SAFETY AND SECURITY POLICY

MES ASMABI COLLEGE

AFFILIATED TO
University of Calicut

SAFETY AND SAFETY POLICY OF MES ASMABI COLLEGE

We have an inclusive policy frame work for the security of the community inside the campus. The responsibility for security rests with all students, staff (including permanent and contract) and with visitors to the College. It is the duty of each and every one to report all activity (suspected or real) of a criminal nature, unacceptable behavior, or any suspicious activity immediately to the security or Reception staff.

I. Security and Safety Responsibility and role

A. Decision Making and Providing adequate facilities

- Management of College
- Principal
- Staff Council

B. Complaints reception, Initial decision and Reporting

- Heads of Departments
- Reception officer
- Chief Security Officer

C. Security and Invigilance

- Security Supervisor
- System administrator (CCTV and Information Security)
- Security Guards
- Hostel security
- Night Security
- Cleaning Staffs

D. Responsibility of reporting and complaint

Student Union

Staff Club

Faculties

Students

Workers and Contractors

Visitors

II. Crime Prevention and Security-Awareness Procedures

A. Procedure: Safety, Security and Crime Prevention

a. Crime reporting

1. All suspicious activity should be immediately reported to the Chief Security officers or at the Reception Staff in the first instance.

2. It is the responsibility of all students and staff (permanent or contract) and visitors of the College to report all activity, suspected or real, of a criminal nature, suspicious and/or unacceptable behaviour.
3. The Chief Security officers or the Reception Staff shall make an initial scrutiny with the support of security guards, HoDs and report to the Principal
4. The Principal shall scrutinize the nature, any criminal activity if found or suspected shall be inspected using the CCTV footage and also with statements from the security officers or the complainant if any.
5. The issue shall be immediately report to the Police Station or Station House Officer for further procedures for any case of reported crimes of assault, indecency, fraud, theft and burglary. In cases of doubt, advice on Police involvement may be sought
6. The principal shall put forward the issue in the College council and enquiry shall be executed through the regular procedures.
7. All Personal valuables should be locked away, placed out of sight or kept on the person. Personal property should never be left unattended
8. Offices must be locked upon leaving, with windows closed and locked
9. The local Police should be informed in all cases of reported crimes of assault, indecency, fraud, theft (including car or cycle theft) and burglary. In cases of doubt, advice on Police involvement may be sought from the Duty Officer

b. Crime Investigation

1. All crimes that occur on College premises shall be investigated appropriately with decision form college council to prevent re-occurrence and aid crime prevention
2. The following shall be used and scrutinized for crime prevention and Investigation
    - Identify cards all staff (permanent and contract), students
    - Visitors identification
    - Security cameras

B. Fire and Emergency

1. Fire Extinguishers installed at each block and corridors
2. Open Corridors
3. Two stairs at both ends
4. Two doors for each class rooms
5. Emergency lift for Divyangjan friendly
6. Open ground space within the campus
7. Two gates
8. Parking facility

III. CCTV Policy and Procedures

There are CCTV surveillance system within the campus for ensuring security screening as a measure of criminal activities within the campus and ensure the safety of the students, faculties and other staff including visitors.

The Principal and the Systems administrator has access to live footage and backup using the Hikvision App for emergency situations.

A. The CCTV surveillance areas and the specification

The specification: 16 Channel Hikvision NVR System with 4 MP camera and 4TB HDD are installed

a. Front area, Office and main block.

1. Cameras in Front gate – 2 Camera
2. Front Pathway and Infront of the office -2 Camera
3. Staircase and front office -1 Camera
4. Within the office including principals cabin and locker room -9 cameras
5. Backside of the office -1 camera
6. Corridors in the main block all floors – 6 cameras
7. Seminar hall -camera
8. Auditorium -camera

b. Commerce , B Voc and Aquaculture and Fish processing blocks

One camera each in all the corridors in each block

c. Physics and Computer lab New block

1. Computer lab -3 Cameras
2. Security of the lift – 4 Cameras
3. Department Corridors in each floor - 4 Cameras
4. Boys Rest room -1
5. Girls Rest Room -1

d. Girls Hostel

1. Front Gate -2 Cameras
2. Hostel Back Side – 2 Cameras
3. Hostel Terrace – 1 camera

All the cameras are connected to DVR system installed at the Hostel Warden's room

e. Boys Hostel and Principal Quarters

1. Front side – 2 Cameras
2. Backside - 2 Cameras
3. Compound and gate - 2 Cameras

IV. Information and Data security

- In order to secure the sensitive information of college personnel, students, and other individuals connected with the college, as well as to prevent the loss of information that is crucial to the functioning of the institution, a policy should be implemented.

