Email: registrar@gkciet.ac.in

Ghani Khan Choudhury Institute of Engineering and Technology

(A Centrally Funded Technical Institute under the Ministry of Education, Govt. of India)
Narayanpur, Malda - 732141, West Bengal
www.gkciet.ac.in

न हि ज्ञानेन सदृशं पवित्रमिह विद्यते

Memo No: GKCIET/2025/315 **Date:** 12/06/2025

NOTIFICATION

The draft Security Policy of the Institute was placed before BoG in the 35th meeting held on 19.03.2025 as agenda item no 35.04.08. The BoG had advised to include cyber security aspect in the policy.

Accordingly, after inclusion of cyber security the 'Security Policy' of the Institute is notified for compliance.

This is issued with the approval of the Director.

Registrar
GKCIET, Malda

Copy to:

1. Security Officer – for kind information and necessary action.
2. All employees- for kind information.
3. Dean (SW)- with the request to circulate among students.
4. Assistant Registrar (A&E) – for information.
5. System Manager- with the request to upload on the Institute's website..
6. Director, GKCIET – for kind information.
7. File Copy

SECURITY POLICY

न हि ज्ञानेन सद्दशं पवित्रमिह विद्यते

GHANI KHAN CHOUDHURY INSTITUTE OF ENGINEERING AND TECHNOLOGY

(A CFTI under Ministry of Education, Govt. Of India)

MALDA, WEST BENGAL

GHANI KHAN CHOUDHURY INSTITUTE OF ENGINEER AND TECHNOLOGY

(A CFTI under Ministy of Education, Government of India)

INDEX

Introduction

GKCIET, Malda is situated at Narayanpur, near Malda Town city. It has a beautiful campus consisting of many Academic buildings, residential area, hostels and administrative building etc.

There are approximately 1200 students and 150 staffs at the Institute plus numerous visitors to the campus daily. There are parkings for the vehicles of staff, students and visitors at the campus during day time.

Open access to GKCIET campus is an essential ingredient of academic life but is not without risks. Some security measures are therefore necessary to maintain a safe and secure environment for our staff, students and visitors.

To enhance the feeling and/or perception of security the GKCIET, Malda will develop and apply Security controls, and procedures which will be widely published. Security is not intended to be a hindrance to academic activity. It is an essential ingredient for the safe and efficient operation of the Institute. This Security Policy applies to all staff, students, visitors and contractors and seeks to formalize a cohesive and integrated approach to security throughout GKCIET.

Policy Statement

GKCIET, Malda will endeavor to ensure, as far as reasonably practicable, the personal safety and security of all students, staff and visitors at the campus and GKCIET controlled buildings. The Estate and Works Department is responsible for the effective operation and enforcement of the Security Policy and Procedures.

Students, staff and visitors to the campus must also take responsibility for their security and personal safety. In particular, students, staff, visitors and contractors should assist the Security Service to ensure the success of the Policy. Whilst minor breaches of the Policy may be dealt with informally, serious or repeated breaches will invoke disciplinary action.

Unless otherwise specified, reference to ‘ The Institute’ in this document refers to GKCIET, Malda.

Responsibilities

Security Service will support the Security Policy by adopting a proactive approach to minimise crime and incidents and their effects on the staff, students and visitors. The Security Service will ensure the response to incidents is well managed by being responsive, effective and efficient. The Security Service will listen and care for our stakeholders and promote a safe and secure work and study environment.

It is in the interest of the GKCIET that members of GKCIET community report to the Security Service as promptly as possible any activity that appears to be criminal in nature.

Security Officer will ensure that support and resources are available to the Security Service for the implementation of the Security Policy. Necessary measures to improve security in essential areas should receive priority consideration. Where appropriate, specific training to achieve acceptable standards of operation will be supported and properly resourced. And will ensure overall development and planning of security strategy, policies and procedures and oversee the operation of the Security Service. Other responsibilities will include, but are not limited to the investigation of serious crime, breaches in security and advising on student disciplinary matters ; provision of expert and impartial up-to-date advice, staff and student inductions, transport, liaison with local police, emergency services and local authorities: Security staff, implementation of Institute Car Parking Policy.

