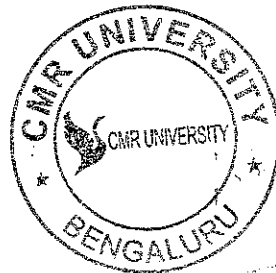




CMR UNIVERSITY
Private University Established in Karnataka State by Act No. 19 of 2013

Information Technology (IT) Policy

238 / 709



CMR UNIVERSITY



VICE CHANCELLOR

Raghunath B

PRAVEEN R

Digitally signed by PRAVEEN R
DN: C=IN, O=C M R JNANADHARA TRUST, OU=ADMINISTRATION, Phone=6468712cb111cd93860f4940e79e456496add0a79fb0432acfb363ebfffa333, PostalCode=560084, S=KARNATAKA, SERIALNUMBER=6abff861b7ca445388cda464b4663c399960f2627eccc05215c52fddca553a9b1, CN=PRAVEEN R
Reason: your signing reason here
Location: your signing location here
Date: 2024.07.10 01:03:28+0530
Foxit PDF Editor Version: 2024.1.0

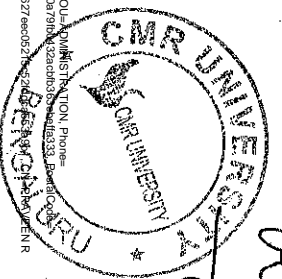


INDEX

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

PRAVEEN R

Digitally signed by PRAVEEN R
DN: cn=PRAVEEN R, o=CMR UNIVERSITY, ou=CMR UNIVERSITY, postalCode=600025, serialNumber=580054, surname=NAIYAKA, email=praveenr@cmru.ac.in, c=IN
Reason: your signing reason here
Date: 2024.07.10 01:03:28+05'30
Font: PDF Editor Version: 2024.1.0



Praveen R



CMR UNIVERSITY
For the University of Madhya Pradesh by Act No. 48 of 2012

1. Introduction

CMR UNIVERSITY

VICE CHANCELLOR
Rupinder K



PRAVEEN R

Digitally signed by PRAVEEN R
DN: cn=PRAVEEN R, o=CMR UNIVERSITY, ou=ADMINISTRATIVE, postalCode=580004, st=JHARKHAND, serialNumber=684f1961b7ca445388c9464663c3999607267eecc0527827dcd6553a8b1, postalCode=580004, st=JHARKHAND, serialNumber=684f1961b7ca445388c9464663c3999607267eecc0527827dcd6553a8b1, cn=PRAVEEN R
Reason: your signing reason here
Date: 2024.07.10 01:03:28+05'30
Foxit PDF Editor Version: 2024.1.0

CMR University IT policy exists to maintain, secure, and ensure legal and appropriate use of information technology infrastructure established by the University on the campus. This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability (CIA) of the information assets that are accessed, created, managed, and/or controlled by the University. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property.

Intranet & Internet services have become most important resources in educational institutions & research organizations. CMR University took initiative during it's inception and established basic network infrastructure in the academic complex of the university.

Over the last many years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the university's academic environment.

University has about 5500 network connections covering many buildings across the campus. Internet Unit is the department that has been given the responsibility of running the university's intranet & internet services.

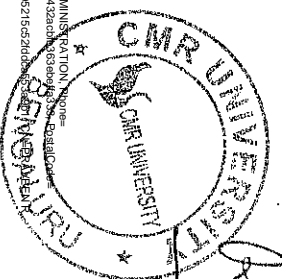
Internet Unit is running the Firewall security, DHCP, DNS, web and application servers and managing the network of the university.

CMRU is getting its Internet bandwidth from Different ISPPs at all campus. Total available bandwidth is upgraded time to time based on revised requirements from respective departments.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations.

CMR UNIVERSITY

VICE CHANCELLOR





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:

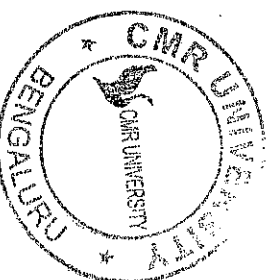
- IT Services Policy
- Data backup Policy for faculty, staff, students
- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- IT Services helpdesk policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Website Hosting Policy
- University Database Use 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.





2. IT Services Policy

CMR UNIVERSITY

VICE CHANCELLOR



7

PRAVEEN R

Digitally signed by PRAVEEN R
DN: cn=PRAVEEN R, o=CMR UNIVERSITY, ou=CMR UNIVERSITY, postalCode=580034, st=KARNATAKA, serialNumber=68d1f861b7ca445388c39996072627
Reason: your signing reason here
Date: 2024.07.10 01:32:28+05'30
Foxit PDF Editor Version: 2024.1.0

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 staffnetwork 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.