- In order to ensure the confidentiality, integrity, and availability of the information technology resources that are available to the colleges, it is necessary to establish procedures that are acceptable and appropriate.
- Take measures to ensure that the information that the college gathers is honest and completely trustworthy.

A. Measures to Prevent unauthorized access to IT Resources

1. Each and every member of the faculty and staff is given access to institutional mail that is supported by G Suit in order to guarantee the safety and security of the communication and data.

2. All individuals are instructed to submit their concerns to the system administrator and to utilise the assistance provider, which is Google's G Suit suite.

3. Every faculty member is required to maintain robust passwords and must update them at least once every three months for all email IDs, department email IDs, and any other software or web-based logins. This instruction applies to all of the faculty members.

4. To ensure that only allowed users may access the computer systems, each and every one of them is secured with a login and user password.

5. The system administrator has direct control over all of the servers and hard disc drives (HDDs), and they are all protected with passwords.

6. The sole purpose of licenced softwires is to guarantee the confidentiality of information.

7. Everyone is required to adhere to the norms and procedures of the college, institution, as well as the regional, national, and international legislations in order to maintain the confidentiality of the information.

8. Programmes of awareness are carried out on a regular basis regarding cyber and

B. Centralized/Decentralized Computing Systems

1. Computer systems that are both centralised and dispersed have been built in order to ensure the confidentiality of the college's information and data.
2. Computing solutions that are centralised are often employed for the purpose of storing and managing vital data and information in an environment that is both secure and under your control.
3. These systems make it possible to govern, monitor, and back up data in a centralised location, which guarantees that the data will be safeguarded from unauthorised access or corruption.
4. Decentralised computing systems, on the other hand, disperse data among a number of different devices or servers. This provides redundancy and fault tolerance in the event that the system fails or a disaster occurs.
5. The use of this strategy has the potential to improve the security of college information by lowering the likelihood of data loss or disruption caused by a single event.

C. ERP Software and cloud computing for safety and backup

1. When it comes to data management, the college makes use of licenced SANCTUM ERP software, which was built specifically for higher education institutions. This software is tailored to our needs, ensuring the data's safety through numerous levels of scrutiny as well as user id and password systems.

2. The enterprise resource planning system (SANCTUM ERP) that is maintained by Affinty opus and is offered by The Niche Ecosolutions.
3. This is a cloud-based computing system that has space in Amazon web servers, which serves to ensure that all of the data that is used is backed up on a regular basis and is secure.
4. The use of this strategy has the potential to improve the security of college information by lowering the likelihood of data loss or disruption caused by a single event.

D. Public information

1. The data that is used in ERP is linked with the website, and the information that is required is accessible to both the general public and students.
2. There are multiple tiers of user IDs and passwords that are used to restrict access to the subsequent information.
3. The information that is supplied on the website is licenced under creative commons in order to guarantee that it is authoritative.

E. Ethical standards and Academic integrity

1. The college is committed to protecting the confidentiality of academic and public information, and it complies with legislative frameworks that are worldwide, national, and regional in jurisdiction.
2. A unique set of policies has been implemented to ensure that ethical and scientific integrity are maintained.
3. has made sure that all student and faculty publications are scanned for plagiarism using software that has been appropriately licenced.
4. It is the responsibility of every student, fellow, faculty member, and research supervisor to make certain that their papers adhere to acceptable ethical standards and do not contain any instances of plagiarism.
5. For the purpose of ensuring that the original authors retain their authority, all of the publications that are made available on the website, journal, and other platforms are licenced under the Creative Commons.

Vi. Disclaimer : The school is not responsible for any illegal behaviour, crime, or loss that occurred on the campus, including losses that occurred to any of the stakeholders who were participating in the activity. Every member of the community is obligated to comply with this policy, as well as the legal frameworks of the college, university, state, nation, and international level, which include ethics and standards, and they will be dealt with in accordance with these frameworks.