Security Officer will also ensure the day-to-day management and execution of the Security operation and monitoring of all policies and procedures to ensure their continued effectiveness, training of staff and investigation of crime.

Security Supervisor/ Security Guard: Verifying the visitors/ vendors/ checking of outsider's vehicles. Ensuring the entry of authorized vehicles only. Issuing visitor's pass/ permits. Keeping record of vehicle passing through GKCIET gates. Parking of vehicles. Opening and closing of main gate and class room building. Maintaining a log of students working in labs. after normal working hours. Switching on/off tube lights. Maintaining a register of non-hosteller student and visitor who are staying over-night. Checking of students bags any prohibited material. Stopping trespassing of outsiders.

Heads of Academic and Non-academic Departments have a key role in promoting security within their area. It is recognised that Heads of Department may wish to delegate responsibility for the routine involved in these tasks to a nominated individual in their Department but the overall responsibility for security matters will remain with the Head of Department.

Staff : All staff must ensure and adhere to the Institute Security Policy, paying particular attention to those issues which are relevant to their activities. They must also co-operate with requests from the Security Service, especially in emergency or evacuation situations.

Students They must follow security procedures designed to protect the Institute property, in particular regulations governing access to computer rooms or areas with other public use equipment. Students must co-operate with requests from the Security Service, especially in emergency or evacuation situations and in relation to security procedures.

General Visitors : (including conference delegates and external event attendees) have a general responsibility to look after the Institute facilities whilst on campus and to give due consideration to security issues. In particular they must follow security procedures designed to protect the Institute property and where issued, carry their visitors pass at all times It is the responsibility of the host to ensure all visitors are informed and comply with the Institute Security Policy, particularly in emergency situations.

SECTION 1 –CRIME PREVENTION

1.1 SECURITY AWARENESS

Proactive crime prevention and security awareness will help to ensure a safe, secure environment, enabling work and study to continue with the minimum amount of disruption. Staff and students should make every effort to counter the threat of crime which is laid out as under (See 1.1.1):

1.1.1 Crime Prevention

i. *All suspicious activity should be reported immediately to Security Officer.*

ii. *Personal valuables are locked away or placed out of sight or kept on the person, and personal property is never left unattended.*

iii. *Windows in ground floor offices/ rooms/ labs must be closed and secured on departure where locks are fitted. Curtains or blinds in these rooms should be closed at dusk and lights (except security lighting) should be turned off when leaving.*

iv. *Laptops and other portable IT/AV equipments are locked out of sight when not in use, particularly overnight, in open areas.*

1.2 INCIDENT REPORTING

Incident reporting is crucial to the identification of patterns of criminal activity. It permits investigation and recommendations to be made to prevent a recurrence. Comprehensive reporting of incidents provides an accurate picture of the level of crime throughout the institute and thus ensures that adequate resources are provided to combat that crime which contributes to the success in the GKCIET's fight against crime. All incidents of a security nature should be reported and managed as described below (See 1.2.1):

1.2.1 Incident Reporting

I. *All security incidents should be reported to the security staff at main gate/ posted at the location (24 hours).*

II. *All reported incidents will generate an incident report and will be forwarded to Security Officer who will forward the reports for an appropriate action.*

III. *All suspected criminal offences will be reported to the Police.*

IV. *All emergency Police involvement on campus is to be notified to the Chairman Estate and Security Officer to enable effective management of any subsequent actions on GKCIET premises.*

