IT POLICY

CMR INSTITUTE OF TECHNOLOGY

(UGC - Autonomous)

Approved by AICTE, Permanently Affiliated to JNTUH, Accredited by NBA and NAAC with A Grade

Kandlakoya(V), Medchal District, Hyderabad-501 401, Telangana State

Landline: 08418-200720; Fax: 08418-200240

E-mail: principal@cmritonline.ac.in Web: www.cmritonline.ac.in

May 2021

INDEX

IT POLICY

A. Objectives of IT Policy

1. The IT policy aims to maintain secure, legal and proper use of IT infrastructure by stakeholders.
2. This policy focuses on the institute-wide strategies and responsibilities to protect the confidentiality, integrity and availability of the information assets that are accessed, created, managed and/or controlled by the institute.
3. Information assets addressed in the policy include data, information systems, computers, licensed software, network devices, audio & video contents, intellectual property, digital documents and verbally communicated information.

The institute's policies and guidelines form the foundation of the IT security and effective IT policy is a sign of due diligence, IT audit & control, risk mitigation and litigations if any. Policy serves as a blueprint for implementation of security measures. This policy facilitates the use of computing facilities such as computer hardware, software, email, information resources and intranet & internet access. IT in general is dynamic in nature and reflects on operational policies that govern IT security process and to set direction, provide information about acceptable/prohibited actions/violations. Guidelines created/provided for conformance of the institute/departments, network administrators and students/staff/stakeholders that are part of institute community to understand how IT policy operates in significant areas.

B. Scope of IT policy

- Hardware Installation Policy
- Software License and Installation Policy
- Network (Intranet & Internet) Policy
- E-mail Account Policy
- Website Maintenance Policy
- Database Use Policy
- CCTV surveillance Policy

HARDWARE INSTALLATION POLICY

The institute's network users need to follow certain precautions while computers or peripherals being installed to face minimum inconvenience caused due to interruption of services.

A. Primary User

An individual in whose room the computer is installed is considered as the "primary" user. If a computer has multiple users, none of them considered the "primary" users and the department Head should depute/make a person responsible for compliance.

B. End User Computer Systems

Apart from the client PCs used by the users**,** the institute will consider servers not directly administered by System Administration Department, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. All the servers in general will be under the control of system administrator unless and otherwise specified.

C. Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty the institute may enter into an AMC with the vendor that includes OS updating and renewal of anti-virus software.

D. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected through UPS only. UPS systems should be connected to the electrical points with proper earthing and well designed and laid electrical wiring.

E. Network Cable Connection

Network cabling design and laid must be in such a way that they should get separated from the interference of electrical/electronic equipment. No other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and with read only access.

G. Re-location of Servers/Computers/Peripherals

Relocation of Computer servers/systems/peripherals are allowed only with permission of Director. System administration department maintains a record of computer identification names/number/IP address/MAC-Id/lab-name/room-number. Any deviations severely viewed which leads to immediate disconnection and will be restored on approval of Director.

H. Maintenance of Computer Systems provided by the Institute

All the computers and peripherals must be purchased through the purchase committee only and are distributed by the System Administrator and system administration department staff will attend the complaints related to any maintenance related problems.

I. Noncompliance

All the staff/students should comply with the computer hardware installation policy so as to not risk themselves and others on network related problems which could result in damage/loss of files which result in loss of productivity. An individual's non- compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

J. System Administration Department

System administration department will notify the non-compliant computer affecting the network will notify to the individual responsible for the system to restore it. The notifications sent by email/SMS. The individual users should follow-up the notification for its compliance. The system administration department will provide necessary guidance to bring the systems into compliance.

SOFTWARE LICENSE AND INSTALLATION POLICY

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. If any piracy found later, the concerned HOD is held responsible.

A. Operating System and its Updating

1. Individual users should make sure that OS/service-packs/patches installed in the devices is updated time to time and helps to fix bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Update of OS should be scheduled on Saturdays so as the day-to-day tasks are not affected.
2. Institute IT policy encourage staff/students to towards open source OS/application software.
3. Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users responsibility to make sure that the updates a being done properly.
4. Computers under institute domain controller will get Microsoft updates automatically.

B. Antivirus Software and its updating

All devices must be protected by licensed anti-virus software to monitor downloads and detect malicious/suspicious software. The antivirus software must be renewed time to time by the department/individual user on intimation to system administrator on approval of the Director.

C. Data Backup

The users should take regular backup of the vital data to protect the information from loss or from virus infections that may destroy data on an individual's computer. Without proper backups, recovery of destroyed files may not be possible. Preferably, at the time of OS installation, the computer's hard disk can be partitioned into two or more volumes typically C, D, E, F, etc. OS and other software should be on C drive and user's data files on the other drives. In case of any OS corrupted, only C drive gets affected and may be formatted. However, it is not a foolproof solution in case of virus attack. The users should take periodical/frequent backup of data on network servers/external hard drive/DVD.

D. Noncompliance

Staff/students not compliant with the security policy leave themselves & others at risk of virus attack and may results in damage/loss of files. Inoperable computer result in loss of productivity/ risk of spread of infection to others confidential data may be revealed to unauthorized persons. An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

E. System Administration Department

System administration department will notify the non-compliant computer affecting the software will notify to the individual responsible for the system to restore it. The notifications sent by email/SMS. The individual users should follow-up the notification for its compliance. The system administration department will provide necessary guidance to bring the systems into compliance.

NETWORK (INTRANET & INTERNET) POLICY

Network connectivity provided in the campus, referred to hereafter as "the Network", either through an authenticated-network-access or VPN connection governed by IT Policy.

The system administration department is dedicated for the maintenance/support of the campus network and internet/intranet applications. Problems of the campus network should be reported to system administration department on it.support@cmritonline.ac.in to trouble shoot.