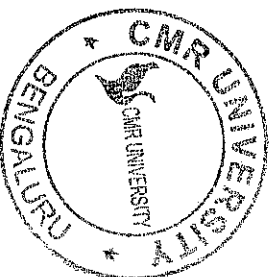
2.2.9.2 Enhancement: Working with the users and suppliers to specify, develop and test changes to existing systems as these arise.

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

CMR UNIVERSITY

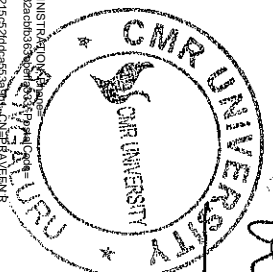
Deputy Chancellor



3. Data backup Policy for faculty, staff and students

CMR UNIVERSITY

Vice Chancellor
Praveen R





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 upto 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. Datadeemed 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:

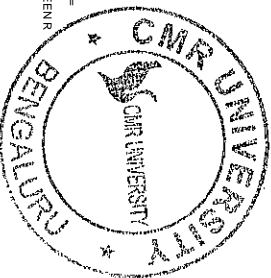
- Examination team
- Content team
- Accounts Head
- IT team
- Administration

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.
CMR UNIVERSITY

Rupke Chandra
CMR UNIVERSITY

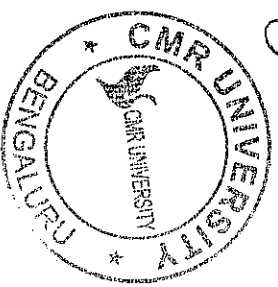




4. IT Hardware Installation Policy

CMR UNIVERSITY

VICE CHANCELLOR
[Signature]





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 **CMR UNIVERSITY** authority that the electronic waste is delivered to authorized recyclers or dismantlers annually after complete documentation is done.

15



Praaveen R
VICE CHANCELLOR

PRAVEEN R

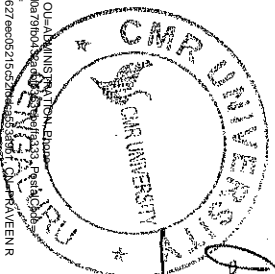


CMR UNIVERSITY

5. Software Installation and Licensing Policy

CMR UNIVERSITY

VICE CHANCELLOR



16

PRAVEEN R

Digitally signed by PRAVEEN R
DN: cn=SANKARAN, o=CMR TRUST, ou=ADMINISTRATION, postalCode=688072, st=KERALA, email=praveenr@cmru.ac.in, serialNumber=580094, surname=SAKARAN, cn=PRAVEEN R
Reason: your signing reason here
Date: 2024.07.10 01:30:28+05'30
Foxit PDF Editor Version: 2024.1.0



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.

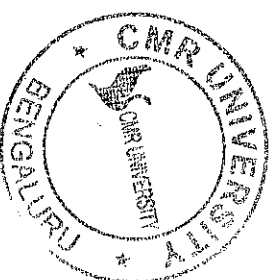
5.3 In the interests of ensuring compliance with licensing requirements, IT Department from timeto time investigates a software compliance audit.

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

CMR UNIVERSITY

VICE CHANCELLOR

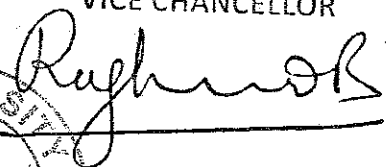


6. IT Services helpdesk policy

255 / 709

CMR UNIVERSITY

VICE CHANCELLOR



18

PRAVEEN R

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.

VICE CHANCELLOR



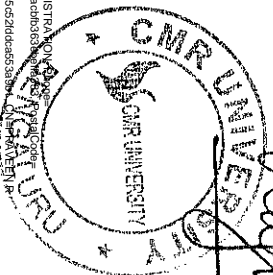


CMR UNIVERSITY

7. Network (Intranet & Internet) Use Policy

CMR UNIVERSITY

VICE CHANCELLOR





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.

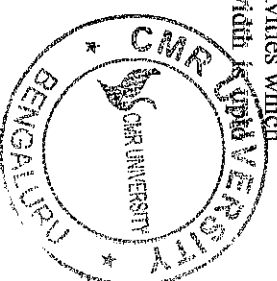
7.4.2 To access the intranet facility, each member of the university – student, research scholar, faculty and staff has been provided with a unique login ID and password, this ensures the network security from the premises outside of the university.