V. *Security Services should be informed as soon as possible when emergency services are requested to GKCIET Campus.*

VI. *Suspicious behaviour–Staff, students and visitors should not place themselves in a vulnerable or confrontational situation if they observe suspicious behaviour. More important is to make a mental or written note of a description, direction of travel, what suspicious acts have been witnessed and any other information which may help Security identify and locate the individual(s). That information should be provided to Security as soon as reasonably possible. Each situation of this type will be different and it is at the discretion of the individuals concerned as to what action they wish to take, but at no time should they put themselves at risk.*

1.3 CRIME INVESTIGATION

All crimes which occur on GKCIET premises will be investigated appropriately to prevent re-occurrence and help crime prevention. The Security Officer or other members of the Security Service as delegated will carry out internal investigations of security related incidents, producing written reports for circulation where necessary.

SECTION 2- PERSONAL SECURITY

Whilst it is the responsibility of the Security Service to provide a safe and secure environment, it is the responsibility of all those on GKCIET premises to take all reasonable measures to **ensure their own personal security**.

2.1 STAFF AND STUDENTS

The Security Service will provide security briefs to staff and students.

2.1.1 Security Advice

a. Be aware of people when using cash and preferably draw out money from ATM.

b. Do be suspicious of e-mails or phone calls requesting too much personal information and destroy papers carrying bank or credit card details. Identity theft is on the increase.

c. Keep a record somewhere safe of plastic cards details and the serial and model numbers of your expensive electrical/electronic equipment.

d. Texting can distract you from what is happening around you. When you are out and about switch your mobile to vibrate mode rather than a ring tone.

e. Consider installing security software on your laptop and always carry it hidden inside a sports bag rather than in its own obvious case.

f. Immobilise your car or lock your bike whenever you leave it even for a few minutes. Moving between GKCIET buildings - students and staff should make themselves aware of their surroundings and of other people when walking between buildings. Try to avoid poorly lit or isolated areas and where possible, walk with other members of staff or students. Report any deficiencies in lighting on GKCIET buildings through the Security Helpdesk at main gate so that remedial action can be taken where appropriate.

g. Reporting suspicious activity is extremely important to Security Staff in helping to prevent and detect crime against the institute.

h. If staff or students are faced with threatening or abusive behaviour, stay calm, avoid raising your voice and the use aggressive body language such as finger pointing/wagging. Call for assistance from colleagues and/ or Security Staff.

i. Immobilise your car or lock your bike whenever you leave it even for a few minutes. Moving between GKCIET buildings - students and staff should make themselves aware of their surroundings and of other people when walking between buildings. Try to avoid poorly lit or isolated areas and where possible, walk with other members of staff or students. Report any deficiencies in lighting on GKCIET buildings through the Security Helpdesk at main gate (7866931514) so that remedial action can be taken where appropriate.

j. Reporting suspicious activity is extremely important to Security Staff in helping to prevent and detect crime against the institute.

k. If staff or students are faced with threatening or abusive behaviour, stay calm, avoid raising your voice and the use aggressive body language such as finger pointing/wagging. Call for assistance from colleagues and/ or Security Staff.

2.2 CONTRACTORS AND VISITORS

All contractors who make use of and work on GKCIET property have a general responsibility to give due consideration to personal security issues. In particular they should follow security advice and procedures designed to protect them whilst on GKCIET property. A visitor’s host or project manager/in charge/SDE has the responsibility to ensure security advice and procedures are made readily available. Contractors must obtain pass/ permit from the Institute Engineer/ Security Officer to work/ carry in or take out materials at GKCIET campus.

SECTION 3 – ACCESS AND IDENTITY CONTROL

3.1 IDENTITY CARDS

All staff and students are issued with a GKCIET photo card which is used as an identity card, access card and a Library membership card. **The card is non- transferable and may only be carried and used by the individual to whom it was issued.** Staff and students should carry their card with them at all times when on GKCIET property and must show their card to Security Staff on request. Loss of identity cards must be reported to Dean Acad./ SW and security section as soon as possible. Overnight visitors, long term visitors (beyond five continuous working days) and contractors will be issued with a ‘security visitor’s pass at security section which must be carried at all times while on GKCIET property **(see 3.1.1 hereunder).** Security will reserve the right to establish the identities of all persons on GKCIET estate and detain any issued identity card or pass following an incident on campus. GKCIET identity cards will be forwarded to the Dean Students Welfare/ Chairman HMC for student issues and retained by the Security Officer for staff, visitor and contractor issues and reissued via departments or GKICET administration if deemed appropriate.

