



# CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

CMRCET/PRIN/IT/AY2017-18/CIR-03


Date: 07/09/2017

## CIRCULAR

All the members of Cyber Security Club of the college are hereby informed that, the Cyber Security Club committee meeting is scheduled on 09.09.2017 & the Venue is CSE Seminar hall at 1:00 pm. All are requested to be present on time.

The Agenda of the meeting is:

- To Discuss about the SOP, Objectives, Roles & Responsibilities.
- Understanding the Behavior of Threat Actors
- Security for the future .
- Discuss Security Attacks and Preventions
- How to avoid Cyber Security in network




Principal

Copy Submitted to: (1)The Secretary Garu – For your kind information Pl.

Copy to:

1. IQAC Coordinator
2. Controller of Examinations
3. All HODS
4. Administrative Officer
5. Accounts Officer
6. Concerned Faculty



**PRINCIPAL**  
**CMR COLLEGE OF ENGG. & TECH.**  
**Kandlakoya (V), Medchal Road,**  
**Hyderabad-501401.**

PRINCIPAL,  
CMR COLLEGE OF ENGG. & TECH.  
Kandlakoya (V), Medchal Road,  
Hyderabad-501401.



**Academic Year: 2017-18  
CYBER SECURITY CLUB COMMITTEE  
MINUTES OF MEETING**

1. The Meeting was held on 9<sup>th</sup> September 2017 from 1:00 to 3:30 pm in the Department of CSE Seminar hall.
2. The Convener welcomed all the Club committee members
3. SOP was finalized during the meeting with Objectives, Roles & responsibilities

**STANDARD OPERATING PROCEDURE OF CYBER SECURITY CLUB COMMITTEE**

**Purpose:** The purpose of this committee is to form guidelines and procedures to be adopted for protect the usability, reliability, integrity and safety of the network.

**Scope:** With the advent of the modern technological age, people and surrounded things get connected with each other. For protecting those connections, there is a great need for the students of **all Engineering** to protect the security of these connections. The experts of this industry are trying to remove the threats but various scandals of big companies have become attractive attention. In the coming years, this market showed expected growth and is more likely to develop and rise.

**Roles & Responsibility:**


1. Monitor network and application performance to identify and irregular activity
2. Set up patch management systems to update applications automatically
3. Work with IT operations to set up a shared disaster recovery/business continuity plan
4. Work with HR and/or team leads to educate employees on how to identify suspicious activity

**Frequency of committee meeting**

- Four times in the every Academic Year. Every meeting at before starting the semester and end of semester.
- Committee may conduct meeting as and when required

**I. Salient Aspects of Cyber Security Policy and Responsibility**

- (a) Internet connections should be on standalone mode PCs only with no classified data on them. Strict air-gap to be main between Internet and Army networks.
- (b) No dial up access should be there on networked PCs. Official PCs will not be used to access Internet using mob phones/ USB dongles.
- (c) PCs should have strong booting and log on passwords.
- (d) No classified info to be stored on PCs permanently. Under no circumstances data classified as CONFID and above will be typed/ viewed on PA/Steno's PC.
- (e) PCs used for processing cl info will NOT be connected on Army One/ Internet/ any other network and these will not have internal CD/DVD writers.

  
**PRINCIPAL  
CMR COLLEGE OF ENGG & TECH.  
Kandlakoya (V), Medchal Road,  
Hyderabad-501401.**



## II. Software & Hardware Security

### System Software.

- Users must use proper licensed version of the system software like Operating System and this must be periodically updated.
- Default setting in the system software must be reviewed during the installation and the same to be checked from time to time. Vendor supplied default user IDs (like Administrator, Guest) must be deleted or password changed before allowing users to access the computer system.
- Critical components of the network like switches, servers, routers and security appliance must be powered using redundant online Uninterrupted Power Supply (UPS) with automatic shutdown facility in case of power failure to prevent crashing of associate system software.