A. IP Address Allocation

Any computer (PC/laptop/Server) connected to the campus network is identified by the IP address assigned by the system administration department. IP address is allocated using DHCP/ manually depending upon the requirement/need. Computer connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where the computer is connected will bind internally with that IP address so that no other person uses that IP address unauthorized from any other location. For any IP base device like network printer, smart TV, bio metric machine, CCTV DVR, IP Camera, Video conferencing device, IP Phone etc. to be installed at any location the concern user should contact system administration department and get proper IP Address.

B. DHCP and Proxy Configuration by Individual Departments /Sections/ Users

Use of any computer at end user location as a DHCP server or Wi-Fi router to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the institute. No individual should configure proxy servers as it may cause interference with the institutions proxies. Even configuration of any computer with additional network interface card or creating Wi-Fi hot spots and connecting another computer to it is considered as proxy/DHCP configuration. Non- compliance to the IP address allocation policy will result in disconnection of the port from the network and restored on approval of the Director.

C. Running Network Services on the Servers

The computer systems are connected to the campus network only on written approval from the system administrator and may run on LAN/WAN server-software, e.g., HTTP/SMTP/FTP/ Web server, any violation leads to permanent termination of connection. System administration department is solely responsible for the content of machines connected to the Network and any potential threats detected through firewall/anti-virus also liable to termination of server/ client. The client machines may also be disconnected against unfair/restricted practices including remote servers/networks. Campus network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons at Campus. Impersonation of an authorized user to the Network server is severely viewed/ punishable.

D. Wi-Fi/Cellular/Dial-up/Broadband Connections

Wi-Fi routers, mobiles, USB Broad band modem, Computer systems or any such devices that are part of the institute's campus-wide network, whether institute's property or personal property, should not be used for Individual-external dial-up/broadband connections, as it violates the institute's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

1. This policy applies, in its entirety, to departments/labs (division) in wireless local area networks. In addition to the requirements of this policy, Department, departments, labs, Research Centers, Project-Labs must register each wireless access point with System administration department with Point of Contact information.
2. Department, departments, or divisions must inform System administration department for the use of radio spectrum, prior to implementation of wireless local area networks.
3. Restricted/shared access to Wireless LAN of Department, departments, or divisions will be regulated for authentication/MAC/IP addresses/Passwords.
4. If any individual Department wants to utilize inter-building wireless LAN/WAN have to obtain permission from System administration department & Director.

F. Internet Bandwidth Obtained by Other Departments

Internet bandwidth acquired by any Section, department of the institute under any research program/project should ideally be pooled with the institute's internet bandwidth, and be treated as institute's common resource. All the computer systems using special network need to have separate IP address and make use of the institute gateway. Such networks should be adequately equipped with necessary IT security measures as prescribed in IT policy. The blue print of the network design with IP address scheme should be submitted to System administration department.

G. Un-authorized Network expansion

Any user or department is not allowed to connect additional desktop network switch as it may create loops or unwanted traffic. The user/department should get approval from System administration department to connect additional devices, any violations leads to suspension of network and penalty as per IT security policy.

H. Internet Access

In general internet access is available to all computers, laptops, servers, mobile devices and other IP based devices which are authorized to connect to the campus network.

It is responsibility of the individual to access Internet in the ethical and legitimate manner. Sometimes the user may be unaware of the risks while accessing some websites/web applications/apps and the computer may get affected with virus/malware/adware/expose vulnerability. Hence the users are categorized as faculty, UG/PG students, admin/clerical/ technical staff, administrators, officers and others. Depending on the category of users the internet access will be filtered at firewall so that intentional/unintentional access to malicious websites/web applications will be avoided by default.

In general on administrative grounds, most of the websites are blocked by the firewall; on special request from the individual/section/department system administration department take necessary action after verifying the need, authenticity and safety.

Wi-Fi IMPLEMENTATION AND USAGE POLICY

A. Applies to all Stakeholders of on/off campus

- Students: UG, PG, Research
- Staff: Teaching, Technical, Non-Teaching and adhoc
- Higher Authorities and Officers
- Management Members
- Board of Governors
- Eminent Guests
- Vendors.

B. Resources

- Wi-Fi Access Points/routers installed by CMRIT
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Multimedia Contents

Wi-Fi facility is implemented for the above mentioned stakeholders in the campus. For uniform, efficient and solicited usage of the Wi-Fi the following policies are defined:

C. Wi-Fi Access and locations

1. All the buildings/blocks/floors in the campus are installed with Wi-Fi access points to facilitate access. Furthermore, the Wi-Fi facility may be made available at many places like canteen, library, hostel, corridors, laboratories, classrooms, departments, auditorium, seminar halls, etc.
2. Wi-Fi Access Points may be temporarily made available on demand for conference, workshops, symposia and any other important events.
3. Personal Wi-Fi Access devices are strictly prohibited as such devices may cause disturbance in IP allotment and security threat to CMRIT's Network. If found the personal devices may be confiscated by system administration department.
4. In special cases the individual/department may approach to system administration department and get proper secure configuration and registration to the personal/department's access points or routers.

D. Authentication/Authorization/Activity Logs for Wi-Fi users

The system administration department authenticates the users and authorizes them to use Wi-Fi facility to prevent the unauthorized access, activity logs helps the system administrators to assess the usage. A onetime registration/identification policy is devised to authorize devices/users of Wi-Fi.

1. Device identification by MAC and user identification by Employee ID, as a one-time process. Necessary Data is collected from administration/accounts by system administration department.
2. UG/PG students are given Wi-Fi access based on their HT number. On one time registration the device of the student is registered for the period depending on their course in prescribed

format. After completion of the course the user will be automatically deleted from the system.

