Annexure

The following guidelines aim to strengthen campus security while maintaining the academic values and openness of IITs. Institutes are requested to give due importance to implementing these measures, in addition to other measures specific to campus, to provide a secure environment to the students and faculty on campus while also ensuring the facilities are accessible to only authorised personnel.

1.1 Visitor and Guest Management

- Mandatory pre-registration may be ensured for conferences, workshops, cultural programmes, and other events involving external participants.
- Visitor details may include name, contact information, purpose of visit, host department/person, and duration of stay.
- Photo identity verification may be carried out at entry points.
- Visitor passes, physical or digital, may be issued for a defined duration and displayed prominently.
- Departments hosting events may designate a responsible officer to ensure compliance with visitor management protocols.
- Necessary approvals (MEA/MoE or other relevant Government Departments) may be obtained in cases where foreign nationals visit the campus.

1.2 Campus Access Control

- Entry and exit points may be clearly identified and adequately staffed by trained security personnel.
- Access to hostels, laboratories, sensitive research facilities, and administrative blocks may be regulated through:
    - Institutional identity cards,
    - Smart cards or biometric systems, as applicable
- Separate access protocols shall be established for vendors, contractual staff, and delivery personnel.
- Norms for night-time access shall be clearly defined and enforced.
- **Access may be further restricted for sensitive areas within the campus, including the labs that are researching emerging and critical technologies.**

1.3 Internal Security and Patrolling

- Regular and systematic security patrols may be conducted across academic areas, hostels, residential zones, and common facilities.
- Patrol frequency may be enhanced during large events, peak hours, and late-night periods.
- A record of patrol schedules and observations may be maintained and periodically reviewed by the campus administration.

1.4 Surveillance and Monitoring

- CCTV surveillance may be installed at entry/exit points, high-footfall areas, and other sensitive locations.
- Surveillance systems may be centrally monitored in real time by trained personnel.
- Clearly defined response mechanisms may be in place for addressing suspicious activity or security breaches.
- CCTV footage may be retained for a prescribed period in accordance with institutional policy.

1.5 Vigilance in Academic and Event Spaces

- Faculty members, event coordinators, and administrative staff may ensure that only authorised or enrolled individuals attend classes, examinations, and restricted events.
- Entry verification mechanisms may be adopted for closed academic sessions and examinations.
- Any suspicious or unauthorised presence shall be immediately reported to campus security authorities.

2. Sensitisation and Capacity Building

- Periodic awareness and sensitisation programmes to be organised for students, faculty, staff, and security personnel.
- Training may focus on the identification of suspicious behaviour, reporting mechanisms, emergency response, and crowd management.
- Security staff may receive regular training on access control systems and surveillance operations.
- Necessary export controls training and workshops may be organised for the faculty and students engaged in research on dual-use goods and technologies, within the campus.

3. Monitoring and Review

- Institutes may constitute or designate a Campus Security Committee to periodically review security arrangements and recommend improvements.
- Institutes may undertake an internal review of existing security mechanisms and implement necessary corrective actions in a time-bound manner.
- Any major security-related incident is to be reported to the Ministry promptly.

****