3.1.1 Access Control for Visitors and Contractors

I. *Long term visitors (beyond five continuous working days) and Contractors will be issued with a ' security visitor's pass' at Security Section near main gate. The member of staff or student responsible for the long-term visitor/contractor will ensure that the visitor/contractor collects or return the pass when signing in or out of the GKCIET.*

II. *Contractors on site for more than a week (five days) will be issued with a 'GKCIET Contractor' pass. Arrangements for these cards are to be agreed in advance by the Contractor or SDE/ Project Manager and Chairman Estate/ Security Officer. The 'GKCIET Contractor' pass must be displayed at all times whilst on GKCIET premises.*

3.2 GKCIET CORE WORKING HOURS

Core working hours are defined as Monday to Friday 8 a.m. to 6 p.m. excluding public holidays. If work needs to be done or continued outside those hours and you feel at risk, the Security Service should be informed.

Access to the GKCIET outside core working hours will be in accordance with the process set out in the lone working policy.

3.3 CONTROL OF LOCKS & KEYS

A. Academic Area (Academic Block- A, B, C, D, Central Library and Workshop)

i. Labs & Faculty Rooms:

Safe custody of all registers, documents and valuables in labs will be the responsibility of faculty/ lab-in-charge/ HoD. The faculty, lab- in- charge/ HoD shall keep all files, documents and valuables in safe custody under lock and key. The keys of labs/faculty rooms will be maintained as under:

a) The first key will be kept with the lab-in-charge / individual faculty member.

b) The second key will be kept in HoD office.

c) A third key will be available with the security staff of the concerned building which shall be operated by security staff for switching off the electronic appliances left running once the room is closed and in case of emergency only. (This key shall not be made available for any routine activities)

ii. The Classrooms:

The classrooms will be opened in the morning at 7 AM by the security staff for cleaning purpose. During the class hours, it shall be the responsibility of the user faculty/ staff to keep the safety of fittings and fixtures in the classroom. The last user faculty/ staff is responsible for the turning off the lights, fans and ACs after academic hours before locking them up. The keys of classrooms will be maintained as under:

a) The first key will be kept with the Staff nominated by the concermed HoD.

b) The second key will be kept by HoD office.

c) A third key will be available with the Security staft of the concemed building.

iii. Under normal circumstances the classrooms will be under the responsibility of individual staff holding the first key.

iv. Whereas, the second key held in the HoD's office shall be used only when individual staff is not available & there is urgent need to open the room/lab.

v. The third key or the key held by the security staff will be used for routine cleaning and in case of emergency like fire or electric short circuit etc.

vi. No lock should be replaced without the permission of Chairman Estate/ Security Officer. In case such eventuality occurs, the complete set of keys i.e. first key, second key and third key should be duly replaced by the office of HoD concemed.

B. Administrative Buildings:

The keys of the offices within Administrative Buildings shall be maintained as under:

a) The first key will be kept by the officer of the concerned room.

b) The second key will be available with security staff. The security staff shall operate the key for switching off the electronic appliances left running once the room is closed and in case of emergency only.

i. The officer using the room will keep all files, documents and valuable under his personal lock inside the room.

ii. If the lock is to be replaced for any reason it shall be done by the concerned officer under intimation of Chairman, Estate/ Security Officer.

iii. Lock and key of the sensitive offices/ section will be kept with concerned officers/ HoS only.

