Layout
Bangalore - 560 043.

Information Technology (IT) Policy

INDEX

S. No	IT Policies & Supportive Content
1	Introduction
2	IT Services Policy
3	Data backup Policy for faculty, staff and students
4	IT Hardware Installation Policy
5	Software Installation and Licensing Policy
6	IT Services helpdesk policy
7	Network (Intranet & Internet) Use Policy
8	Email Account Use Policy
9	Website Hosting Policy
10	University Database Use Policy
11	CCTV Surveillance Policy
12	Data Recovery in case of Disaster
13	Power Backup policy for IT hardware
14	Cyber Security and Data Privacy
15	Network /internet usage policy for Hostel Students
16	ERP User Policy
17	Review and Revision Policy

1. Introduction

Guidelines are created and provided to help organization, departments and individuals who are part of university community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies.

The current IT policy is sub-divided into following:

- IT Services Policy
- Data backup Policy for faculty, staff, students
- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- IT Services helpdesk policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Website Hosting Policy
- University Database Use Policy
- CCTV Surveillance Policy
- Data Recovery in case of disaster
- Power Backup policy for IT hardware
- Cyber Security and Data Privacy
- Review and Revision policy

Further, the policy will be applicable at two levels:

1. End Users Groups (Faculty, Students, Senior administrators, Officers and other staff)
2. Network Administrators

It may be noted that university IT Policy applies to

1. The technology administered by the university centrally or by the individual departments
2. The information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorized resident or non-resident visitors on their own hardware connected to the university network.
3. The resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university recognized Associations/Unions, or hostels and Guest houses, or residences wherever the network facility was provided by the university.

4. 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 university IT policy.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure, must comply with the guidelines. The violation of this IT policy by any university member may result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

2. IT Services Policy

2.1 Objective: IT Services provides a wide range of computing and communication facilities for faculty, staff and students. IT Services has a clear user focus, which is aimed at “providing a high- quality service”, includes

- Ensuring services meet user requirements
- Monitoring the performance of services
- Providing a cost-effective service
- Applying a flexible operation appropriate to the vision of the University
- Providing effective communication and keeping the users informed
- Achieving user satisfaction

2.2 Types of services included: The purpose of this policy is to set out the services provided by IT. The Services IT manages includes:

- Desktop & Laptop computing and support
- Central computer hardware and networks
- IT Strategy and the introduction of new systems
- Day to day operation of existing systems
- Centralized printing facility
- Internet service and support to the end users

A brief summary of the range of services University IT Services is set out below:

2.2.1 IT Helpline: the IT Services Helpline provides a first point of contact to IT Services for most users. Helpline Advisers provide help with a wide range of standard queries and ensure that problems are dealt with. The Helpline also deals with the communications to all staff about service availability for all systems.

2.2.2 Standard Hardware IT Services: Advise and recommend the choice of IT equipment. This includes purchases made with external/research funding. IT Services also co- ordinates ordering of all IT equipment and software to ensure cost-effective investment in IT.

2.2.3 Software and Hardware

2.2.3.1 Systems and software Provision: Staff and faculties are provided with Laptop and Desktop (whichever is applicable) to the respective department/schools for their day-to-day usage. These systems are equipped with licensed OS and software applications. To install any new application or hardware, the end user will have to connect to IT helpdesk.

2.2.3.2 Procurement: University has a centralized procurement body which received new procurement requests from respective schools and departments. It should be approved by Registrar and submitted to the IT team for further processing. The IT team would then evaluate the requirement, design an optimal solution, collect the quotations/proposal through various vendors, partners, OEMs and submit all these in a comprehensive manner to the management to take it further.

2.2.3(a) Important Note: All new bulk procurements should be planned well before the new fiscal year beginning and included in the budgetary requirement of that respective School/department.

2.2.4 Desktop/laptop support (including Audio Visual)

Support for around 2,000 University desktop computers/laptops. Core support includes:

- Installation of relevant software
- The setup of network connections, access to email, network file space and Internet
- Fault diagnosis
- Application of fixes on software and hardware
- Central Computer Hardware and networks

2.2.5 University has various networks i.e. the campus' internet, Intranet, IPBX network and importantly its connection, which interconnects each other.

2.2.6 Servers

Management of the University's core servers housed in specially equipped server with secure Physical Server and Cloud server. Key activities include back-ups, upgrades, patches, and service enhancements. These servers host main University systems, departmental systems, web applications, data and student and staff network file space.

2.2.7 Telecommunications

IT Services are responsible for the management of the University's Telephone systems, which includes all cordless handsets, desk sets and mobile phones.

2.2.8 Peripheral devices and services: University also maintains a university wide printer strategy including deployment, maintenance and service of MFPs & Scanners.

2.2.9 Day to day operation of existing systems

2.2.9.1 Support: Maintaining a wide range of the Universities existing systems to diagnose and fix problems, which arise as well as applying and testing supplier upgrades and patches.

2.2.9.2 Enhancement: Working with the users and suppliers to specify, develop and test changes to existing systems as these arise.

2.2.10 Operational Services

- a. IT Helpline & Problem Resolution
- b. New Username & Password: for Access the University internet and network
- c. New or replacement standard PC
- d. Specialist computer Hardware
- e. Mobile phone or mobile computing device
- f. Specialist computer Software
- g. Desktop software
- h. Network access and Wi-Fi connectivity
- i. Personal Storage
- j. Email Services – Students& staff
- k. Power backup through secure Online UPS facility along with Diesel generator

3.Data backup Policy for faculty, staff and students

3.1 Scope of Procedure and Rationale

The main goal of the data protection strategy is to protect CMRU's data by having it backed up to an alternate location away from where the primary data resides. Electronic backups are a requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, sabotage, ransomware, data entry errors, or system operations errors.

3.2 Technology Used

3.2.1 Duplicate disk-based technology through AWS and NAS is currently used to back up the data of university level systems. The backup solutions reside in the secondary and tertiary backup Server. The primary backup is done using cloud. At pre-defined time intervals as specified in a backup plan, a backup of the live data will be performed to our storage located in the primary Server. This data represents a point in time and is considered backup data.

3.2.2 For most non-critical systems, backup data and the live data constitute the two locations. Data deemed as mission critical may be replicated between locations using our Storage Area Network (SAN) technology. This guarantees that the data resides in at least two locations in a live production mode as well as at the second location as point-in-time backup data.

3.2.3 Active Directory server, through Network Storage and NAS Backup solution is in place and following departments will be using the NAS storage facility:

- Examination team
- Content team
- Accounts Head
- IT team
- Administration

3.2.4 For mission-critical data that requires a higher level of protection, data is replicated to the tertiary backup data centers. The use of a replicated data solution is limited to select university mission critical systems, typically defined as Disaster Level Zero (DR0).

3.3 Service Availability

3.3.1 Backup services are available as a standalone option. Backup services are bundled with storage services. The bundled storage/backup services are primarily done using cloud and a secondary storage/backup is available in datacenter using General NAS server.

3.3.2 The backup service is used for Student records including their admission records, academic details, student login records. The backup of the web activities is also maintained (which are being done using student login). Employee records including their employment details, qualifications, salary records, attendance (presence, absence, leaves (used, remaining), in and out timings)

3.3.3 Faculty records includes their qualification, faculty development programs attended/organized, research work (ongoing/published), e-learning material developed by them. These records are maintained under both the department and school categories.

3.3.4 Administrative staff records are maintained to record their web activities (done using the stafflogin).

3.3.5 The records of all the academic and non-academic activities which include the details of organizing committee, participants, advertising, pictures, videos, financial details are also maintained.

3.4 Guidelines

The purpose of these Guidelines is to establish the rules for the backup of electronic information. These guidelines shall be followed by all individuals responsible for the installation and support of technology resources, individuals charged with technology resources security, and data owners.

3.4.1: ERP, Web site, HRMS are hosted on cloud. All these are SaaS services. There is a provision for backup of all this data over cloud

3.4.2: Secondary backup of ERP data is backed up in Local server at Campus

3.4.3: Biometric servers are hosted locally. Their daily backup is taken into a NAS storage device.

3.4.5: Daily backup of university website is taken on a local server as a secondary protection

3.4.5: All contents developed by inhouse team are stored in a local NAS storage with back up protection and 256-character encryption and protection. This is again backup in the cloud for tertiary protection.

3.4.6: Internet usage is managed by firewall and firewall database back up is taken on a weekly basis and automatically stored into a NAS storage device which backs it up again on a secure Google drive for tertiary protection.

3.4.7: CCTV footage is available for a period for minimum 7 days to maximum days as per regulatory compliances in the DVR/NVR hard disk.

3.5 Responsibilities

Data owners are required to keep the data into defined locations in their devices. Technology resources and data owners are responsible for data backup validation and testing recovery. The end user department/school will have to conduct random audits for their data backup.

4. IT Hardware Installation Policy

4.1 The life of any desktop, laptop, or peripheral at CMR University should be at least three years. Desktop computers, laptops, and peripherals should not be replaced until their minimum life has expired, unless the device encounters malfunctions which cannot be repaired. The Information Technology team is responsible for supervising the acquisition of desktop computers, laptops, and peripherals in the departments.

4.2 No academic or administrative staff member may obtain more than one computer (either desktop or laptop). Devices whose guarantee periods have expired, will be assessed and maintained regularly through preventive maintenance/AMC wherever applicable.

4.3 IT Manager assesses and prepares the reports and plans the replacement of devices annually, at the beginning of each academic year, in consultation with the university fraternity. Applications for replacements that are outside the ordinary replacement cycle are submitted to the IT Manager by School/department Head.

4.4 The replacement applications depend on the following criteria:

1. Expiry of guarantee period.
2. A new technology or a practical need that requires replacement.
3. New technologies or requirements for work.
4. Repeated malfunctions.
5. Budget availability.

4.5 The Manager, Information Technology evaluates and consults specialized sales agents to choose the best national/international brands and quality of model, price, and efficiency that are suitable for university.

4.6 The Manager, Information Technology supervises the purchase and distribution process for desktop computers, laptops, and peripherals in coordination with Procurement team.

4.7 All the desktop and laptop computers are equipped with a preloaded operating system in line with the needs of the different colleges / Schools and departments, after being approved by the Manager of Information Technology.

4.9 The process of replacement and distribution of the devices should be documented.

1. Through Approval letter / Request raised through an email by HR team for the Manager and Above designation
2. Department/School head need to submit approval copy signed by Pro Chancellor for other staffs if the desktop/laptop is required for them
3. Old and defective material should be returned to the IT team in case of replacement
4. The device custodian will have to bear the cost of repair for any physical damage caused due to negligent and wrong handling of device.

4.10 E-waste management is done in accordance with the E- Waste (Management) Rules, 2016 (amendment, 2018) [Government of India], under which it is ensured by the authority that the electronic waste is delivered to authorized recyclers or dismantlers annually after complete documentation is done.

5. Software Installation and Licensing Policy

5.1 Scope of Procedure and Rationale

The purpose of this Policy is

- To underline the importance of compliance with softwarelicensing provisions
- To define specific responsibilities relating to this compliance.

5.2 The specific responsibilities: Responsibility for ensuring software license compliance rests with the Head of Department.