3. An extendable free open OTP based Wi-Fi is available for guest users for sixty minutes.

E. Changes/ Modifications in the user details

1. In case a mobile device is lost/stolen/sold/transferred the user should intimate the system administration department.
2. For Wi-Fi access to new mobile device an employee should intimate the new MAC Id of the device to system administration department through official email id only. System administration department will modify accordingly.
3. For Wi-Fi access to new mobile device a student should intimate the new MAC Id of the device to system administration department by an application forwarded through the respective HOD.

F. Wi-Fi Usage

1. The individual user will be responsible for the Wi-Fi usage made.
2. Solicited and ethical usage is expected from the users.
3. The internet access through Wi-Fi is filtered access. Possible phishing, spurious, unsolicited/ obscene, gaming, shopping/multimedia streaming site are blocked at firewall.
4. Students access in limited with fixed daily data usage.
5. There shall be a unlimited browsing with shared access.
6. The users will access the CMRIT resources properly and should not harm the resources.

G. Misuse and actions

1. If a user/device is found to harm resources/other users by malicious software/application/ virus, then such a user will be warned by system administration department. User's intention and device are verified and the details are passed on to respective HOD for necessary action as per cyber law.
2. A virus infected device may create noticeable network problem or attempt for cyber-attacks, the users will be notified and the access shall be blocked until the infected device is cleaned/free from viral attack.

E-MAIL ACCOUNT POLICY

Utilize only institute email services for efficient dissemination of formal academic/administrative communication to all departments/cells/institute staff/students/stakeholders.

Email services meant for formal communications such as notices, circulars, administrative/HR/ event information, official announcements, policy messages & documents to students/staff/ stakeholders.

It is essential that the user should check email daily for notifications; otherwise the account will be deactivated after 15 days from the last login. Staff also should use this facility by log on to http://cmritonline.ac.in/mail with their user ID and password.

The user should contact system administration department with filled in application to obtain the institute's email account.

By use of institute email facility, the users agree to abide by the following policies:

1. The facility is meant for official purposes and should not use for illegal/commercial purposes (unlicensed/illegal copying/distribution of software/bulk-mails/ threatening/harassing/abusive/ obscene/fraudulent messages/images). Any violation may leads to suspension of account.
2. Avoid use of large attachments in emails and should clean the mail box regularly to receive notifications and limit to 80% of storage space to avoid bounce of mails/attachments.
3. The user should not open suspicious mails & attachments even from known sources as such mails leads to potential threat and may damage the valuable information on your device/system.
4. Users should configure messaging software on the device to enable periodical downloads of mails on to their computer to release the servers disk space. Users should keep a backup of mails.
5. User should not share their email account details with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
6. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
7. Do not peep into other mail accounts if by chance they kept open. Ethically sign out of all the email accounts kept open, before they sign-in into own account.
8. Impersonation of others email account is a serious offence and summoned for prosecution.
9. It is the users responsibility to keep their email account free from risks/threats/violations of institute's email usage policy.
10. Any Spam mail received by the user should be forwarded to spam@cmritonline.ac.in to block and any mail wrongly stamped as spam should be forwarded to wrongspam@cmritonline.ac.in to unblock.

The above laid down policies are broadly applicable even to the users of other email service providers i.e., hotmail.com, yahoo.com, gmail.com, etc., as long as they are being used from the institute's campus network, or by using the resources provided by the institute to the individual for official use even from outside.

WEB SITE HOSTING POLICY

1. Official Pages

Institute, cells, departments, clubs, professional chapters and associations of staff/students may have own pages on CMRIT's intranet channel of the official webpage. Official WebPages must conform to the CMRIT guidelines for web hosting. As on date, the CMRIT's webmaster is responsible to maintain the official web site of the CMRIT viz., http://www.cmritonline.ac.in only.

2. Personal Pages

The CMRIT provide limited number of pages to each cell/department/club/professional-chapters/ technical-associations of staff/students to showcase their talent, strength, caliber, creativity and innovations in organizing various courses/programmes/events/publications/conferences/TTPs/ seminars/workshops/symposiums/R&D activities. The individual/department requirements are addressed by web development and maintenance committee for their web-pages/URL-link/QR-code on submission of their request through Director to link on official web site of the CMRIT. However, illegal or improper usage will result in termination of the web-link and prosecuted. The contents of web pages regulated by IPR laws and not to be used for any other purpose. The information provided through this web link must not be contradictory/controversial to government. Hosting of guest pages is prohibited and content owners are responsible for any violations.

3. Affiliated Pages

Faculty can host web pages for "affiliated" professional organizations on institute web servers on approval of Director. Individuals/departments/cells reserve the right to continue the web services.

4. Web Pages for eLearning

Digital literary resources of the faculty such as syllabus, academic calendar, time tables, course file, e-resources, hyperlinks, question banks, quiz, assignments, etc through department web pages. Students may host web pages/links for clubs/chapters under the supervision of mentor/HOD and should not mislead/misinterpret any information as institute website viewed by many stakeholders.

5. Servers

It is recommended that pages be placed on the information server, but pages developed for classes also may be placed on departmental servers or the main campus server meant for eLearning.

6. Maintenance

The pages published/maintained on the eLearning information server shall follow default rules for personal eLearning pages. The web manager shall maintain servers for eLearning purpose.

7. Policies for Maintaining Web Pages

All individual/department/cell/chapter web pages are in corollary with CMRIT's vision & mission and are required to announce their web presence by a mail to webmaster@cmritonline.ac.in and the announcement should include (i) The URL and (ii) A brief explanation of content or purpose of the pages (i.e., Web pages for an administrative or academic unit, etc.). The primary page must include a link to the CMRIT home page and, if applicable, contain additional links to the sponsored organization or department.