C. Hostel Buildings:

The keys of the Hostel will be maintained as under:

(a) Student room keys are the responsibility of the student to whom they were issued and may not be transferred or used by anyone other than the person who signed for them.

(b) Security personnel will only issue/ deposit keys of hostel facilities' (Common room, Gym, TV room) from the "Hostel Key Box" to the students only after making entry in the register.

(c) Security staff shall be responsible for issue /deposit the key from the "Hostel Key Box".

Any requests for locks and keys for new premises, refurbishments and replacements will be in consultation with the Chairman Estate and Security Officer.

Security carries out duties over 24hrs, 365 days per year and requires access to all areas especially in emergency situations. Any request made by Security for keys (or access to keys); any others means of access, must be granted in order that emergencies can be dealt with immediately. In exceptional circumstances certain restrictions may apply to sensitive areas (research) but agreement will be achieved between interested parties regarding access in any emergency situation.

3.3.1 Contractors

I. Contractors access to GKCIET buildings will be strictly controlled by the Security Service according to agreed access control procedures.

General

II. All losses of the keys must be reported immediately to concerned HoD and Chairman, Estate/ Security Officer. It shall be the responsibility of the concerned officials to deposit a copy of the key in the security key box, for emergecy use, at the time of replacement of the lock.

3.4 MOVEMENT OF GOODS/ MATERIAL

I. Any of the GKCIET property or personal property can be taken out of the campus only with the authorised gate pass issued by the SO as per procedure.

II. The authorised gate pass will be issued by Secirity Office on receipt of request from HoD/HoS/Contractor/Individual employees.

III. All are expected to cooperate with the security staff at main gate of the GKCIET during checking and varification for taking the goods out of the campus.

SECTION 4 – PROTECTION: EQUIPMENTS/ DOCUMENTATION

4.1 SECURITY OF EQUIPMENTS

The safekeeping of all property will help to ensure that the maximum amount of equipment is available for use at all times. Students and staff are to make all possible efforts to ensure that all equipment is protected from the possibility of theft or damage as described hereunder (See 4.1.1):
4.1.1 Security of Equipments

a. *All computer/AV equipments should be secured depending on its use.*

b. *The physical protection of IT and AV equipments is important on and off campus. Equipment used in departments must be managed to reduce the risk of the equipment being damaged, stolen or accessed by unauthorised persons.*

c. *All valuable portable IT and AV equipments such as laptops & PDA's must be locked away out of sight when not in use, especially overnight.*

d. *All valuable equipments should be marked using the appropriate identification method (i.e. UV pen, Smartwater mark etc).*

e. *Suspected thefts of equipments should be reported promptly to the HoD/Chairman Estate/ Security Officer.*

f. *Heads of Departments are responsible for maintaining inventories for all equipments and furniture in their respective departments.*

4.2 SECURITY HARDWARE

Installation of CCTV, intruder alarms or access control systems on GKCIET property will only be undertaken following consultation with the Director and the Chairman Estate who will advise on equipment, installers and security response. Where CCTV is installed, the requirements of the GKCIET's Data Protection Policy and of the IT Act if any must be adhered to.

4.3 HEADED PAPER AND STATIONERY

Pre-printed headed paper and other stationery displaying the GKCIET logo, staff names and telephone numbers should be locked away when not in use.

4.4 DATA PROTECTION

The data of living persons must be protected and staff should handle personal data in accordance with the GKCIET's Data Protection Policy and the IT Act. Staff should ensure that they are aware of GKCIET policy in this area and of the sources for further advice.

4.5 PROTECTING INFORMATION ASSETS

Maintaining the security of computers and related equipment is vital to the GKCIET. Computers are prime targets for theft ; they are easily disposed of and have a high value. The theft of a computer may also lead to delays in GKCIET processes, the loss of important data and disruption to learning and teaching activities.