Following are the major responsibilities under this policy:

- Maintain a register to provide proof of purchase of software.
- Maintaining a register of disposal of software through on-sale (for example software sold with a computer).
- Maintaining an inventory detailing where licensed software is installed. This must track redeployment of software within the department.

5.3 In the interests of ensuring compliance with licensing requirements, IT Department from timeto time investigates a software compliance audit.

5.4 To ensure the continuous education of students, the university encourages the usage of

- Open-source software
- Academic licenses of the software
- Virtual labs for conduction of practical
- LMS complier and emulators
- Licensed software
- Swayam and NPTEL for online certifications

6. IT Services helpdesk policy

6.1 IT Team provides a wide variety of technical support to students, faculty and staff to enhance learning through the use of technology. All are mentioned in **Policy 2.1**.

6.2 Hours of Operation: IT support is available Monday to Sunday 8:30 AM – 5:30 PM (excluding holidays)

6.3 Campus Support Request Process

6.3.1 The faculty or coordinators need to call respective campus System Admin in case of any issue in IT infrastructure during the classroom/event/session. The contact numbers are made available to departments time to time.

6.3.2 For all other types of issues which are not related to ongoing event or classroom has to be raised through our [internal ticketing system](#). It is a completely transparent system which gives user the status of ticket and gives notification anytime the ticket status changes. There are basically 3 statuses, 1. Open, 2. Pending for approval 3. Resolved. (Annexure 1 contains the User manual).

6.4 Operational Services

- IT Helpline & Problem Resolution
- New Username & Password: for Access the University internet and network
- New or replacement standard PC
- Specialist computer Hardware
- Mobile phone or mobile computing device
- Specialist computer Software
- Desktop software
- Network access and Wi-Fi connectivity
- Personal Storage
- Email Services – Students & staff

6.5 Services Provided - First line support to staff, students, external customers and partner Universities is available 24 hours a day all year round.

6.6 End-User responsibilities - Provide adequate information in order that a ticket can be logged relating to the nature of the query.

6.7 IT Team monitors all open incidents and escalate unresolved incidents to individuals and groups who can help to resolve the problem. When a problem arises, we will deal with it based on an initial assessment using severity table.

6.8 Service tickets resolution matrix

Help Topic/ Ticket Type	Description	Resolution	Service time (Max)
Classroom and Seminar Hall (with ongoing class or event) IT issues	Projector, screen, sound system etc.	Resolution	Immediately on call by system admins
Internet Issue Wi-Fi	Unable to connect internet, Wi-Fi connected but no internet, less speed, Access credentials not working	Rectification for seamless internet connectivity	1 Hr
Internet Issue LAN			1 Hr
ERP Related	Any functionality not working, any UI not responding, any configuration issues or tech glitch which is not critical	Rectification	1 Day
	New Requirement, customization, major glitch which is not critical but important	Evaluation, discussion and resolution	Variable. Depends upon the requirement.
Google Workspace (G suite/Email IDs)	Forgot/reset password	Reset the password	2 Hrs.
Online Transaction Issue	Payment not updated, double payment	Resolution	1 day
	issue in online payment	Resolution	Immediate
Software Issues	Any OS, system software, application software related issues (Nonacademic)	Resolution	4 Hrs.
Hardware related	Peripheral devices not functioning, sound issue, non-critical malfunctioning	Resolution	2 working days

Note: Any service that requires purchase or incurs cost in any format would require written approval from the Management. For any emergency approval over call can be considered as immediate remedy. This might increase the resolution time.

7. Network (Intranet & Internet) Use Policy

7.1 Introduction:

The university will take reasonable and appropriate steps to protect the information shared with it from unauthorized access or disclosure. The university strives to implement security measures that protect the loss, misuse, and alteration of data collected. The university maintains a computer security policy.

7.2 The IT Manager is responsible for ensuring the security of information maintained on servers in accordance with government guidelines. All information maintained on CMR University computers is considered the property of CMRU. Access to CMRU computer systems is restricted to authorized users only. Access to administrative applications is determined by the owners of the institutional data.

7.3 Authorized users are responsible for:

1. Maintaining the security of their passwords.
2. Ensuring that removable media containing sensitive or critical data are put into locking storage when not in use or maintained, in areas that are locked when not in use;
3. Backing up critical data maintained on their google drives.
4. Ensuring that only authorized software is loaded onto any university's computer system. Authorized PC software packages are those developed, approved, or installed by the Office of Information Technology, or those obtained from reputable vendors who guarantee their products. The use of unauthorized PC software and programs (software obtained from unauthorized computer bulletin boards, friends, other employees, etc.) is strictly forbidden.
5. Protecting CMRU computers from viruses by using authorized virus protection software and scanning disks.
6. Ensuring that software installed on CMRU computers is not copied illegally.
7. Documenting sensitive or critical PC applications developed for departmental use and used to perform CMRU business.
8. Maintaining the confidentiality of all records as required by applicable University policy, central and state law.
9. Any workstation (terminal, personal computer, etc.) that is left unattended for longer than fifteen minutes is to be protected from unauthorized access by either.
10. Using a screen saver with password protection to prevent access, or logging off from all computer systems. When using a password-protected screen saver, this password is to be known only to the individual who is responsible for that workstation.

7.4 Security Arrangements (Completely covered in details in Policy 14):

7.4.1 The university's intranet has been secured by using the Firewall – SOPHOS. Sophos's product range offers network security (Firewall and UTM appliances), Sophos's network security appliances include multiple features like Firewall – VPN (SSL VPN & IPsec), Captive Portal, Gateway Anti-Virus, Anti-Spyware & Anti-Spam, Intrusion Prevention System (IPS), Content & Application Filtering, Web Application Firewall, Application Visibility & Control, Bandwidth Management, Multiple Link Management for Load Balancing and Gateway Failover, over a single platform.

7.4.2 To access the intranet facility, each member of the university – student, research scholar, faculty and staff has been provided with a unique login ID and password, this ensures the network security from the premises outside of the university.

7.5 Internet Users Policy

There are various types of defined user groups in Firewall:

7.5.1 High data consumers: IT Team, Content team, OSA etc types of users require data download in large capacity because of their core works such as system updates, firmware updates, new system installations, cloud backup, design browsing, data sharing with external agencies, event planning etc.

These types of users get 100GB of data per month with bandwidth upto 15 Mbps.

7.5.2 Standard Data consumers: All other types of staff use internet browsing and other activities which require less data so for these staff we configured the data usage limit to 20GB and bandwidth is upto 15Mbps.

7.5.3 Lab Systems internet access: We have defined a user policy for the lab systems where students will use a common login ID and password where they will be able to use 5Mbps bandwidth and 10GB data per user.

7.5.4 Guest User Access: The guest user is created to accommodate temporary users such as visiting faculties, guests, vendors, delegates etc. This user login can accommodate upto 10 concurrent logins on any device with limitation of 10Mbps Bandwidth and 10GB data per user per month

7.5.5 Hostel Students: Hostel is a managed services facility. The Hostel Students have been provided with a uniform policy of 25 Mbps Bandwidth and 250GB data download per month as a default plan. Any additional data or bandwidth can be purchased through the ISP.

7.5.6 Mac Binding: Mac binding is only applicable during a critical usage and is unable to connect during an ongoing event. It is a temporary arrangement. Any permanent mac binding internet usage has to be approved by the Pro Chancellor.

8. Email Account Use Policy

computer; as such messages may contain viruses that have Potential to damage the valuable information on your computer.

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

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

8.6.8 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.

8.7.8 Students will be allowed to use the CMR Email IDs after 1 year of getting passed out

8.7.9 Email IDs of the students will get deactivated on the request of the respective head of the schools in case of nonpayment of academic fee which will be reactivated only after a communication from the respective school again.

8.7.10 Any Email or google workspace related issue will be communicated to the technology team from the faculty.

8.7.11 Email of any staff who leave the organization is deactivated at the last working day. It is responsibility of respective department/school head to transfer all the required information before the concerned staff leaves the organization.

8.7.12 To reactivate the deactivated email ID the concerned department/school head should send an email to IT Manager.

8.7 Impersonating email account of others will be taken as a serious offence under the university IT security policy. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

8.8 Any email coming from @cmr.edu.in domain which is an official communication from University should not be marked as SPAM. If any suspicious email is received from @cmr.edu.in domain email, it has to be sent to itmanager@cmr.edu.in for immediate action.

8.9 All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible.

8.10 The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside

8.11 Storage limit (Max) in Google accounts:

S. No.	Department	Personal Drive storage	Shared Drive storage
1	Administration & Accounts	100 GB	100 GB
2	HR	15 GB	100 GB
3	IT Team	15 GB	100 GB
4	Content Team	15 GB	100 GB
5	Leadership (School and Non School)	15 GB	100 GB
6	Students	15 GB	100 GB
7	Academic team	15 GB	100 GB

8.12 Email Nomenclature SOPs:

8.12.1 For Students: Email ID Nomenclature suggested for students:

- <first name>.<surname>
- In case of more than 2 similar IDs of case 1 & 2, we should use <first name>.<initials (2 letters only)>

- In case of repetition of above 3 use <initials>.<first name>

8.12.2 For Staff:

- Nomenclature will be <first name> . <initial of surname or last name>
- Inbox of the left staff can be shared with any other person only after an official mail from the respective department head/head of the school.
- Post/designation-based Email IDs will only be issued after approval from Pro Chancellor

8.13 Email Groups:

8.13.1 There will be students' email groups for each academic year program wise and school wise.

8.13.2 Provost, Vice Chancellor, Registrar and Dean Academics will be members/owner of each Email group.

8.13.3 A standard nomenclature will be used for creating the Email groups.

8.14 Mass Email Guidelines:

8.14.1 Mass mailers should be sent from designation/school Email IDs instead of name/personal email ids.

8.14.2 Maximum number of emails allowed from one mail ID is 2000/day and 10000/month. Beyond this the Email ID is deactivated for 24 Hours.

8.14.3 School leadership and Non-school leadership is advised to use Email groups for all types of communication with students besides ERP communication module.

9. Website Policy

9.1 CMR University Web site & Official Pages at <http://www.cmr.edu.in>

Schools, departments, and Associations of Teachers/Employees/Students may have pages on CMR University Intranet Channel of the official Web page. Official Web pages must follow the University Website Creation Guidelines for Website hosting. As on date, the university's content team is responsible for maintaining the official web site of the university through the authorized vendor only.

9.2 Affiliated Pages:

Faculty may host Web pages for "affiliated" professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

9.3 Hosting Policy

9.3.1 Web site hosting and maintenance is taken care by specialized vendor organization who have expertise and experience in the same field.

9.3.2 The vendor is responsible to do the changes/customizations/improvements on web site as per the SLA document.

9.3.3 Any communication regarding above changes will go to the vendor through a functional in-house content team sitting at the University office.

9.3.4 Any department/school who wishes to change/add/update any information related to their respective school/department should contact in house Content team for the same by using an [Online form](#) mentioning all required details.

9.3.5 All the department/school head are supposed to check their respective web page on web site for regular updates. It will be responsibility of respective school heads (Dean/Director) to ensure all the information updated on their school web page is accurate and up to date.