DATABASE USE POLICY

All the databases of the institute are maintained by the systems administration department. The data is vital, voluminous, enormous, critical & important in many aspects and its use must be protected. CMRIT has its own policies regarding the creation of database and access to information and a more generic policy on data access.

1. **Database Ownership:** CMRIT is the database owner of the entire data generated in the institute.
2. **Custodians of Data:** Individual departments are custodians for their respective data.
3. **Data Administrators:** Data administration of the department(s) delegated to respective HOD.
4. **MIS Components:** For the purpose of e-Governance, MIS broadly categorized as follows:

   - Manpower Information Management System (MIMS)
   - Students Information Management System (SIMS)
   - Financial Information Management System (FIMS)
   - Physical Resources Information Management System (PRIMS)
   - Project Information Monitoring System (PIMS)
   - Library Information Management System (LIMS)
   - Learning Management System (LMS)
   - Document Management and Information Retrieval System (DMIRS)

Database Policy guidelines for departments, cells, chapters, administration and other data users:

1. Do not allow the distribution of data that is identifiable to a person outside the institute.
2. Data collected by institute/departments/staff/students must be used for internal purposes only.
3. The data sharing by individual/department is allowed only to discharge of their duties/ responsibilities being a head/in-charge of any department/cell to any affiliating body.
4. Any data sharing by the individual to the external agencies what so ever may be the reason must obtain prior permission through proper channel.
5. Direct sharing of data by staff/students against legal-issues/court-cases to the advocates/courts strictly prohibited and the required data may be furnished by the HOI to courts under RTI.
6. All reports to JNTUH/AICTE/UGC/NBA/NAAC/TSGOVT shall be submitted by the HOI only.
7. Database users can repackage on approval to share the data to other users and inform the same.
8. Tampering of the data/database/reports/forms in any manner treated as gross violation of IT security policy and liable for prosecution. Tampering may includes and not limited to

   - modify/delete the data items or software components by using illegal access methods.
   - modify/delete the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
   - cause database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
   - try to break security of the database servers.

   Such data tampering actions by institute member or outside members will result in disciplinary action against the offender by the institute authorities.

VIDEO SURVEILLANCE POLICY

A. The Video Surveillance System

The system comprises of fixed/pan-tilt/zoom cameras, monitors/multiplexers/digital recorders, SAN/NAS storage, public information signs, etc. Cameras are fixed at strategic/vulnerable conspicuous-main locations of the campus with signboards and there are no hidden cameras placed. All the stakeholders are advised to take care of themselves/belongings. The systems recordings are not for upload on world-wide-web/DSS/covert recording unless specified by HOI.

B. Need for the system

The system aims to reduce crimes & ensure campus protection/safety through a well established control room equipped with sophisticated equipment and well trained security; and

- Deter physical/psychological criminal intent and assist in the prevention/detection of crimes.
- Identify & prosecute offenders, initiate disciplinary proceedings/warrants as per Govt. norms.

C. Covert recording

Covert cameras may be used by security on administrative approval of HOI to prevent/identify the suspected behaviour of individuals on unauthorized activity and the recordings are documented.

D. The Security Control Room

A round the clock surveillance system is in place to monitor the movement of individuals and capture unwanted/suspicious recordings/images in the campus with restricted access to the display-monitors. Students/staff/visitors/police-officials may be granted access to the control room to check footage on approval from the Director. Individuals who verify footage should enter their details in the logbook.

E. Recording and access to images

All recordings are in real time and in lapse mode. The Images will normally be retained for a maximum of fifteen days from the date of recording and then automatically over written. All required/doubtful recordings are safely stored at the discretion of HOI. Individuals/third-party-agents/ officials can access the recordings through RTI cell.

The details of disclosure of recorded material will be limited to the following authorities:

- Law & Order/RTI/Nirbhaya/Disha/Media/CID officials on approval from management.
- Prosecution agencies, relevant legal representatives/assignee on approval from the HOI.
- Suspicious recordings would be retained till prosecution/file closed/withdrawal of petition.
- Emergency services in connection with the investigation of an accident.

F. Access to images by a subject

CCTV/IP camera digital images related to recognizable person(s) are entitled to demand a copy of such recordings subject to the Data Protection Act and no individual should influence/coerce in any manner any of the persons in the institution. All recordings can be obtained through RTI Cell only on payment of prescribed fees, if any and institute reserves all the rights unless and otherwise judicial.

G. Complaints

All complaints against the existing surveillance system should be reported to AO, CMRIT for necessary action in consultation with security control room and on approval of HOI.

USAGE POLICY

A. Computer Usage

The purpose of this policy is to protect institute's computer & network usage by stakeholders. Inappropriate use exposes the institute to risks, virus attacks, hacks, compromise of network-systems-services and legal issues. Access of computer & network usage to the stakeholders to be treated as a privilege service and all the users are expected to be positive in use of cyber space by CMRIT community. Any violation to this policy is liable for prosecution and may be punishable.

B. Acceptable Use Policy

The usage of IT resources/networks is free for stakeholders in support of e-governance/lifelong education and inappropriate use may jeopardize interests of CMRIT. Policy covers IT services such as email, internet, voice, mobile IT equipment, etc applicable to all users. This policy applies to all information available on website/servers/cloud in whatever form related to CMRIT own & other academic/administrative activities/communications.

Unacceptable uses include, but are not limited to, the following:

1. Use of resources for any other purpose other than mentioned in IT policy of CMRIT.
2. Bulk use of data to send/store chain-letters/sales/advertising/broadcasting/commercial purpose
3. Misinterpret/mislead/impersonated/masquerade information.
4. Hacking, cracking, snooping, injection & phishing on the network and intercept/alter data packets.
5. Reproduce/distribute/copy/modify/damage of any material/content of CMRIT.