Damage of this type is not inevitable and by being aware of simple security measures and observing them, the chances of loss and damage can be minimised. Information on how to protect data and the equipment on which the data is processed may be obtained from GKCIET IT Cell.

4.6 CONFIDENTIAL WASTE

It is the responsibility of the Departments requesting disposal through the Chairman Estate to ensure confidential material is secured at all times until collected.

SECTION 5 – ASSET PROTECTION

5.1 CONTROL OF CASH

Security discourage the storage of any large amount of cash (Rs.10.000/- or over) on GKCIET premises outside appropriate secure rooms. Cash kept on GKCIET premises must be held in accordance with the GKCIET's Finance Policy if any.

5.2 SECURITY OF ACADEMIC BUILDINGS

It is the responsibility of the Security Service to secure the external entrance/exit door to each academic building outside core working hours. This will be through electronic or manual methods.

5.3 SECURITY IN THE OFFICES

It is the responsibility of all staff to secure their own office space as laid out hereunder (See 5.3.1)

5.3.1 Security in the Office :

At the end of the working day, staff must ensure that :

a) Valuables and confidential documents (laptops, exam scripts, research data, personnel files etc.) are locked away with keys secured in departmental key box or taken home.

b) Any departmental keys that have been issued during the day have been returned and any losses reported immediately.

a. A 'clear desk policy' is maintained where possible to ensure confidential documentation is locked out of sight.

c) *Doors and windows are closed and locked as appropriate.*

d) *Curtains and blinds are closed with any items on windowsills, which hinder closure, removed and lights turned off.*

e) *Intruder alarms (where installed and a local responsibility) are set.*

f) *PCs are switched off or password protected when not in use to prevent unauthorised access to information.*

5.4 DRUGS AND ILLEGAL SUBSTANCES

All suspicions of the handling or using of controlled or illegal substances should be reported to the Chairman Estate and Security Officer in the first instance, so that appropriate investigation and consultation with GKCIET authorities may take place. Departments which hold substances that might constitute a security or safety risk should contact the Medical Officer and the Chairman Estate for advice on best practices.

5.5 LOST AND FOUND PROPERTY

All lost and found property should be handed over to the GKCIET Security Section main gate. When property is handed over, the date/time, finder's name, department and contact details will be recorded. If the property is not returned to the owner or left unclaimed for more than 3 months, the property will be destroyed. A guide to dealing with lost and found property is detailed hereunder (See 5.5.1) :

5.5.1 Lost and Found Property guide

a) All GKCIET lost and found property will be logged by Security at main gate and then collected and stored by the Chairman Estate and Security Officer as soon as practical.

b) All unclaimed articles will be held for a minimum of 60 days. After 90 days all articles will be destroyed. Found cash will be donated via local charity boxes. Articles of a personal nature such as credit cards or driver's licenses will be destroyed (shredded) and disposed of in a non-compromising manner.

c) Destruction of items will be recorded by Security Officer and counter signed by the Chairman (EMC).

d) Any person(s) reclaiming items will need to offer a full description and evidence that the item to be reclaimed is their property. All reclaimed must be signed for.

e) The finder of lost property must advise Security if they intend to claim the property if the rightful owner does not.

SECTION 6 – PARKING

6.1 PARKING

Parking on GKCIET property, including the parking of cars, motorcycles and bicycles, will only take place in recognized and designated parking locations and requires an appropriate permit/sticker to be displayed. A guide to parking and permit/sticker requirements is laid down as under (see 6.1.1):

6.1.1 PARKING

a) Vehicle Parking faculty/ Staff/ officers : Parking is available to staff and all cars must display a valid GKCIET parking permit/sticker issued by security. Stickers are available from GKCIET Estate office and at Security Section**.**

The vehicles should be parked at earmarked/ authorised parking places only.

b) *Halting/ stopping/ alighting/ parking of the vehicles on roads shall be strictly prohibited.*

c) Car parking by the students with mobility limitationon a temporary or permanent basis and Student Parking During Core Working Hours 0700-1800hrs.