9.3.6 All the requested changes in the web site once updated should be signed off by respective school heads through an official email to content@cmr.edu.in

10. University Database Use Policy

10.1 Scope of Procedure and Rationale

This Policy relates to the databases maintained by the university administration under the university's E-Governance. Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential. CMRU has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this university resource.

10.2 Database Ownership: CMR University is the data owner of all the University's institutional data generated in and for the university.

10.2 Custodians of Data: Individual Sections or departments generate portions of data that constitute University's database. They may have custodianship responsibilities for portions of that data.

10.3 Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

10.4 ERP Components: For the purpose of E-Governance, ERP System of the university may broadly be divided into following categories. These are:

- ❖ Employee information management system
- ❖ Students' information management system
- ❖ Financial information management system
- ❖ Event information management system
- ❖ Document management and information retrieval system
- ❖ Examination management information system
- ❖ Attendance management information system

10.5 General policy Guidelines and parameters for schools, departments and administrative unit data users:

10.5.1 The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.

10.5.2 Data from the University's Database including data collected by departments or individual faculty and staff, is for internal university purposes only.

10.5.3 One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the university makes information and data available based on those responsibilities/rights.

10.5.4 Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the University Registrar.

10.5.5 Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University and departments should never respond to requests. All requests

from law enforcement agencies are to be forwarded to the Office of the University Registrar for response.

10.5.6 At no time information, including that identified as ‘Directory Information’ be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the university or its departments.

10.5.7 All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar of the University.

10.5.8 Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

10.5.9 Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:

- a. Modifying/deleting the data items or software components by using illegal access methods.
- b. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
- c. Causing database or hardware or system software crash thereby destroying the whole or part of database deliberately with ulterior motives by any individual.
- d. Trying to break security of the Database servers. Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities. If the matters involves illegal action, Law enforcement agencies may become involved

11. CCTV Surveillance Policy

11.7 Covert recording

11.7.1 Covert cameras may be used under the following circumstances on the written authorization or request of the senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

- ❖ That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- ❖ That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

11.7.2 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.

11.7.3 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

11.8 The Security Control Room

11.8.1 Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

11.8.2 No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry.

11.8.3 Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.

11.8.4 Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the center. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

11.9 Security Control Room Administration and Procedures

11.9.1 Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

11.9.2 Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

11.9.3 Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

11.10 Recording

11.10.1 Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time. Images will normally be retained for minimum 7days to maximum as per the regulatory compliances from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

11.10.2 All hard drives and recorders shall remain the property of university until disposal and destruction.

11.10.3 The recording by default is available for 7 days in DVR hard disk post that it gets auto deleted.

11.11 Access to images

All access to images will be recorded in the Access Log as specified in the Procedures Manual. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

11.12 Access to images by third parties

Disclosure of recorded material will only be made to third parties only if matter involves illegal actions such as antinational, piracy, snooping etc. and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

11.14 Request to prevent processing

An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Head Security Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

11.15 Complaints

It is recognized that members of University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralized Complaints Procedure by obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Head Security Officer; these rights do not alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.

11.16 Compliance monitoring

The contact point for members of University or members of the public wishing to enquire about the system will be the Security Office which will be available during the hours of 1020 and 1400 and 1430 to 1800 Monday to Friday, except when University is officially closed.

11.17 The effectiveness of the system in meeting its purposes will be kept under review and report submitted as required to the Estates Management Committee.

12. Data Recovery in case of Disaster

12.1 Overview

In order to facilitate the recovery and restoration of University IT systems that support critical functioning of organization, units shall engage in disaster recovery planning efforts.

Disaster recovery planning is the ongoing process of developing, implementing, and testing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption, irrespective of the source of the interruption.

Engaging in disaster recovery planning ensures that system dependencies have been identified and accounted for when developing the order of recovery, establishing recovery time, recovery point objectives, and documenting the roles of supporting personnel.

In addition, data backup is an integral component of disaster recovery planning. Data backup protects against the loss of data in the event of a physical disaster, database corruption, and error propagation in resilient systems, hardware or software failure, or other incident which may lead to the loss of data. The backup requirements found in this document will allow university business processes, teaching and learning activities and research projects to be resumed in a reasonable amount of time, based on criticality, with minimal loss of data.

12.2 Scope

This Disaster Recovery Standard applies to:

12.2.1 Critical core IT infrastructure and other services which facilitate the transport, authentication and security of systems and data. Critical core infrastructure is defined as components which, when they experience degradation or failure, compromise all other services (e.g., Server, identity and access management, network, firewall, DNS, Active Directory).

12.2.2 Information technology systems that process or store mission critical data managed by, or on behalf of, the University, as determined by the unit that maintains the system; this specifically excludes desktop devices and workstations which do not require disaster recovery plans but may require data backup.

12.2.3 The processes, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage.

12.3 Roles and Responsibilities

12.3.1 Information Assurance/IT Manager (IA)

- Maintains and publishes UNIVERSITY disaster recovery planning templates and processes.
- Units or research projects that maintain information technology systems (system or business owner)
- Identify mission critical systems.
- Maintain adequate infrastructure resiliency and data backup and restoration processes for mission critical data and the IT systems assigned to them.
- Develop, implement, document, maintain, and test disaster recovery plans.
- Update the status of their DR planning to IA every two years.

12.3.2 Unit IT Leader and/or Security Unit Liaison

- Coordinate unit activities to satisfactorily implement or complete above unit responsibilities.
- Work with unit IT to review unit DR plans at least annually or whenever significant system architecture or personnel changes occur.
- Brief unit leadership on status of DR efforts and resources needs.
- University Unit or Executive Leadership (Deans, Directors, University Office of Research)

12.4 We ensure that sufficient financial, personnel, and other resources are available as needed for the successful creation and ongoing maintenance of unit DR plans.

12.5 Definitions

12.5.1 Mission Critical: Mission critical IT systems and applications provide essential IT functions and access to data and whose unavailability will have an immediate and significant detrimental effect on the University and campus units if the system fails or is interrupted. A system or application may be designated mission critical if it meets one or more of the following conditions:

- Risk to human and research.
- Significant impact on the University's research, learning and teaching, and administrative working.
- Significant legal, regulatory or financial costs.
- Serious impediment to a campus unit carrying out its critical business functions within the first 48 hours following an event (48 hours Recovery Time Objective – RTO).

- Loss of access to data with defined availability requirements.
- Loss of particular systems or applications may be originally assessed as not mission-critical, but may become more critical after an extended period of unavailability.

12.5.2 Critical Business Functions: Critical operational and/or business support functions that cannot be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing UNIVERSITY operations. Following are such functions:

12.5.3 Recovery Time Objective (RTO): The duration of time within which a business process must be restored and a stated service level achieved following a disruption in order to avoid unacceptable consequences associated with a break in service.

12.5.4 Recovery Point Objective (RPO): The maximum tolerable period in which data might be lost from an IT system or service due to a major incident. RTO and RPO timeframes for each criticality level are listed in Table 1 below.

12.5.5 Disaster Recovery Planning: The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage.

12.5.6 Business Continuity Planning: Business continuity planning, as opposed to disaster recovery planning, is the process of developing detailed plans, processes, and strategies that will enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption and fully recover as quickly as possible.

12.6 Standard

The following are the core components required of all information technology disaster plans:

12.6.1 Critical Systems: All units and research programs that maintain critical information technology systems will develop, implement, and regularly test (exercise) disaster recovery plans for those systems;

12.9 The following table should be used to determine disaster recovery and backup requirements for systems or machines that create, process, maintain, or store Restricted, High, or Moderate data and for mission critical systems irrespective of data classification. Where data can be classified into more than one of the categories listed below or RTO classification/criticality level), the classification with the most stringent data backup requirements must be met.

Data Classification	Data Backup	Data Backup Encryption	Disaster Recovery Plan Requirements
Restricted: ERP, Tally, Content, IQAC, Examination	Required	Required – At rest/in transit	At the earliest possible
High: Administration, Purchase, Operations, Civil works etc.	Recommended	Recommended	Within 1 working day
Moderate: Templates, Academics communication	Recommended	Recommended	Within 2 working day
Low: All others	Recommended	Optional	Within 1 week

12.10 Violations and Sanctions

12.10.1 Violations of this policy by faculty may result in appropriate sanction or disciplinary action consistent with applicable University procedures. If dismissal or demotion of qualified faculty is proposed, the matter will be addressed in accordance with the procedures set forth in. In addition to disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

12.10.2 Any department or unit found to have violated this Standard may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.

12.11 Implementation

Information Assurance/IT Manager is responsible for the implementation, maintenance and interpretation of this Standard.

13 Power Backup policy for IT hardware

13.1 CMR University is having its power back up generators for enough back up energy around 10 hours for entire load. The generators turned on automatically and all the protected electric loads seamlessly transferred to the backup power system.

13.2 All IT enabled essential applications are on online UPS power supply. All academic blocks are having central online UPS which are with redundancy.

13.3 A substation is created which draw power from national grid and step down to 40 KVA. It is operational 24x7. Power supply will be guaranteed and generators start automatically.

14 Cyber Security and Data Privacy

14.1 The university will take reasonable and appropriate steps to protect the information you share with us from unauthorized access or disclosure. The university strives to implement security measures that protect the loss, misuse, and alteration of data collected. The university maintains a computer security policy.

14.2 IT Manager is responsible for ensuring the security of information maintained on computer systems in accordance with State Agency Guidelines. All information maintained on CMR University computers is considered the property of CMRU. Access to CMRU computer systems is restricted to authorized users only. Access to administrative applications is determined by the owners of the institutional data.

14.3 All University campuses are protected with Sophos Firewall systems which is enabled with all security features available for screening any unwanted data flow inside the network.

14.4 University has a centralized Anti-Virus system to protect the network from any malware attack

14.5 To access the organizational network, the users have the Internet access credentials of captive portal.

14.6 The critical data storage access is shared only with authorities and users approved by Registrar, VC and Pro VC.

14.7 Authorized users of computing facilities are responsible for:

14.3.1 Maintaining the security of their passwords;

14.3.2 Ensuring that removable media containing sensitive or critical data are put into locking storage when not in use or maintained in areas that are locked when not in use;

14.3.3 Backing up critical data on cloud which is maintained on their micro computers' hard disks;

14.3.4 Ensuring that only authorized software is loaded onto any computer system.

14.3.6 Protecting CMRU computers from viruses by using authorized virus protection software and scanning disks;

14.3.7 Ensuring that software installed on CMRU computers is not copied illegally;

14.3.8 Documenting sensitive or critical PC applications developed for departmental use and used to perform CMRU business;

14.3.9 Maintaining the confidentiality of all records as required by applicable University policy, federal, state and local law.

14.3.10 Any workstation (terminal, personal computer, etc.) that is left unattended for longer than fifteen minutes is to be protected from unauthorized access by either:

14.3.11 Using a screen saver with password protection to prevent access, or logging off from all computer systems. When using a password-protected screen saver, this password is to be known only to the individual who is responsible for that workstation.

15. Network /internet usage policy for Hostel Students

15.1 Introduction:

15.1.1 The Edufice team in coordination with Campus House team will take reasonable and appropriate steps to provide seamless internet connectivity to registered hostelite. The Edufice team strives to implement security measures that protect the loss, misuse, and alteration of data collected. The university maintains a network security policy.