C. Computer Access Control – Individual's Responsibility

Individual access to the devices is authenticated by user ID, password and accountable for their login.

Individuals must not:

1. Disclose their username, password, leave the system logged-in and masquerade/fabricate.
2. Cross authentication/limits and connect any objectionable devices to the network/systems.
3. Make a copy of official data or store unauthorized data and share any software with outsiders.

D. Internet and email Conditions of Use

All users are accountable for office internet & email for academic and administrative purpose only.

Individuals must not:

1. Use for harassment/abuse/profanity/obscenities/derogatory remarks in communications.
2. Access/download/send/receive any offensive data such as pornography, gender discrimination.
3. Use for gain/gamble/betting/cross-word puzzles/entertainment/shopping/gaming/chain-letters.

4. Place any negative comments/opinions/rumors/gossips of any kind about institution.
5. Store/download/retrieve/share/send any unprotected sensitive confidential information to anyone.
6. Breach IPR in any manner and use objectionable devices.

E. Clear Desk and Clear Screen Policy

This policy helps to reduce the risk of unauthorized access or loss of information as follows:

1. Confidential-academic-administrative information and network devices must be protected.
2. Switch computers to sleep-mode and shutdown when not in use.
3. Do not leave original-confidential-material at printer/photocopier/scanner shelves.
4. All extra confidential printed materials must be disposed as per the institute policy.

F. Working Off-site

It is accepted to make use of office laptops and mobile devices outside the campus with password protection i.e. off-site and the following precautions must be observed and followed.

1. Working away from the office must be in line with (CMRIT) remote working policy.
2. Any IT/ICT equipment taken off-site by a staff member should be ensured of safe custody.
3. Laptops must be carried as hand luggage while travelling.
4. Information should be protected against loss or compromise when working remotely.

G. Mobile Storage Devices

Mobile storage devices such as memory sticks, CDs, DVDs and external hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only (CMRIT) authorized encrypted mobile storage devices must be used while transferring sensitive or confidential data.

H. Software

Employees must use only software that is authorized by CMRIT on institute's computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All approved software on computers must be and installed by the system administrator.

I. Storage

Staff / students should not store personal/private data & files such as music, videos, photographs or games in servers/storage equipment of the institute. At the same time staff/students should not bring their personal equipment of any nature without proper permission from security and systems administrator.

J. Virus Protection

CMRIT has implemented centralized, automated virus detection and anti-virus software updates within the campus. All systems have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

1. Remove or disable anti-virus software.
2. Attempt to remove virus-infected files or clean up an infection on their own.
3. Install unauthorized anti-virus solutions.

K. Conditions to use Voice Equipment Facilities

Use of CMRIT's voice equipment is exclusive for academic and administrative purposes. Individuals are restricted to use institute's voice facilities for private communication, but for exceptional cases.

Individuals must not

1. Use CMRIT's voice equipment for conducting private academic and administrative, making hoax or threatening calls to internal or external destinations.
2. Accept reverse charge calls from domestic or International operators.

L. IT privacy policy against Termination of Contract/Course completion/Service

1. All equipment and data of CMRIT such as laptops and mobile devices including telephones, smart phones, USB memory devices and CDs/DVDs, must be returned to systems administrator on approval of HOD at the time of termination of contract/course-completion/service.
2. All data or intellectual property developed or gained during the period of employment remains the property of CMRIT and must not be retained beyond termination or reused for any other purpose.

M. Monitoring and Filtering

1. All the data that is created and stored on institute's computers is the property of CMRIT only and there is no provision for individual data privacy.
2. Systems administrator of CMRIT has all rights to enquire/inquire/investigate/detect/ confiscate/disable login permanently and bring to the notice of the Director CMRIT.
3. Any monitoring, audit and any internal control process shall be in accordance with existing IT Policy in additional to judicial and operating precedents.
4. This policy must be read in conjunction with information Technology (IT) Policy of CMRIT prevailing at that time.

It is individual responsibility to report suspected breaches of security policy without delay to computer center and System Administrator through proper channel. Any breach to IT policy of CMRIT shall lead to investigation to prove misconduct and disciplinary action may be initiated.

RESPONSIBILITIES OF SYSTEM ADMINISTRATION DEPARTMENT

A. Campus Network Backbone Operations

The campus network backbone and its active components are administered, maintained and controlled by system administration department. It operates/provides necessary and demanding services to the Institute sections, departments, and divisions covered by the campus network backbone to the best of its practices.

B. Physical Demarcation of Campus Buildings' Network

1. Demarcate/connect/terminate network for existing and newly constructed buildings is the responsibility of system administration department. The manner in which the buildings are to be connected to the campus network backbone is a matter of concern of the department.
2. It will consult with the client(s) to ensure that end-user requirements and integrity of the campus network.
3. The department actively examines and monitors the internet activity on the network to optimize traffic on the Institute's Internet links.

C. Network Expansion

Network expansion/modernization/renovation is the responsibility of system administration department which reviews the existing networking facilities time to time on approval.

D. Wireless Local Area Networks

1. System administration department provide network connection through wireless technology in addition to Fiber Optic/UTP at all possible locations.
2. System administration department is authorized to consider the applications for the use of radio spectrum and setup the same on approval.
3. System administration department is authorized to restrict network access to the Sections, departments, or divisions either via authentication or MAC/IP address restrictions.

E. Electronic logs

Electronic logs are created/retained/destroyed for monitoring of network traffic/administration.

F. Global Naming & IP Addressing

System administration department has right to provide IP addressing and domain name services.

G. Providing Net Access IDs and email Accounts

System administration department provides Net Access IDs and email accounts to the individual users on request with prescribed format.