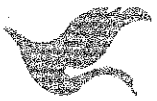
7.5 Internet Users Policy

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.

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 15Mbps.





8.1 Scope of Procedure and Rationale

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services with domain name **@cmr.edu.in**, for formal University communication and for academic & other official purposes.

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

8.3 To receive these notices, it is essential that the e-mail address be kept active by using it regularly. To use this facility faculty, staff, and students must log-in on Gmail based domain with their university's email id and password.

8.4 Students will receive their email IDs after confirmation of their admission from administrative office. IT team is supposed to create the student email IDs and their groups based on school and program. Policies to create email IDs nomenclature are mentioned in the end.

8.5 Staff(academic/nonacademic) will receive the university email ID after IT team receives the appointment confirmation email from HR team.

8.6 Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

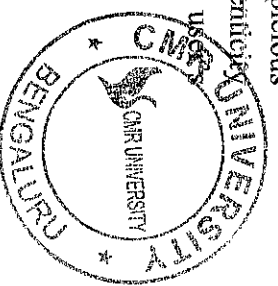
8.6.1 The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

8.6.2 Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages and generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

8.6.3 While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

8.6.4 User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.

8.6.5 User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authentic nature before opening it. This is very much essential from the point of security of the user.





CMR UNIVERSITY

9. Website Policy

CMR UNIVERSITY

VICE CHANCELLOR



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.

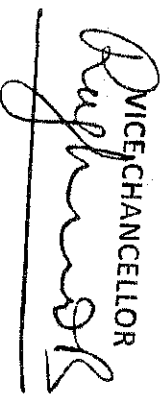
9.3.3 Any communication regarding above changes will go to the vendor through a functional in-house content team sitting at the University office.

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

CMR UNIVERSITY

VICE CHANCELLOR






10. University Database Use Policy





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 repackaged 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 of 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

CMR UNIVERSITY

VICE CHANCELLOR





CMR UNIVERSITY
Promoting the Spirit of Learning, Research, Innovation and Service

11. CCTV Surveillance Policy



PRAVEEN R

Digitally signed by PRAVEEN R
DN: cn=PRAVEEN R, o=CMR TRUST, ou=ADMINISTRATION, phone=+9198807123011, c=IN, email=praveenr@cmru.ac.in, serial=580054, s=KARNATAKA, serialNumber=68d1f861b7ca445388c3d964b4663c39996072b7
Reason: your signing reason here
Date: 2024.07.10 01:03:28+05'30
Foxit PDF Editor Version: 2024.1.0



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.

CMR UNIVERSITY

VICE CHANCELLOR





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 reports 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.

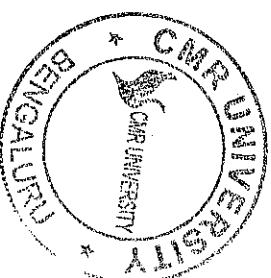
12.2 Scope

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

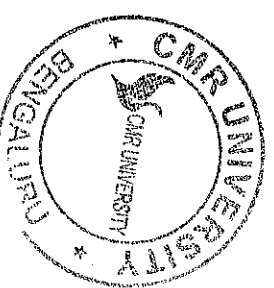
- Coordinate unit activities to satisfactorily implement or complete above unit responsibilities.
- Work with unit IT to review unit DR plans at least annually or whenever significant system architecture or personnel changes occur.
- Brief unit leadership on status of DR efforts and resources needs.
- 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;





12.6.2 Disaster Recovery Plan Template: Disaster recovery plans should follow the general content and Guidelines.

12.6.3 Disaster Recovery Review/Plan Testing: Disaster recovery plans must be reviewed annually and updated whenever a significant change to system architecture, system dependencies or recovery personnel occurs. At a minimum, an annual tabletop exercise or equivalent should be conducted that simulates the abrupt and unscheduled loss of critical functions.

12.6.4 New System Evaluation: New applications or systems will be evaluated; systems determined to be critical require a disaster recovery plan to be documented and tested prior to go-live;

12.6.5 Risk Assessment: Environments designated as mission critical must have a performed at least every four years or in accordance with the regulatory requirements of the system. Disaster recovery plans need to include mitigation of potential negative impacts to the mission critical system.

12.6.6 Data Backup: Backups are the result of copying or archiving files for the purpose of restoring them to a specific point-in-time or in the event of data loss resulting from computer viruses, hardware failures, file corruption, accidental or intentional destruction, etc. Backups preserve data integrity in the event of data corruption or other loss of the primary copy.