Parking for students with mobility limitations on a temporary or permanent basis is available. Cars will display appropriate GKCIET permit available from security. All applications for this type of pass will be via the Dean Students Welfare office.

No parking is offered to students at Administration and various academic blocks parking from ***0700-1800hrs.***

Limited parking is available to students at the GKCIET parking during term time on a

"first come first serve basis". All student car owners must apply to Dean Student Welfare and

display a valid permit/sticker available from security.

d) ***Visitor Parking***

Visitor parking is available (but limited) on all sites. It is the responsibility of the member of staff issuing the invitation to make the necessary arrangements.

Where possible, visitors should be encouraged to use public transport.

e) ***Contractor Parking***

It is the responsibility of the IE and member of staff leading a project to make the necessary arrangements with the Chairman Estate and Security Officer for the issue of a permit. This should be arranged at pre contract meeting by IE/project managers and limited to a max of two 2 parkings permits.

f) ***Enforcement***

Drivers of Vehicles parked in breach of the Car Parking Policy are liable to receive a penalty notice.

Cars parked for more than 48 hours without prior permission may receive a penalty notice and removal from the GKCIET estate.

g) ***Motorcycle Parking***

All motorcycle owners will register their motorcycles with security and display a valid permit/sticker issued by security.

Anyone leaving a motorcycle or scooter on GKCIET premises must leave it safely and securely locked. All motorcycles must display a valid permit/sticker available from security. Applications should be submitted through the Dean Students Welfare to security service.

h) ***Cycle Parking***

Anyone leaving a bicycle on GKCIET premises should be aware of the importance of having a robust lock and knowing how to use it effectively and having it insured. All cycles owners will register their bicycles with security and display a valid permit/sticker issued by security.

Non registered cycles locked in one location for more than a two week period without prior notice will have the cycle removed. This will occur after a period of not less than seven days notice on the cycle informing of the security intention to remove.

GKCIET does not accept any liability for vehicles, motorcycles, scooters or bicycles or their contents when parked or left on GKCIET premises.

SECTION 7 - USE OF CLOSED CIRCUIT TELEVISION (CCTV)

7.1 REASONS FOR USE

CCTV is recognised as a powerful tool in the fight against crime, both for prevention and detection. The GKCIET intends to use CCTV systems around the campus covering many of the vulnerable areas, public access points and adjacent streets.

CCTV

i. May reduce the fear of crime and offers public reassurance for students, staff and visitors to the campus.

ii. Can assist in the detection, deterrence and prevention of crime on campus by securing evidence to identify, apprehend and prosecute offenders and to provide evidence for internal disciplinary hearings.

iii. Appropriate signs will be placed around the GKCIET warning that CCTV is in use.

7.2 LOCATIONS

The GKCIET CCTV system may consist of both internal and externally located overt cameras with telemetry and digital recording. It may be agreed that some departments may benefit from a local CCTV system for the reasons described above. The operation of these systems and any future installations in departmental areas, must be authorised by the Director and comply with the IT Act.

7.3 CCTV OPERATING PROCEDURES

It is intended that the information obtained from CCTV will give public confidence that the rights of individuals are being fully protected and the requirements of IT Act are complied with.
Access to the CCTV monitoring and recording systems will be strictly controlled and limited to duty security staff or authorised management.

7.4 THE POLICE (GENERAL) AND CCTV

It is recognised that the Police in the course of their duties may have reason to enter the GKCIET estate. This can be as a result of immediate follow up to an incident, search of premises, being invited to assist the Security Service or post incident investigation.

The Police (where practically possible) should always inform security they intend to work on the GKCIET estate in emergency situations and immediate incident follow up. Security staff should always remain with the Police whilst on the GKCIET estate in such a situation. If Security staff are asked to leave the area by the Police they should remain within the vicinity and ensure the Chairman Estate and Security Officer are informed.