H. Network Operation Centre

The system administration department is responsible for the operation of a centralized Network Operation Control Center round the clock. All network failures, excess utilization; non-intrusive monitoring and network traffic in regular intervals will be monitored & resolved by the system administration department and report the same as the case may be to higher authorities.

I. Network Policy and Technology Standards Implementation

The system administration department is authorized to take necessary steps to ensure network compliance/standards designed to protect the integrity and security of the network.

J. Receiving Complaints

Any complaints related to computer systems and network related issues received by the system administration department will be resolved instantaneously on approval from higher authorities and a Log book shall be maintained to this affect.

K. Scope of Service

The system administration department will be responsible only for solving the hardware/software/ network related problems or services.

L. Disconnect Authorization

The system administration department is authorized to disconnect any section/department/ division/cell/user with/without any notice for the network violations and reconnect on proper approvals and requests.

M. Maintenance of Computer Hardware & Peripherals

System administration department is responsible for maintenance of the institute owned/allowed computer systems and peripherals that are either under warranty or annual maintenance contract.

N. Installation/Reinstallation/Upgrade of Software/OS

1. System administration department is authorized to install legal/licensed/open-source software and should not encourage installation of any unauthorized software in the computer systems of the institution by the end users. They should strictly refrain from obliging of such requests.
2. System administration department is authorized to format/reformat/install/re-install of any OS /application-software/patches/anti-virus and necessary care should be taken to restore the data, hostname, IP address, network mask and gateway.
3. A backup of data must be taken before reformatting the hard disk and restore the same after proper re-installation. Under no circumstances, software files from the infected hard disk should be restored back on the newly formatted hard disk(s).

RESPONSIBILITIES OF ADMIN UNITS/DEPARTMENTS/ SECTIONS

A. Responsibilities of Administrative Units

System Administration Department collect the latest information from all the administrative units of the institute to provide network and IT facilities to the new members and withdrawal of permissions from those who are leaving the institute and update the same in the official website.

The information required is broadly of the following nature:

- New Appointments/Enrolments/Promotions.
- Superannuation/Termination of Services.
- Expiry of Studentship/Removal of Names from the Rolls.
- Restriction on use of network facilities to any user against orders issued by the institution.
- Important Events/Developments/Achievements.

B. Responsibilities of Departments or Sections

1. User Account

The new user account will be activated by System Administration Department, upon a request in prescribed format through proper channel. Once a user account is activated the user is personally responsible for any violations against to the institute's policy and pride. If users find any difficulty to access the network, the department provides necessary training. It is mandatory for all the users to go through the IT policy of the institute and follow the guidelines.

2. Logical Demarcation of Department/Section/Division Networks

Each Section, department, or division should provide a Single Point of Contact (SPoC) and communicate the same to System Administration Department so that department can directly contact in case of any network/system related problem at its end. The SPoC is responsible to operate and maintain the network effectively and efficiently without any disturbance/overlapping to other network segments.

3. Supply of Information by Section, Department, or Division for Publishing on/updating the CMRIT Web Site

All the sections/departments/centers/cells/divisions should provide updated information concerned to their department through SPoC time to time. A hardcopy of such information duly signed by the competent authority along with a softcopy of the same must be sent to the System Administration Department. This policy is applicable even for all official external and internal correspondence including LMS and digital literature to be hosted in website.

4. Setting up of Wireless Local Area Networks/Broadband Connectivity

a) Notwithstanding with anything each and every sections/departments/ centers/cells/ divisions has to obtain network access through proper channel on approval. Further all sections/departments/centers/cells/divisions has to maintain proper records/documents/ files/digital documents for ready access in case they are stored in cloud.
b) Institutes IT Policy does not allow any broadband connections within the campus.
c) All sections/departments/centers/cells/divisions must secure proper permission for the use of radio spectrum/WLAN from System Administration Department. Network access must

be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

5. Security

Network security issues are to be resolved by Single Point of Contact of the originating department in coordination with System Administrative Department.

6. Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the institute are the property of the institute and are maintained by System Administration Department.

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

- Removal of network inlet box.
- Removal of UTP cable from the room.
- Opening the racks, changing the connections of the ports at jack-panel/switch level.
- Taking away the UPS or batteries from the switch room.
- Removal/renovation/dislocation/displacement of any network access component/ peripherals is strictly prohibited and any violation leads to prosecution followed by remedy/performance.

7. Add-ons to the Existing Network and Cabling

No add-ons to the existing network are allowed by individuals/sections/departments/ centers/cells/divisions under any circumstances.

All the new facilities in campus need to have the structured cabling against blue prints of building plans, surface/underground electrical/telephone cabling for LAN/WAN as a part of the campus layout. All such network cables/hubs/drivers should strictly adhere to the ISO standards.

8. Campus Network Services Use Agreement

The “Campus Network Services Use Agreement” should be read and accepted by all the members of the institute who are covered under the policy. In general all the staff, students, visitors, guests, hosts and stakeholders are members covered under this agreement and no ignorance of IT policy is excused for any user.

9. Enforcement

System Administration Department periodically scans the Institute network for provisos set forth in the Network Use Policy. Failure to comply may result in discontinuance of service.

GUIDELINES FOR COMPUTER NAMING CONVENTIONS/RUNNING APPLICATION/INFORMATION SERVERS

A. Guidelines on Computer Naming Conventions

Naming conventions are essential to address network issues and to extend necessary timely service. In general all network systems/computers names are assigned by System Administration Department only. It is the sole discretion of the department to consider any other requests.

All the computers should follow the standard naming convention:

Ex: CMRIT/CSE/202/Sys-1 where CMRIT-Institute name, CSE- department, 202-room no, Sys-1- desktop/laptop/server-sequence number.

B. Guidelines on Running Application or Information Servers

Section/Departments may run an application or information server and other retail users can run with prior approval from System Administration Department.