15.1.2 The IT Manager is responsible for ensuring the security of the network in accordance with government (DoT) guidelines. All registered hostelites will be authenticated by the Campus House team. The shared data by Campus house team will be enabled as Internet User by Edufice team.

15.3 Authorized users are responsible for:

- Maintaining the security of their internet login credentials.
- Maintaining virus protection in their device/s
- Refrain from Phishing by unauthorized web clients
- Ensuring non pirated and authentic software are installed and used in their devices
- Not to install any P2P client (e.g, Torrent, VPN, Darkweb etc.) in their device
- To keep a track of their internet usage

15.4 Security Arrangements:

The university's intranet has been secured by using the Firewall – SOPHOS and a radius server.

Sophos's product range offers network security (Firewall and UTM appliances), Sophos's network security appliances include multiple features like Firewall – VPN (SSL VPN & IPsec), Captive Portal, Gateway Anti-Virus, Anti-Spyware & Anti-Spam, Intrusion Prevention System (IPS), Content & Application Filtering, Web Application Firewall, Application Visibility & Control, Bandwidth Management, Multiple Link Management for Load Balancing and Gateway Failover, over a single platform.

To access the internet facility, each Hostelite will be provided with a unique login ID and password of the captive portal, this ensures the network security from the premises outside of the Hostel.

15.5 Internet Users Policy

There are various types of defined user groups in Firewall:

15.5.1 Staff: Hostel admin, Warden, Unit manager/s, Asst Warden will get the Internet access with 1 device login. The allocated bandwidth will be **10Mbps** with **50GB** data download limit per month. To recharge the data if it gets exhausted, the concerned user will have to get the request approved by Hostel Admin and submit the same to Edufice team for further action. Edifice will take the appropriate action within 24 Hours.

15.5.2 Standard Data plan: By default all the Hostelites will get **25Mbps** speed and **250 GB** data download limit per month. Student will have the self service portal in their captive portal login where they can

15.5.3 Data and bandwidth beyond the standard plan: There will be defined data plans with daily and monthly durations which the user can purchase anytime through the self service portal. These will be revised based on the standard market price.

15.5.4 Guest User Access: The guest user will get the login from Campus House team. The guest user login will be able to access the internet with a 10 Mbps connection having a data limit of 5GB per day. At most 5 logins will be allowed to use this concurrently.

16. ERP User Policy

16.1 Introduction:

CMR University is using Juno Campus ERP for its operations which includes Academics, Examination, Fee collection, Administration, LMS, Hostel Management, Asset management, Purchase, Alumni and many other University operation automation. All the staff (teaching and non-Teaching) and students have the access to the ERP.

16.2 Staff Onboarding or User Creation for Staff

Only HR team will onboard any new user in ERP at the time of their joining. It is mandatory to have University domain Email ID (@cmr.edu.in) to onboard a user into the ERP. Post that IT team gives the Required access to the user after receiving a request email from head of the School/Department.

16.3 Staff login deactivation

HR team will be deactivating the user login on the last working day of the staff.

16.4 Student onboarding

There are 3 ways through which students can be onboarded on ERP:

16.4.1 Applicant data transfer from the CRM which is used as a admission management platform. There will no human intervention and all the student details filled at the application stage will flow into the ERP after validation from the admission team.

16.4.2 Direct admissions in case of government admissions such as CET, ComedK, PGCET etc. In these cases Admission team will be responsible to validate the student details and upload the required essential documents.

16.4.3 Readmission when a student joins back the University after a gap of at least 1 year. In these cases if the profile is already there in ERP as Left or Discontinued, we just reinstate that but if the profile is not there IT team creates a new one. This process can be initiated only after receiving a University notification and Account head approval.

16.5 Student account deactivation

There are following categories for student account deactivation in ERP after which student cannot login into the ERP. Nobody except Accounts Head & Administration team will have the access to this student profile:

16.5.1: Left: When the student has left the University just by submitting the application. Once the same application is approved by Registrar office, Accounts Head will send an email to IT team to mark the student as left.

16.5.1: Discontinued: When the student leaves the studies in between but have certain possibility to join back later submits the application to registrar office. Once notice received from registrar office, Accounts Head will send an email to IT team to update student status as “Discontinued”.

16.5.3: Admission Cancelled: During the first year if any student applies for admission cancellation, Accounts Head processes the admission cancellation where they mark the student as admission cancelled by updating refund amount entries in the ERP

16.5.4: Block: This is a temporary suspension of a student account after which student can not access his/her ERP login. IT Team updates this student status in ERP after receiving email communication from Accounts Head.

16.6 IT head and ERP Admin will have Super admin access across all the modules of ERP.

17. Review and Revision Policy

17.1 CMRU has a provision for reviewing and revising this policy. For this the members of the CMRU fraternity mentioned below are the committee members who will meet annually at the beginning of each academic session for the aforesaid purpose. The committee members can suggest/advise/Counsel the changes based on:

- ❖ New and/or amended government laws/acts
- ❖ Addition or removal of the end-users
- ❖ Revised university's policies
- ❖ Need of the university infrastructure

17.2 The committee members will include

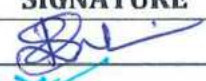


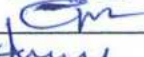
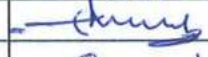

- ❖ Management – CMRU
- ❖ Vice-Chancellor, Pro – VC
- ❖ CEO
- ❖ Registrar, RE
- ❖ Deans / Directors
- ❖ Manager, IT
- ❖ Head of Security
- ❖ Student representatives (five – 2 from Masters, 3 from Bachelors)
- ❖ Senior Professors – 2 to 5 (Various Campus)

DEPARTMENT OF CSE/IT

LAB POLICY

Engineering as a professional training has two inseparable and mutually complimentary components – theoretical understanding and practical problem solving. While the statutory requirements of all the laboratory courses as per scheme and syllabi have to be met, our laboratories have to graduate further. They are required to offer our students the opportunities to explore beyond those confines. In essence, our laboratories must be where students actually experiment rather than merely follow the procedures as per manuals. Hence, our students must be provided with the space, time, freedom and support necessary to implement new ideas and carry out innovative projects, albeit with suitable guidance, mentoring and hand- holding.

To move up the value chain in this direction, a Laboratory Refinement Committee is hereby constituted with minimum one member from each of the engineering departments as below and with immediate effect.

MEMBERS	DESIGNATION	SIGNATURE
Dr. RUBINI.P , HOD/CSE	Chair	
Dr.Saravana Kumar S, HOD/IT,AIIML,DS	Co-chair	
Dr.Shweta A, Asst.Prof/CSE	Member	
Prof, Nandi Kesavan, Asst,Prof/CSE	Member	
Mr.Ganaraj Bhat, Lab inst/CSE	Member	
Mr.Tippeswamy , Lab inst/CSE	Member	
Mr.Suraj Kumar Saw, Student	Member	
Ms. Nimisha Kumari, Student	Member	

ROLES AND RESPONSIBILITIES

1. Reviewing the experiments required to be conducted as per university stipulations.
2. Reviewing the existing facilities in terms of infrastructure, equipment and components / consumables;
3. Consulting the relevant industries / labs for refinement and addition of experiments to make them meaningful for the students to improve their understanding of concepts and acquire hands-on skills aimed at enhancing their employability;
4. Propose the lab requirements – infrastructure, equipment and personnel – as and when required;
5. Ensure preparation of laboratory manuals for all experiments within the university syllabi before the commencement of every semester;

6. Ensure that faculty handling lab courses have themselves actually conducted all the stipulated experiments before the commencement of every semester;
7. Provide or ensure necessary guidance for faculty handling lab courses, if and when required;
8. Overseeing the stock maintenance; and
9. Any other item that may be deemed necessary from time to time with the concurrence of the Chair.

The Members will be guided by the Chair and shall report to the Chair on matters of status, compliance and progress. They may seek and avail assistance from the faculty colleagues in their respective departments.

The departmental faculty shall cooperate with their fellow Members in this refinement process. On specific assignments and as per contingencies, the Chair may co-opt any faculty other than the Members and from any engineering department in consultation with the relevant departmental head.

The respective departmental heads shall facilitate as required to ensure effective and smooth functioning of all laboratories.

Do's and Don't s in the Lab

Do's

1. Keep the bags in the designated place as you enter the lab.
2. Enter the details in the log book like name, registration number, System number, Time in and signature.
3. Only Observation Books and writing material (Pen, Pencil and Eraser etc.,) are allowed near the working place.
4. Take the component required for your programming work by registering your name, date and the component taken in the register kept at the staff counter.
5. Switch on the power located behind the CPU Power on the system as well as the monitor.
6. Login to the system allotted to you by the procedure of entering the password.
7. Before leaving the lab, upload all the work done to github account in the same session.
8. Shut down the system.
9. Power off the monitor and switch off the power located behind the CPU cabinet.
10. Keep the chairs properly below the computer table.
11. Return all the components if taken earlier and make entry into the book returned with signature and the date to avoid any damages losses recover from you.
12. Make entry in the leaving time in the login register.
13. Wearing of ID Card is compulsory in the lab,

Don'ts

1. Do not occupy the others seat.
2. Avoid using external USB drive to prevent the computer systems from viruses.
3. Do not go to other student place as it may affect his learning process.
4. Do not use the internet for browsing beyond the syllabus content.
5. Do not use your personal earphone/Mobile phone at the working desk.

List of Labs under CSE/IT

Sl.No.	Name of the lab	Location	No. of Systems
1	Machine Learning Lab	G007/E	30
2	Full Stack Lab	G007/A	30
3	Data Science Lab	G007/D	30
4	C,C++ and Java Lab	G006	30
5	AI&ML Lab	G007/F	30
6	IT & Networking Lab	G007/C	30
7	Programming using Python Lab	G005	30
8	Cloud Computing Lab	G004	30
9	Big Data Lab	G007/B	30
10	System software Lab	G003/A	30



HoD's Signature



Dean,SOET (i/c)

DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149
Page 3 of 3



CMR UNIVERSITY
SCHOOL OF ENGINEERING AND TECHNOLOGY
Lakeside Campus
Department of Basic Science and Humanities
Engineering Physics Laboratory

DO's

1. Maintain cleanness in the working area.
2. Perform the experiments as allotted in the register.
3. Read the laboratory manual and follow the instructions carefully before starting the experiment.
4. Carry your own pencil, eraser, graph sheets, calculator and other required materials to the laboratory.
5. Use the laboratory instruments with utmost care.
6. Any breakdown of equipment should be immediately reported to the staff-in-charge/instructor.
7. In case of fire, glass breakages and serious incidents, bring it to the attention of the staff-in-charge and instructor immediately.
8. Handle mercury thermometers with utmost care.
9. Any technical discussions should be carried out in a low voice so as not to disturb other laboratory users.
10. Keep your personal belonging in the rack
11. Wearing the shoes is compulsory
Loose clothing is not permitted in the lab.

DON'Ts

1. Do not insert metallic objects such as screwdriver, needle, connecting wires in the electrical sockets.
2. Do not view laser beams directly with your eyes.
3. Do not modify the settings of the laboratory equipment in any way unless it is directed by the staff-in-charge/instructor.
4. Do not perform the experiments which you are not authorized to do.
5. Do not spill liquids in the laboratory.
6. Do not carry any unnecessary/ objectionable material to the laboratory (bag consisting of books/stationary are allowed to be kept separately in the laboratory).
7. Do not bring Mobiles into the lab.

hm
07/03/24.