### Application software.


- All application software development will ensure secure coding practices such as Input data validations, checking for internal processing errors, output data validation, buffer overflow and use of minimum privileges for execution.
- The application software, both being developed in house or procured throughout outsourcing, also needs to be clear of any embedded malicious codes. The developing agency be asked to certify the same. Care needs to be taken to choose to a trusted developing agency with credible capability of producing error-free software.
- All computer issued to the environment are the property of the org for carrying out official tasks only. Only those applications will be installed in the network resources as are needed for official purposes

### Hardware Security

- Hot-Standby Systems. Critical servers, at all nodes must always run with hot standby systems. Other servers must provision back up of their data through auxiliary storage devices, wherever possible.
- UPS Devices. All computer systems must always run with UPS devices. Online UPS devices must be used for all access/control equipment at all communication nodes and other types of UPS may be used for other computers.
- While procuring IT related hardware, the structured evaluation process, in vogue, be resorted to with the info security features duly identified within the Request for Proposal Compliance of these features be confirmed during installation and Acceptance Testing process. Necessary provisions be included in the contract document to allow up-gradation/modification to hardware by the seller to ensure desired info security.

### User Awareness, Security Checks and Reporting of Security Breach

- Security of info especially in the context of cyber security is dynamic. All users of the computers and networks need to be aware about cyber security and must exercise better security consciousness.
- A six-monthly cyber security audit will be carried out in the HQ Dte Gen NCC by a bd of offrs. Proper records of such audit will be maint and a report will be fwd promptly if any security breach is detected/ reported. Imp DOs and DON'Ts on cyber security for all users are given at att appx.

  
**PRINCIPAL**  
**CMR COLLEGE OF ENGG & TECH.**  
**Kandlakoya (V), Medchal Road,**  
**Hyderabad-501401.**



- Upon discovery of cyber security breach/ loss, report to be initiated on such occurrence and subsequent investigations will be carried as per instrs contained in classification and handling of classified documents 2001.


## IMP CYBER SECURITY DOs AND DON'Ts FOR ALL USERS

### Do's. Users are advised to observe the following Do's:-

- Do use computer lock when not in use to avoid unauth access. Do use passwords for:-
  - (i) Booting and screensaver.
  - (ii) Login/access to computer
  - (iii) Access to indl files/ folders.
- Do keep the backup data on CDs/DVDs which are kept in safe custody and are properly accounted for.
- Do keep only system files and programs on hard disk as far as possible.
- Do copy data/files created after each session on removable media like floppies/CDs and keep it at physically secure place.
- Do erase data/files by shredding from the hard disk.
- Do log off PCs in a network to obviate unauthorized client stations accessing e-mails and stored files.
- Do avoid networked configuration file sharing to rule out access by unauthorized persons.
- Do open email-box regularly and scrutinize its contents. Info/ data not required must be deleted periodically.
- Do scan external storage media for viruses before these are used on computers.
- Do report questionable/unidentified files on your PC.
- Do report any loss of media immediately to offr auth to ensure cyber security in the br/sec/est.

### Don'ts. Users are advised to observe the following Don'ts:-

- Don't give access to the computer to any outside/ unauth pers and Don't disclose your password to any unauthorized pers.
- Don't permit copying of files/ info from your computer to any outsider.
- Don't let the vendor/ mech take away hard disk in the event of a hard disk crash /failure. If it is certified that the disk is unserviceable, it will be removed and destroyed by a bd of offr.
- Don't use external storage media on your computer unless scanned for virus . Virus can destroy all the files on your hard disk.
- Don't copy programs from unauth sources.
- Don't leave any confd docu/letters on the computer hard disk. In case of large vol of confd data on hard disk being used repeatedly, ensure computer is kept in the auth offr's office and clk/opr work under supervision/obsn.
- Don't keep data of classified nature on hard disk of PCs on a network.

  
**PRINCIPAL**  
**CMR COLLEGE OF ENGG & TECH.**  
**Kandlakoya (V), Medchal Road,**  
**Hyderabad-501401.**



# CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

The List of Cyber Security Club Committee members attended the meeting:


S.No	Name of the member	Designation	Position	Signature
1.	Dr.V.A Narayan	Principal	Chairman	
2.	Mr S Siva Skanda	Associate Professor	Convener	
	Mr.B.Tulasidasu	Assistant Professor	Coordinator	
3	K.LOHESWARAN	Assistant Professor	Member	
4	Mr. P.Ramesh	Assistant Professor	Member	
5	Mr. Y.CHITTIBABU	Assistant Professor	Member	
6	Mr. M.SUNEEL KUMAR	Assistant Professor	Member	
7	Mr .Vinayak B. Naduvnamani	Assistant Professor	Member	

  
Convener

Copy Submitted to: (1) The Secretary Garu - For your kind information Pl.

Copy to:

1. IQAC coordinator
2. Concerned Faculty

  
PRINCIPAL  
CMR COLLEGE OF ENGG. & TECH.  
Kandlakoya (V), Medchal Road,  
Hyderabad-501401.