Responsibilities for Those Running Application or Information Servers:

- Those who run an application/information server are solely responsible for maintaining servers.
- Ownership of server content/services must follow standards/purpose of IT policy of the institute.
- IP address/Host name/DNS are manually allotted by System Administration Department.
- Ensure that the servers are protected against virus-attacks/intrusions/phishing/threats/ malware by installing standard firewalls and anti-virus software.
- Operating System and security software should be updated time to time.
- Sections/departments/centers/cells/divisions running application/information servers should solve own network issues within their scope in addition to System Administration Department.

GUIDELINES FOR HOSTING WEB PAGES ON THE INTERNET/INTRANET

A. Mandatory

1. Provide the official e-mail address of the website administrator.
2. Provide a link to the CMRIT home page from the parent (department of origin) home page.
3. Provide a link to the parent home page (Return to department's home page) on all supporting local pages.
4. Maintain records of proof-read pages of the web content before publishing on the website and update website content/test links time-to-time.
5. Design user friendly web-pages and with mobile device compatibility.

B. Recommended

1. Provide timely information to update website.
2. Provide a section indicating 'What's New'
3. Provide a caution statement if link will lead to large pages/images.
4. Indicate restricted access where appropriate.
5. Avoid browser-specific terminology.
6. Provide link text that is clear without the link saying **'click here'** whenever hyperlinks are used.
7. Maintain visual consistency across related pages.
8. Provide a copyright statement (if and when appropriate).
9. Keep home pages short and simple and provide links to mentioned pages.
10. Avoid using large graphics or too many graphics on a single page.
11. Provide navigational aids for Link to Home, Table of Contents, Next Page, etc.
12. Design web pages with ease of maintenance by any authorized person.
13. Avoid active links to pages that are in development. Place test or draft pages in your 'test', 'temp', or 'old' subdirectory. Remember that nothing is private on the Internet: unlinked pages in your directory may be visible.
14. Check finished page with a variety of browsers, monitors, and from both network and modem access points. It is also recommended to check pages with a Web validation service.
15. Keep in mind all categories of users with high and low speed browsers/modems

GUIDELINES FOR DESKTOP USERS

A. Guidelines for users of the computers in the campus network

To forestall hackers and unauthorized users of campus network IT Policy identified the following guidelines to strengthen security and safe guard users.

B. Recommendations

The following recommendations include:

1. All computers should be installed with recommended antivirus software with scheduled updates of virus definitions from the central server.
2. All computers should be installed with institute recommended OS/patches/drivers and updated time to time.
3. All computers should have a secured administrator and user login.
4. The password must be an alphanumerical one with following conditions
    a. minimum of 6-8 characters in length
    b. include punctuation such as ! $ % & * , . ? + - =
    c. must start and end with letters
    d. must not include the characters # @ ' " `
    e. must be new, not used before
    f. Avoid using names of family members/vehicles/assets/houses/offices/places/DOBs.
    g. Change passwords periodically and also when suspected.
    h. Never use 'NOPASS' as your password
    i. Do not leave password blank
    j. Make it a point to change default passwords given by the software at the time of installation
5. The guest account should be disabled.
6. New machines should activate the built-in firewall and all users should protect their data from virus attacks/phishing/hacking/threats.
7. All the users should take the help of System administrative department for installation and re-installation to secure and protect their existing data.
8. Follow guidelines of System Administration Department as a regular backup strategy.
9. System Administration Department will take care of shut the port Off/On in case of compromise of the systems. Till the time the compromised system will be isolated from network.
10. If department has its own servers, System Administration Department technical personnel can scan the servers for vulnerabilities upon request.

———

CMR INSTITUTE OF TECHNOLOGY
UGC AUTONOMOUS
(Approved by AICTE, Permanently Affiliated to JNTUH, Hyderabad, Accredited by NBA and NAAC with 'A' Grade)
Kandlakoya (V), Medchal Road, Hyderabad – 501 401

CAMPUS NETWORK SERVICES USE AGREEMENT

Read the following important policies before applying for the user account/email account. By signing the application form for IP addresses allocation/Net Access ID (user account)/email account, you agree to act in accordance with the IT policies and guidelines of CMRIT. Failure to comply with these policies may result in the termination of your account/IP address. It is only a summary of the important IT policies of the institute. User can have a copy of the detailed document from the Intranet (viz.http://www.cmritonline.ac.in/CMRIT_ITpolicy.pdf). A Net Access ID is the combination of a username and a password whereby you gain access to Institute computer systems, services, campus networks, and the internet.

I. Accounts and Passwords

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID is password protected. The User should not share the password or Net Access ID with anyone. Network ID's will remain only for active students, staff and stakeholders. Net Access ID and associated files will be deactivated for the students, staff and stakeholders who are not currently affiliated to the Institute.

No User will be allowed more than one Net Access ID at a time except to those staff hold more than one portfolio.

II. Limitations on the use of resources

On behalf of the Institute, System Administration Department reserves the right to disable the Net Access ID of any user on violation of storage restrictions intimated time-to-time.

III. Computer Ethics and Etiquette

The User shall not attempt to override or break the security of the Institute computers, networks, or machines/networks accessible there from. Services associated with the Net Access ID shall not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk e-mail messages comes under IT Policy violation. It should be noted that for any cyber offences from any network id will be prosecuted under local govt. norms in addition to institute's image.