[Signature]
27/3/2024
DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149



CMR UNIVERSITY
SCHOOL OF ENGINEERING AND TECHNOLOGY
Lakeside Campus
Department of Basic Science and Humanities
Engineering Chemistry Laboratory

<u>DO's</u>	<u>DON'T's</u>
Students should come to the lab in time.	No students shall enter the laboratory prior to the permission from instructor/in-charge faculty.
Record your observations and write the experimental procedure during the course of experiments only.	Never taste any laboratory chemicals and do not play with solutions.
Maintain an observation notebook for recording the experimental details.	Eatables and soft drinks are strictly prohibited inside the laboratory area.
Record should be submitted regularly	Do not use mobile phones while carrying out the experiments.
Keep the reagent bottles in their proper place after use.	Unauthorized experiments shall not be performed in the laboratory.
Use the specified quantities of reagents/indicators and do not contaminate it.	Do not use wet hands during weighing.
Clean the used glassware and the working table after the experiment.	Never pick up hot objects with your hands. After heating, place glassware/crucible on a wire gauze to cool.
Gas outlets and water taps must be turned off before leaving the lab.	Never discard any liquids/solutions and waste/used materials directly into the sink.
Report all injuries (cuts and burns, if any) to the laboratory instructor immediately.	Do not play with any chemicals and engage in shrill discussions in the lab.
If your availability is very less to the lab sessions on medical excuses, immediate information must be given to the instructor/in charge faculty through Dean, SOET, CMRU at the earliest to provide alternate sessions for carrying out the experiments.	

hm
07/03/24.

[Signature]
07/3/2024

DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149

School of Engineering & Technology
Department of Electronics and communication Engineering
Embedded System and ARM processor Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Save your lab work in respective folder and shutdown the system
Before leaving the lab
5. Regularity and Punctuality should be maintained
6. Students should come well prepared for the lab classes and observation books are to be maintained.
7. Students should write their Names, Registration number & sign apparatus.
8. Correct specifications of the equipment have to be mentioned in the circuit Diagram
9. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
10. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
11. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
12. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.



School of Engineering & Technology
Department of Electronics and communication Engineering
Making with Electronics Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment have to be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. Ezhumalai

Dr. A. B. Srinivas

School of Engineering & Technology
Department of Electronics and communication Engineering
Analog Electronics Circuits Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment have to be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.



School of Engineering & Technology
Department of Electronics and communication Engineering
Analog System Design Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment have to be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.



HEAD OF THE DEPARTMENT
ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY
CMR UNIVERSITY, BENGALURU-562149



DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149

School of Engineering & Technology
Department of Electronics and communication Engineering
Power Electronics and Control Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment must be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/ instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. E. J. J.

School of Engineering & Technology
Department of Electronics and communication Engineering
Digital Logic Design Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment have to be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. Ezhumani

Dr. A. S. Thirumangalakudi

School of Engineering & Technology
Department of Electronics and communication Engineering
Microcontroller & Embedded System Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Save your lab work in respective folder and shutdown the system
Before leaving the lab
5. Regularity and Punctuality should be maintained
6. Students should come well prepared for the lab classes and observation books are to be maintained.
7. Students should write their Names, Registration number & sign apparatus.
8. Correct specifications of the equipment have to be mentioned in the circuit Diagram
9. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
10. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
11. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
12. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. E. Z. h. t.

School of Engineering & Technology
Department of Electronics and communication Engineering
Embedded System and ARM processor Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Save your lab work in respective folder and shutdown the system
Before leaving the lab
5. Regularity and Punctuality should be maintained
6. Students should come well prepared for the lab classes and observation books are to be maintained.
7. Students should write their Names, Registration number & sign apparatus.
8. Correct specifications of the equipment have to be mentioned in the circuit Diagram
9. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
10. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
11. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
12. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. E. Z...

HEAD OF THE DEPARTMENT
ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY
CMR UNIVERSITY, BENGALURU-562149

Dr. J. S. ...
DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149

School of Engineering & Technology
Department of Electronics and communication Engineering
Advance Communication Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment must be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/ instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. Ezhumalai

School of Engineering & Technology
Department of Electronics and communication Engineering
Microwave and RADAR Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment have to be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/ instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. E. Z. J.

School of Engineering & Technology
Department of Electronics and communication Engineering
Principles of Communications System Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment have to be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Do not come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. Ezhumalai

School of Engineering & Technology
Department of Electronics and communication Engineering
Transmission Lines and Antenna Lab

DO's

1. ID card is compulsory in lab.
2. Do entry in Login book after entering the lab.
3. Read and understand how to carry out an activity thoroughly before coming the laboratory
4. Regularity and Punctuality should be maintained
5. Students should come well prepared for the lab classes and observation books are to be maintained.
6. Students should write their Names, Registration number & sign apparatus.
7. Correct specifications of the equipment have to be mentioned in the circuit Diagram
8. Handle the equipment with care & strictly follow the instructions given by the faculty/instructor.
9. Power supply is to be Switched ON only after the connection are checked by the Staff/Instructor.
10. Upon completing the experiment, student should switch off the power supply and then remove the circuit connection.
11. The completed lab record should be submitted in every class.

DON'T's

1. Don't come late to the Lab.
2. Do not remove anything from the computer laboratory without permission.
3. Do not touch, connect or disconnect any plug OR cable OR without permission
4. Avoid metal bangles/straps and long untied hair. this may be dangerous while conducting experiments.
5. Do not switch on the supply without getting the circuit verified from the faculty/ instructor.
6. Do not leave without obtaining the permission of the staff in charge.
7. Usage cell phone is strictly prohibited.

K. Ezhumalai

HEAD OF THE DEPARTMENT
ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY
CMR UNIVERSITY, BENGALURU-562149

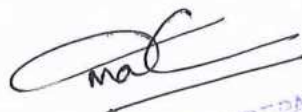
[Signature]
DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149

Engineering Workshop DO's and DON'Ts

DO'S

1. Conduct yourself in a responsible manner at all times in the laboratory
2. Dress properly during a laboratory activity. Long hair, dangling jewellery and loose or baggy clothing are a hazard in the laboratory.
3. Observe good housekeeping practices.
4. Replace the materials in proper place after work to keep the lab area tidy. Any break-down of equipment must be reported to the Lab In-charge.
5. Obtain authorization from the lab In-charge prior to entering the lab working area.
6. Eye protection should be worn when performing tasks with potential to generate flying particles or debris. Most power tool related tasks generate such hazards.
7. Every Student should know the locations and operating procedures of all safety equipment including, First AID KIT, Fire extinguisher and Exits are located.
8. Safety wear (goggles, aprons, gloves, etc.) may be required for certain activities. Goggles should be worn whenever you use dangerous tools or chemicals, or are near such use. If you are required to wear any safety equipment, you must keep it
9. After handling dangerous or dirty items, wash your hands. Do so even if you were wearing gloves.
10. Wear the glassware gloves while handling chemicals
11. ID card is compulsory in the lab

Amey
7/3/24



HEAD OF THE DEPARTMENT
MECHANICAL ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY
CMR UNIVERSITY, BENGALURU-562149


7/3/24

DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149

DON'TS

1. Don't let fingers get too close to the saw blade
2. Don't push too hard, let the tool do the work
3. Don't cut unsecured ROUND material
4. Don't back out of a cut while the blade is running.
5. DO NOT FORCE TOOL. It will do the job better and safer at the rate for which it was designed.
6. USE RIGHT TOOL. Do not force tool or attachment to do a job for which it was not designed.
7. NEVER LEAVE TOOL RUNNING UNATTENDED, TURN POWER OFF. Do not leave tool until it comes to a complete stop.
8. DO NOT OVERREACH. Keep proper footing and balance at all times.

Lab Incharge.

Amy

7/3/24



HEAD OF THE DEPARTMENT
MECHANICAL ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY
CMR UNIVERSITY, BENGALURU-562149



DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149

**School of Engineering and Technology
Department of Mechanical Engineering
Computer Aided Engineering Drawing Lab**

System Configuration:

Device Specification:

Device name	CMR-University
Processor	Intel(R) Core(TM) i3-9100 CPU @ 3.60GHz 3.60 GHz
Installed RAM	8.00 GB (7.89 GB usable)
Device ID	31DA9884-E2D6-4063-AE00-A5C6D4A896E2
Product ID	00327-35160-21806-AAOEM
System type	64-bit operating system, x64-based processor

Windows Specification:

Edition	Windows 11 Home Single Language
Version	23H2
Installed on	10/6/2022
OS build	22631.3235
Experience	Windows Feature Experience Pack 1000.22687.1000.0

Software:

Solid Edge ST10 by Siemens

Room No:

CAED Lab 001, Room no 004 (Basement, SOET)

CAED Lab 002, Room no 004 (Basement, SOET)

Do's and Don't's


School of Engineering & Technology Department of Mechanical Engineering Computer Aided Engineering drawing lab

DO's

1. Conduct yourself in a responsible manner at all times in the laboratory
2. Dress properly during a laboratory activity. Long hair, dangling jewellery and loose or baggy clothing are a hazard in the laboratory.
3. Observe good housekeeping practices. Replace the materials in proper place after work to keep the lab area tidy.
4. Any break-down of equipment must be reported to the Lab In-charge.
5. Obtain authorization from the lab In-charge prior to entering the lab working area.
6. Eye protection should be worn when performing tasks with potential to generate flying particles or debris. Most power tool related tasks generate such hazards.
7. Every Student should know the locations and operating procedures of all safety equipment including, First AID KIT, Fire extinguisher and Exits are located.
8. Safety wear (goggles, aprons, gloves, etc.) may be required for certain activities. Goggles should be worn whenever you use dangerous tools or chemicals, or are near such use. If you are required to wear any safety equipment, you must keep it on.
9. After handling dangerous or dirty items, wash your hands. Do so even if you were wearing gloves.
10. ID card is compulsory in the lab

DON'T's


1. Don't talk aloud in lab.
2. Do not use a flash drive on lab computers.
3. Do not upload, delete or alter any software on the lab PC.
4. If working with LASER machine, never look into the LASER beam and do not try to touch the LASER beam.