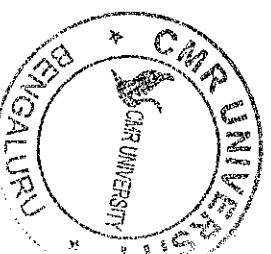
12.7 Data Backup Requirements

Data backup and restoration should include a documented process for recovery, accounting for data dependencies or relationships where data from multiple systems must be in sync or share common data elements. The method and media for data backups should allow meeting RTO and RPO requirements for restoration.

In addition to system criticality requirements, data backups are:

- *Required*, for all mission critical systems and for any system or machine that creates, processes, maintains, or stores data classified as Restricted or High. Those are ERP data, Tally Server data, Administration data, Content team creative data, IQAC data etc.
- *Recommended*, for Moderate data, and for data that cannot be recreated in a timeframe satisfactory to the owner such as Civil works team, Operations team etc.
- *Optional*, for all other systems or data.

12.8 System resiliency is a desirable objective, but is not a substitute for, and does not negate the necessity to perform, data backups and have a disaster recovery plan.





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

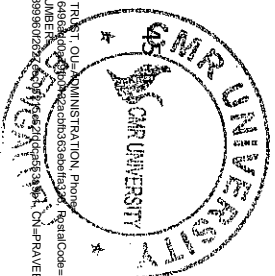
12.10.2 Any department or unit found to have violated this Standard may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.

12.11 Implementation

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

PRAVEEN R

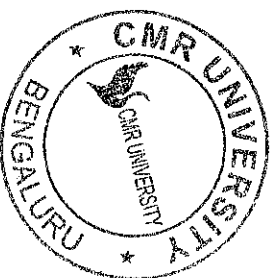
Digitally signed by PRAVEEN R, DN: cn=RA, o=CMR UNIVERSITY, ou=ADMINISTRATION, postalCode=560004, serialNumber=684f1981b7ca45388cd464e4663c3995607207, email=praveenr@cmr.ac.in, c=IN, givenName=PRAVEEN R, reason: your signing reason here
Date: 2024.07.10 01:03:28+05'30
Fossil PDF Editor Version: 2024.1.0



VICE CHANCELLOR
[Signature]



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.

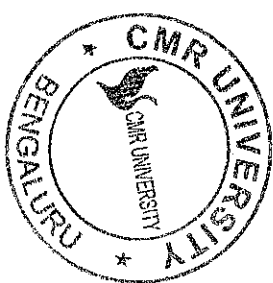
13.2 All IT enabled essential applications are on online UPS power supply. All academic blocks are having central online UPS which are with redundancy.

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.

CMR UNIVERSITY



VICE CHANCELLOR

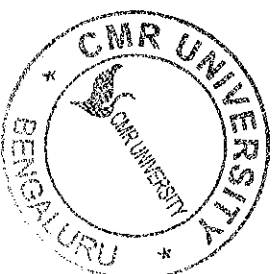




CMR UNIVERSITY
Promoting the Pursuit of Knowledge and the Development of Character

14 Cyber Security and Data Privacy

285 / 709



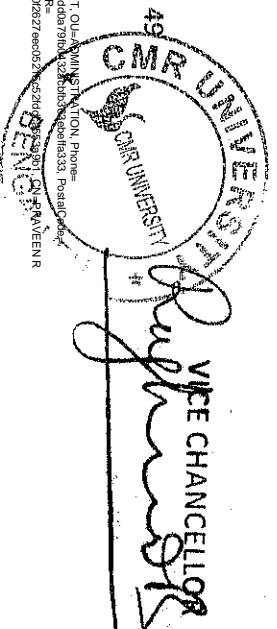
PRAVEEN R

Digitally signed by PRAVEEN R
DN: cn=PRAVEEN R, o=CMR UNIVERSITY, ou=ADMINISTRATION, phone=+9198871230111, c=IN, email=praveenr@cmruniversity.ac.in, postalCode=580054, serialNumber=6481981, cn=PRAVEEN R
Reason: your signing reason here
Date: 2024.07.10 01:33:28+05'30
Foxit PDF Editor Version: 2024.1.0



- 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.

CMR UNIVERSITY

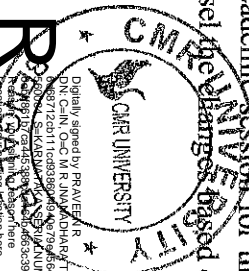




17. Review and Revision Policy

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:

CMR UNIVERSITY



Praveen R...
VICE CHANCELLOR



CMR UNIVERSITY

For the University/Institution/Department/Office by Act No. 18 of 2016

- ❖ 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)

CMR UNIVERSITY

VICE CHANCELLOR
Ruph...



292 / 709