In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

User's Net Access ID gives access to e-mail, and campus computing resources. The use of these resources must comply with Institute policy and applicable. Electronically available information

1. should not contain copied material or software unless it is from open source,
2. should not violate the Institute policy of prohibiting sexual harassment,
3. should not be used for any commercial use,
4. should not represent the institute/others without appropriate permission as the case may be,

5. should not contain material/software which violates pornography laws,
6. should not contain algorithms or software which is transferred under violation of cyber laws,
7. should not contain scripts/code that could cause a security breach under Institute policy,
8. WWW pages should clearly show identifying information of the owner of the page and we suggest that it also show date of last revision and an address (e-mail or postal) for correspondence. System Administration Department equipment does not support use of scripting in individual pages.

IV. Data Backup, Security and Disclaimer

System Administration Department is not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of user.

System Administration Department provides technical assistance to the user(s) to resolve network/computer related issues. Though System Administration Department put necessary efforts to upkeep/restore data integrity, security and privacy; it is the onus of the user to keep backups of files/data under the assigned Net Access ID, storage space and email account.

The user is held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold the System Administration Department of CMRIT against the loss of damages both by way of performance/remedy.

V. Account Termination and Appeal Process

Accounts on CMRIT network systems may be terminated or disabled without any notice or assigning any reasons. However, as a formality System Administration Department will notify the disabled-user about the process of enabling account if there is a chance.

If the user feels such termination is unwarranted, that the user may be given a reasonable opportunity to be heard to appeal for re-allotment of network access id through proper channel to the System Administration Department. Disabled users may note that the Institute's Network Security System maintains a history of infractions/violations and will be considered for decision regarding re-allotment/suspend/dismiss.

CMR INSTITUTE OF TECHNOLOGY

UGC Autonomous

(Approved by AICTE, Permanently Affiliated to JNTUH, Accredited by NBA & NAAC with 'A' Grade)

Kandlakoya (V), Medchal District, Hyderabad-501 401

Phone: 08418 – 200720 / 9247605109 Fax: 08418 – 200240, www.cmritonline.ac.in

REQUISITION FORM FOR E-MAIL ACCOUNT/Wi-Fi ACCESS FOR STAFF

Name of the Staff Member		Affix recent Stamp Size Photograph
Designation		
Department		
Date of Joining		
Contact No		
E-mail ID		
Please specify the E-mail Account Name wish to have		
Option One	@cmritonline.ac.in	
Option two	@cmritonline.ac.in	

Staff Declaration

The above information furnished by me is correct, and I undertake to abide by the rules and regulations of the CMRIT for proper use of email/Wi-Fi facility for my academic purpose only.

Signature of Staff Member		**Date**		**Place**	

Head of the Department

Recommended / Not Recommended

Signature of Staff Member		**Date**		**Place**	

System Administration Department

The created email ID	@cmritonline.ac.in				
Wi-Fi Access	Provided / Not Provided				
Date					
Authorized Signature		**Date**		**Place**	

Counter Signature of Staff Member

Received the above mentioned email ID/Wi-Fi access

Signature of Staff Member		**Date**		**Place**	

CMR INSTITUTE OF TECHNOLOGY

UGC Autonomous

(Approved by AICTE, Permanently Affiliated to JNTUH, Accredited by NBA & NAAC with 'A' Grade)

Kandlakoya (V), Medchal District, Hyderabad-501 401

Phone: 08418 – 200720 / 9247605109 Fax: 08418 – 200240, www.cmritonline.ac.in

REQUISITION FORM FOR E-MAIL ACCOUNT / Wi-Fi ACCESS FOR STUDENTS

H.T. No.		Affix recent Stamp Size Photograph
Name of the Student		
Programme		
Department		
Year of Admission		
Present Semester / Year		
Address for Correspondence		
Mobile No.		
E-mail ID		

Student Declaration

The above information furnished by me is correct, and I undertake to abide by the rules and regulations of the CMRIT for proper use of email/Wi-Fi facility for my academic purpose only.

Signature of the Student		**Date**		**Place**	

Mentor / Head of the Department

Recommended / Not Recommended

Signature of the Mentor / HOD		**Date**		**Place**	

System Administration Department

The created email ID	@cmritonline.ac.in				
Wi-Fi Access	Provided / Not Provided				
Date					
Authorized Signature		**Date**		**Place**	

Counter Signature of Student

Received the above mentioned email ID/Wi-Fi access

Signature of the Student		**Date**		**Place**	

CMR INSTITUTE OF TECHNOLOGY

UGC Autonomous

(Approved by AICTE, Permanently Affiliated to JNTUH, Accredited by NBA & NAAC with 'A' Grade)

Kandlakoya (V), Medchal District, Hyderabad-501 401
Phone: 08418 – 200720 / 9247605109 Fax: 08418 – 200240, www.cmritonline.ac.in

R & D CENTRE

CONFIDENTIALITY AGREEMENT

I_____ working as Asst. Prof./Assoc. Prof./Professor in the department of _____ and have access to computer/computer network, internet and data/information and confidential information of the data related to CMRIT. As an employee of the CMRIT, I undertake

a. To communicate only through the official email id assigned to me.
b. To maintain the confidentiality of data/passwords/user id/login credentials assigned to me.
c. To take all possible steps to preserve strict confidentiality regarding any information.
d. To never pass any information obtained as part of the duty/assigned work to anyone outside the section/department/Institute, unless I have been directed to do so by concerned authority.
e. To maintain confidentiality of work, names, contact details and personnel information secure.

I understand that any breach of the above will result in disciplinary action against the loss of damages both by way of performance/remedy.

Signature of the Staff		**Date**		**Place**	
Witness					
1. Name		**Sign**		**Date**	
2. Name		**Sign**		**Date**	
Office Use Only					
Dean, R & D					
Recommended / Not Recommended					
Signature of the Dean, R & D		**Date**		**Place**	
System Administration Department					
Allotted System No.					
Authorized Signature		**Date**		**Place**	
Counter Signature of Staff					
Received System ID and login credentials					
Signature of the Staff/Student		**Date**		**Place**	