R. P. Umith
Lab Incharge.



26/3/2020
DEAN
SCHOOL OF ENGINEERING & TECHNOLOGY
CMR UNIVERSITY
Bengaluru - 562 149



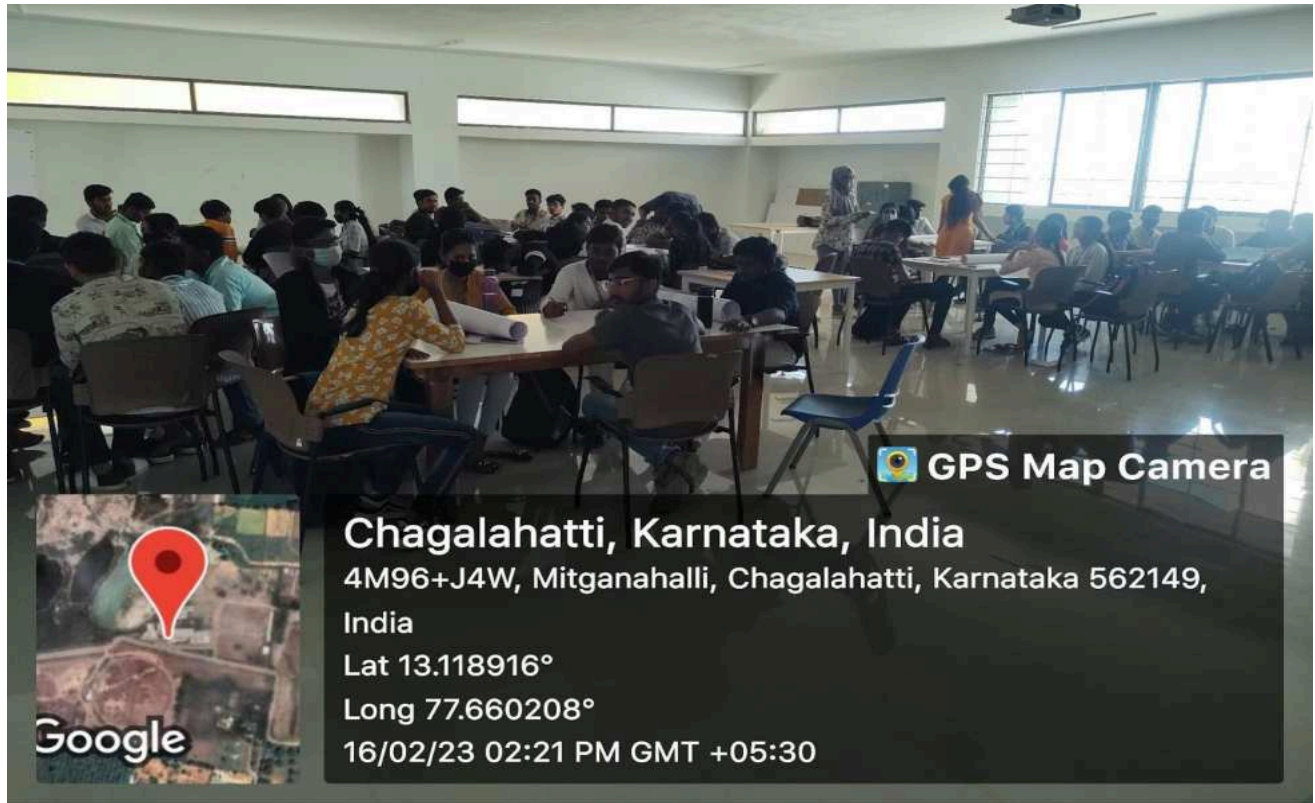
Head of the Department
HEAD OF THE DEPARTMENT
MECHANICAL ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY
CMR UNIVERSITY, BENGALURU-562149



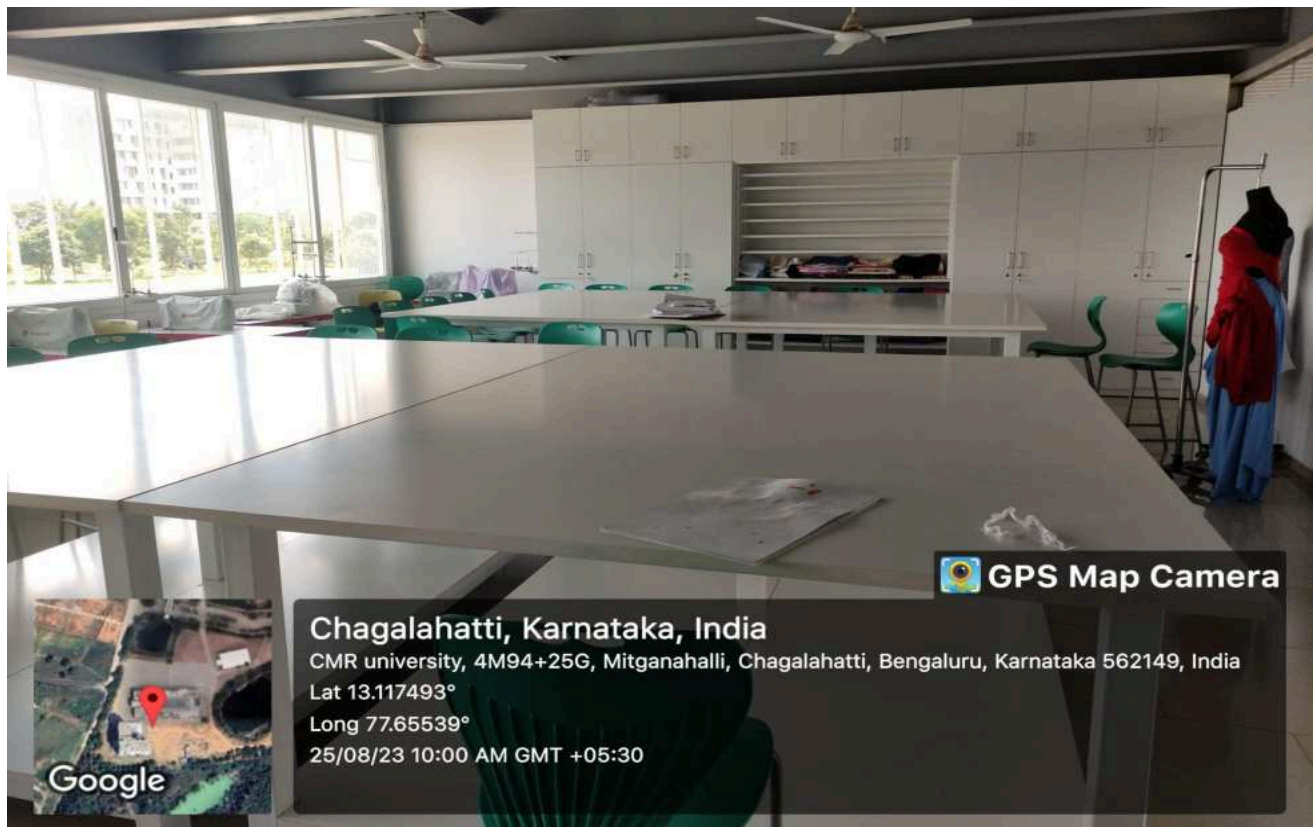
MOOT COURT HALL



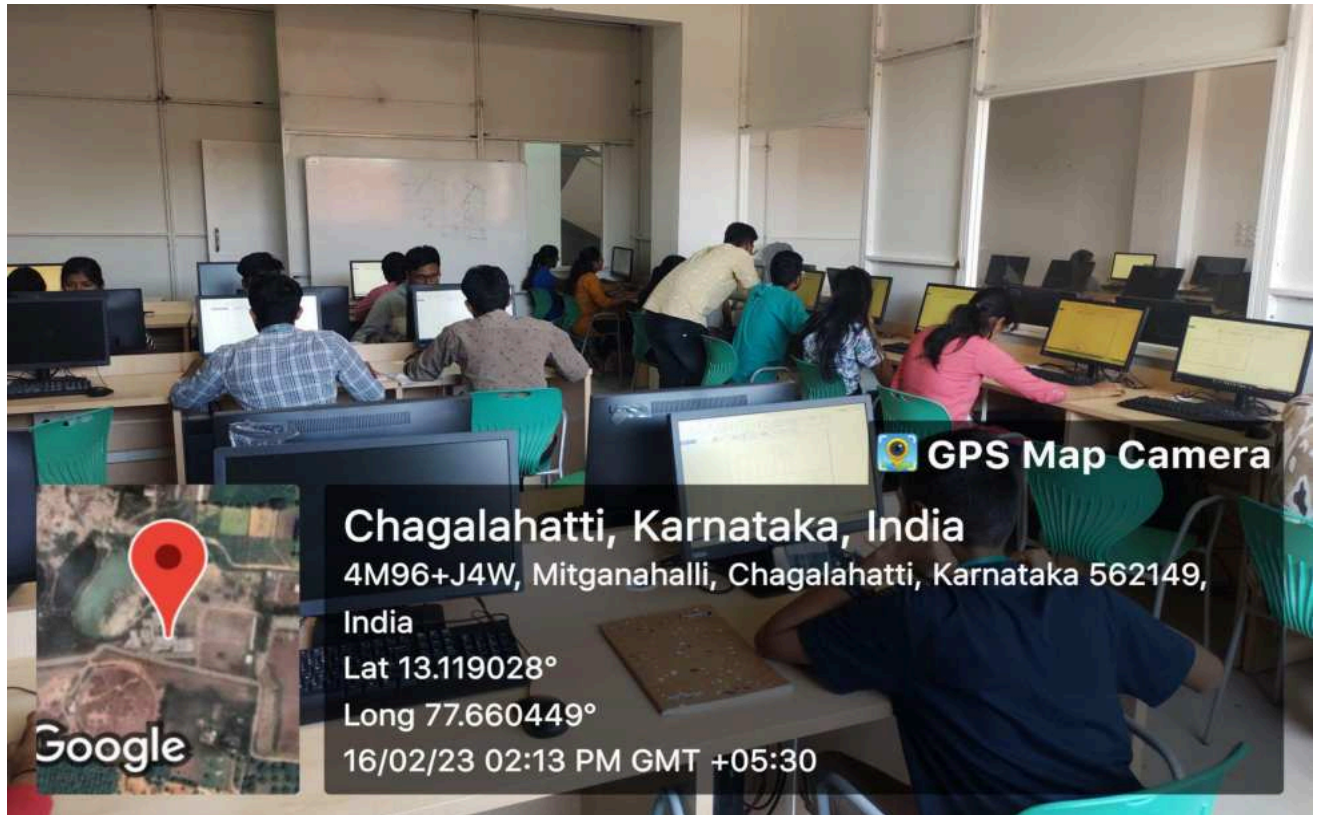
MECHANICAL LAB



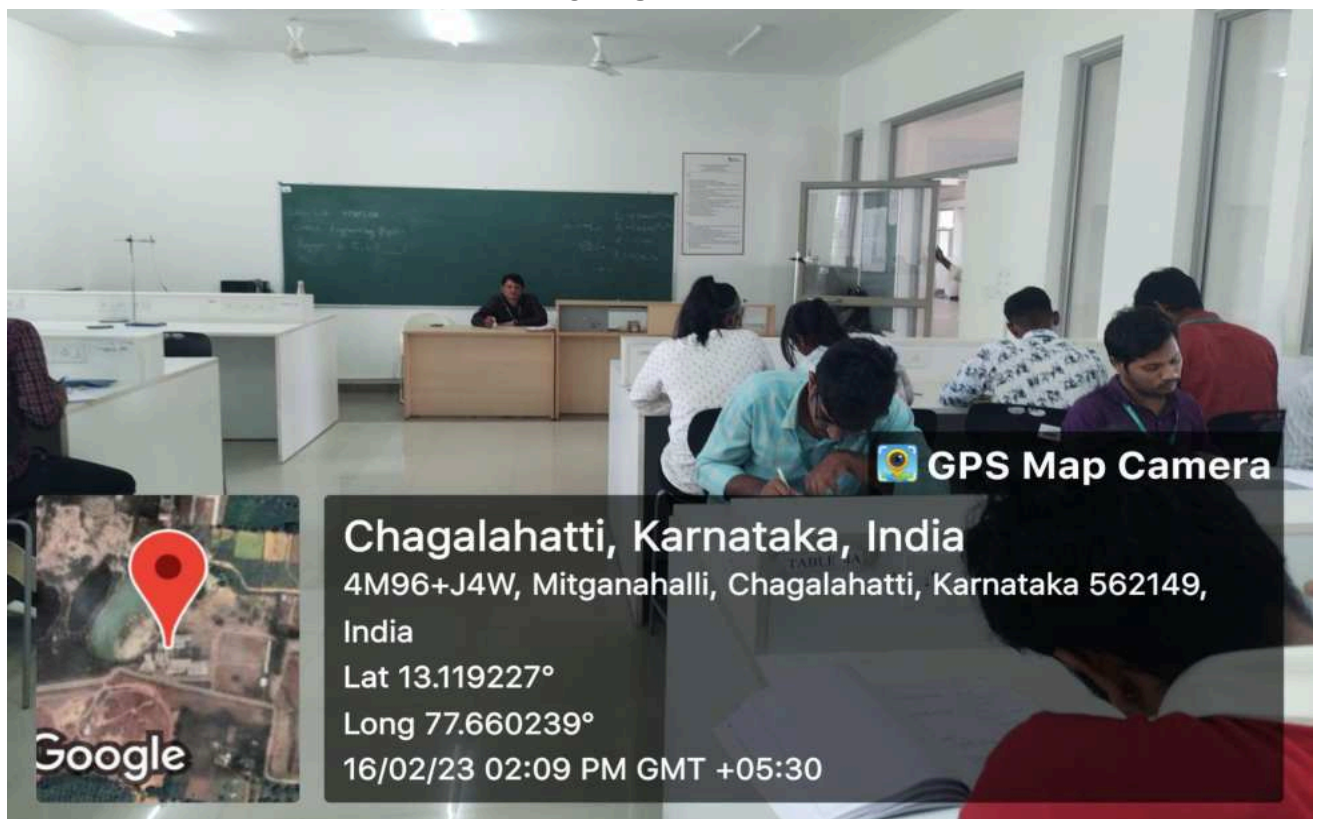
DESIGN THINKING LAB



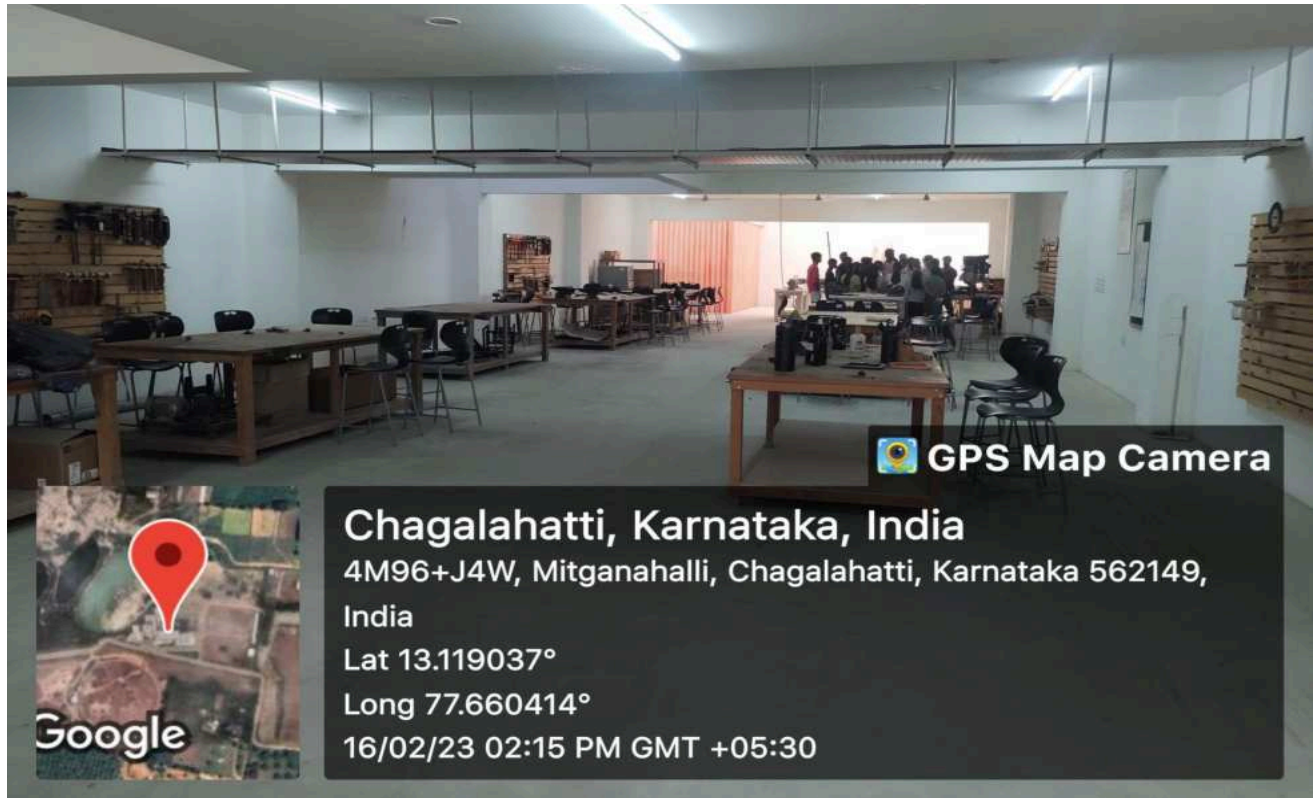
FASHION DESIGNING LAB



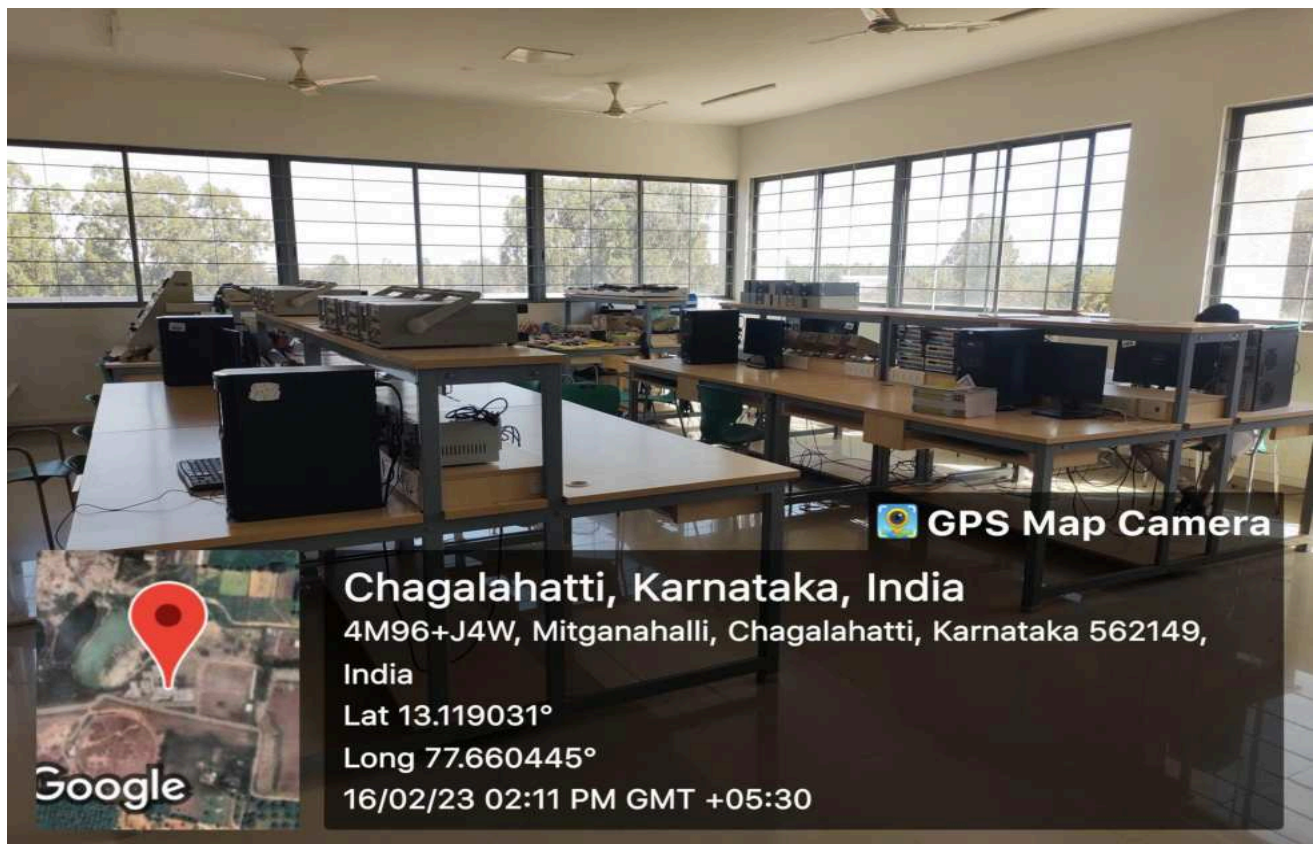
COMPUTER LAB



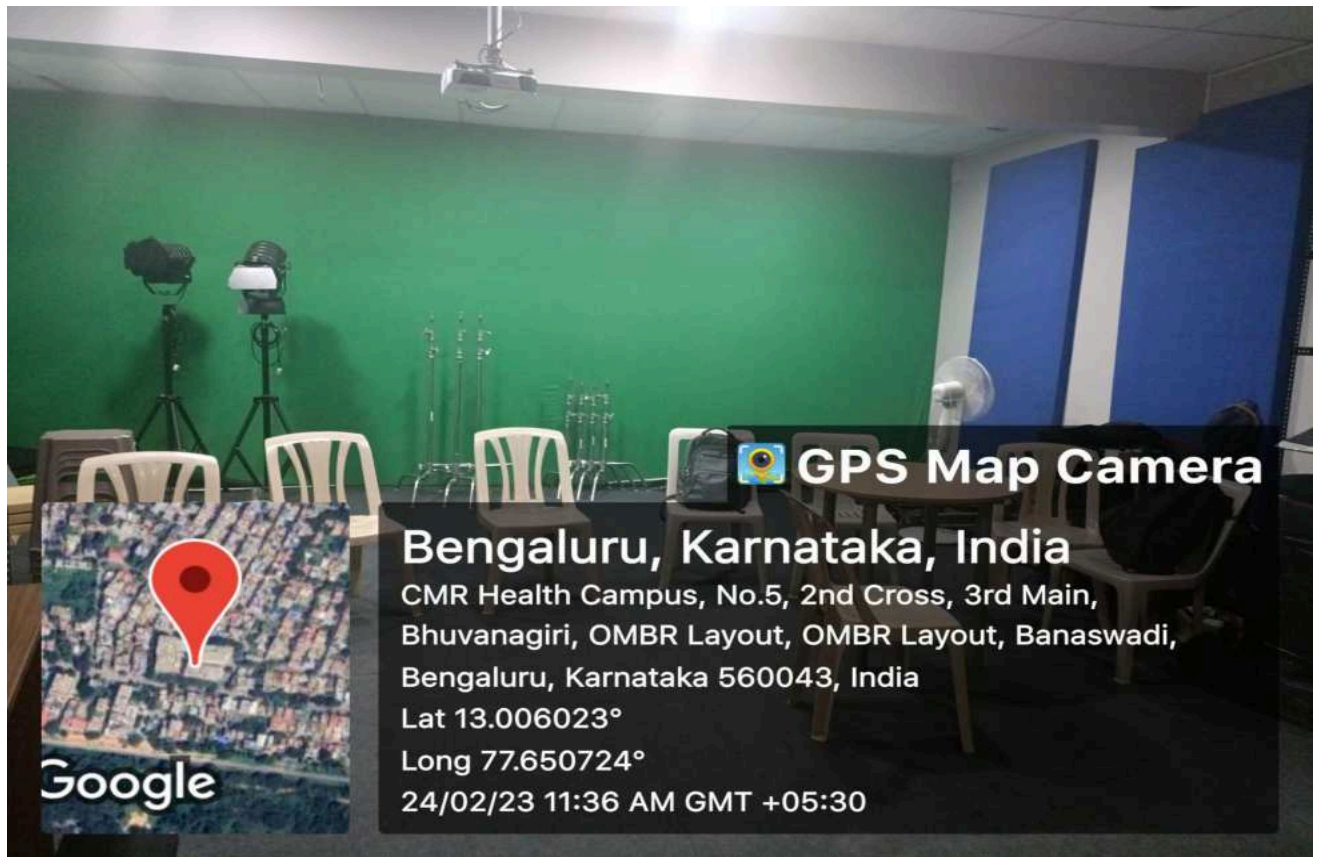
PHYSICS LAB



MECHANICAL LAB



ELECTRONICS LAB



MEDIA LAB

CMR UNIVERSITY SPORTS POLICY

Preamble

"Strength is life, weakness is death." -- Swami Vivekananda

At CMR University, our vision is to *nurture creative thinkers who will drive positive global change*. The Physical Education Department (PED) helps us achieve this vision by training students to be in perfect physical and mental health through sports and other physical activities.

Our objective is to build competitive teams in sports like Cricket, Football, Hockey, Basketball, Throw ball, Badminton, Shuttle Badminton, Tennis, Table Tennis, Swimming, and others. Therefore, we have planned to develop our sports facilities and support the sportsmen to achieve their ambitions.

Apart from preferential admission to the University, talented sportsmen will be provided -

- Accommodation in hostels
- Coaching
- Travel Allowance, reimbursement, and other support
- Financial and academic support

COMPOSITION OF SPORTS ADVISORY COMMITTEE

- 1) Chancellor
- 2) Vice Chancellor
- 3) Registrar
- 4) Physical Education Directors
- 5) U.G / PG. – Students- 01 (Boy)
- 6) U.G / PG - Students -01 (Girl)


Physical Education Director
CMR UNIVERSITY
BANGALORE




Physical Education Director
CMR UNIVERSITY
BANGALORE

CMR UNIVERSITY SPORTS SCHOLARSHIP

a) Summary:

- i. Students who show exceptional talent in sports shall be eligible for the Scholarships under Sports quota.
- ii. The major objective of the scholarship is to provide incentives and grant awards to sportspersons to maintain sustained interest among students to participate and perform progressively.
- iii. The merit for the scholarship shall be decided based on student's performance and level of competition.

b) Eligibility:

- i. The sports scholarship will be awarded on the basis of performance in recognized competitions held during the previous two academic years.
- ii. Both prospective as well as bonafide students of CMR University can apply for the sports scholarship.
- iii. A student shall not receive any other sports scholarship from any other source. In case any student is already receiving such scholarship, he/she has to surrender that in order to avail the benefits of CMRU's sports scholarship.
- iv. The student shall apply only in one sports/games in which he/she has achieved the highest performance during the previous two academic years.
- v. The University Sports Committee has the right to decide awarding the scholarships depending on the number of scholarships available for different sports/games.

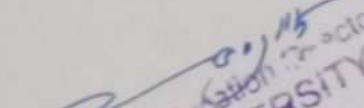
c) Duration of Sports Scholarship:

- i. Any sports scholarship awarded to a student shall be initially for one year and will be renewable every year provided the awardee is improving /maintaining the proficiency in the sport/game concerned. Exceptions to this policy will be made at the discretion of the sports committee only in case of injury, disease, or ill-health provided the student submits relevant documents.
- ii. A student shall submit a new application on prescribed form for the renewal of scholarship every year failing which it will be stopped even if one is eligible.
- iii. The form should then be forwarded through the proper channel to the University's Sports committee.

d) Selection:


Physical Education In-charge
CMR UNIVERSITY
BANGALORE




Physical Education In-charge
CMR UNIVERSITY
BANGALORE

- i. The University's Sports committee will scrutinize the applications and select candidates on the basis of performance and merit.
- ii. The decision of the Committee will be final and no correspondence in this regard will be entertained.

e) BENEFITS UNDER SPORTS SCHOLARSHIPS:


- i. **National Level Medalist / AIU- Medalist / Federation Cups Medalist / National federation of School Games Medalist /World Games Medalist If first three position -**
 - 70% Fee waiver
 - Free Food at University Hostel
- ii. **National Level participated / AIU- participated / Federation Cups participated / DYESS / SAI / National federation of School Games participated -**
 - 60% Fee waiver
- iii. **State Level - First three Positions/ South zone - Frist four Positions -**
 - 40% Fee waiver
- iv. **State /Junior / Senior Level participated -**
 - 30 % Fee waiver

f) BENEFITS UNDER SPORTS SCHOLARSHIPS FOR CRICKET:

- **If student is member / played in National cricket team**
 - 100% Fee waiver
- **If students Played / member in team for State, Vijay Hazere, Deodhar Trophy, Indian camp, IPL Free Food at University Hostel.**
 - 90% Fee waiver
 - Free Food at University Hostel


Physical Education In-charge
CMR UNIVERSITY
BANGALORE




Physical Education In-charge
CMR UNIVERSITY
BANGALORE

- If students-played / member in U-16, U- 19, U7 23, KPL, C.K. Naidu trophy, State probable, 1st— 2nd Division.

- 75% Fee waiver

- KCSA — If students Zonal / state Probable / 3rd Division.

- 50 % Fee waiver

g) Academic support:

a) The teaching-learning process is governed by the UGC norms. Accordingly, all Schools of Studies conduct classes and evaluate students as per the Scheme of Teaching and Evaluation announced at the beginning of each academic year. Also, the admission of students, programme details, registration for courses, attendance requirement, award of grades, promotion and other academic information is specified in the Regulations of the concerned programme for which the students are admitted.

b) The UGC (Minimum Standards of Instruction for the Grant of the First Degree through Formal Education) Regulations, 2003 specifies that:

5.8 The minimum number of lectures, tutorials, seminars and practical which a student shall be required to attend for eligibility to appear at the examination shall be prescribed by the university, which ordinarily shall not be less than 75% of the total number of lectures, tutorials, seminars, practical, and any other prescribed requirements.

6.4 There shall be continuous sessional evaluation in each course in addition to trimester/semester/year-end examinations, and the weightage for sessional evaluation and examination in respect of each course shall be prescribed by the appropriate academic body, and made known to the students at the beginning of the academic session.

The Schools of Studies of the University have framed their Programme Regulations strictly within the framework of the UGC Regulations. However, understanding the special requirements of the students/ sports persons representing the University and attending recognized academic (Paper presentation / Debate / Seminar / conferences)/

Sports activities outside/within the University, following provisions are made:

- The students are treated as 'on duty' and provided attendance on the specified number of days, certified by the concerned Dean, if there is shortage of attendance that is beyond 25%. However, arrangements will be made for the students to catch up with the missed portion of the syllabus.

[Signature]
Physical Education In-charge
CMR UNIVERSITY
BANGALORE




[Signature]
Physical Education In-charge
CMR UNIVERSITY
BANGALORE

- ii) In case the students attending the above activities miss the internal assessment tests or assessments, the concerned faculty shall arrange for separate test/assessment covering the same syllabus. It shall be a part of the duty of the concerned Dean of the School to facilitate the tests/assessments.
- iii) However, the Physical Education Director or concerned faculties shall co-ordinate with the Registrar in all such cases in advance.

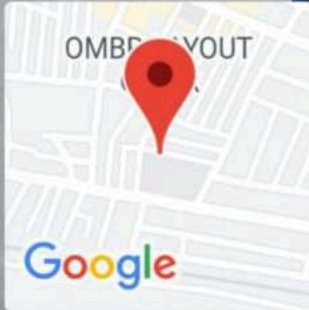

Physical Education Director
CMR UNIVERSITY
BANGALORE




Physical Education Director
CMR UNIVERSITY
BANGALORE



GPS Map Camera



Bengaluru, Karnataka, India

316, 2nd BC Cross Rd, OMBR Layout, Banaswadi,
Bengaluru, Karnataka 560043, India

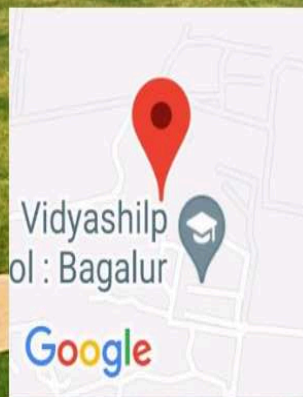
Lat 13.006429°

Long 77.650463°

02/12/22 02:44 PM



Geotag Photo



Chagalahatti Karnataka India

**4M94+5CP, Mitganahalli, Chagalahatti, Bengaluru,
Karnataka 562149, India**

Lat: 13.12 | Long: 77.66

28/02/2024 11:37 am, IST

Wed, 28 Feb



OMBR LAYOUT



Google

Bengaluru, Karnataka, India

4th Main Road, Kasturi Nagar, Bennigana Halli, OMBR
Layout, Banaswadi, Bengaluru, Karnataka 560043, India

Lat 13.006221°

Long 77.650491°

02/12/22 02:42 PM



GPS Map Camera



Geotag Photo



Chagalahatti

iversity
mpus)



Google

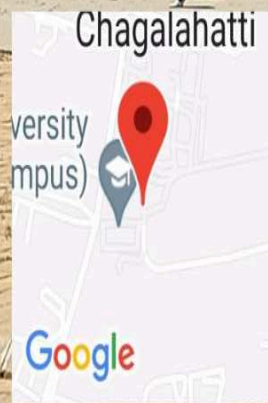
Chagalahatti Karnataka India

4M94+5CP, Mitganahalli, Chagalahatti,
Bengaluru, Karnataka 562149, India

Lat: 13.12 | Long: 77.66

28/02/2024 11:42 am, IST

Wed, 28 Feb



Chagalhatti Karnataka India


4M94+5CP, Mitganahalli, Chagalhatti, Bengaluru,
Karnataka 562149, India

Lat: 13.12 | Long: 77.66

28/02/2024 11:42 am, IST

Wed, 28 Feb



 **GPS Map Camera**



Bengaluru, Karnataka, India

316, 2nd BC Cross Rd, OMBR Layout, Banaswadi,
Bengaluru, Karnataka 560043, India

Lat 13.006333°

Long 77.650564°

16/01/23 02:59 PM GMT +05:30