Security staff in attendance would not be applicable for pre-arranged visits or appointments.
Police asking to enter student accommodation/ hostel will be asked by Security Service to produce a warrant ; if a warrant cannot be produced then Dean Students Welfare, the Chairman, (EMC) and Security Officer should be informed. Security staff will not automatically allow access before obtaining clearance. Police should not require access to (nor be allowed access to) GKCIET CCTV Systems except under the following circumstances :

- Emergencies or investigation of serious incidents.
- Identification of offenders.
- Liaison and training purposes, by prior arrangement with the Head of Security.
- As authorised by the Director.

Requests by Police to remove CCTV recordings must comply with the IT Act and will be registered accordingly.

7.5 RECORDED IMAGES

CCTV Images will be kept securely and in line with the requirements of the IT Act.

7.6 COVERT CCTV

Covert CCTV will not generally be used within the GKCIET but may be used in exceptional circumstances to assist in the detection of crime or apprehension of offenders. Before use, permission to use covert CCTV will be obtained through the Director. It will be sited only for a time specific and necessary to the operation. Recordings from covert CCTV will be treated in accordance with the IT Act.

SECTION 8 – CYBER SECURITY POLICY

8.1. Aim and Scope

This policy aims to ensure the confidentiality, integrity, and availability of digital assets, protects institutional data, and safeguard the privacy and security of all stakeholders.

This policy applies to:

- All students, faculty, administrative staff, and third-party users associated with GKCIET Malda.
- All IT resources including computers, servers, internet, Wi-Fi, data centers, email, websites, learning management systems (LMS), ERP systems, and cloud services of GKCIET Malda.

8.2. Objectives

- To prevent unauthorized access to institute networks and data.
- To ensure secure usage of digital infrastructure.
- To establish roles and responsibilities.
- To align with national cyber security and data protection frameworks.

8.3. Governance Structure

A **Cyber Security Committee (CSC)** shall be established comprising:

- Director (Chairperson)
- IT Head (Convener)
- Cyber Security Officer
- Network/System Administrators
- Faculty Representative
- Student Representative

The CSC will oversee implementation, monitoring, and updates to the policy. However, the format of the committee may be segregated if required into two small committees under the Chairperson (Director of the institute) to look after IT Systems and CCTV surveillance of the institute.

8.4. User Responsibilities

All users including faculties, students and staff of GKCIET are required to comply with the security policy. The policy is also applicable to the contractors and third party of GKCIET Malda. Major concerns with the policy are:

- **Authentication:** Users must use strong, unique passwords and not share credentials.
- **Usage Policy:** IT infrastructure must only be used for academic, research, and administrative purposes.
- **Reporting Incidents:** Users must immediately report any suspicious activity or breaches to the IT Cell.
- **Device Security:** Personal and institute-provided devices must have up-to-date antivirus and security patches.

Centralized Committee / IT Cell will be responsible to monitoring and administering the security functions:

- ✓ Fostering a security awareness among all stake holders of the institute including employees, staff and students.

- ✓ Committee will maintain technical security controls and perform risk analyses with responding to security incidents.
- ✓ All stakeholders have a duty to abide by this policy, report security events, and take part in cybersecurity awareness and training programs.

8.5. Network and Infrastructure Security

- **Firewalls and IDS:** A robust firewall and Intrusion Detection System (IDS) to be maintained.
- **Wi-Fi Access:** Role-based access; student access to be monitored and restricted to academic usage.
- **Remote Access:** VPN usage with two-factor authentication (2FA) is mandatory for remote access to sensitive systems.
- **Data Backup:** Critical data should be backed up regularly and stored securely (including offsite/cloud backups).

8.6. Email and Internet Policy

- **Official Email:** All institute communications should be done through official email IDs.
- **Email Security:** Spam filters and malware protection should be enabled.
- **Internet Use:** Browsing of illegal, obscene, or non-academic websites is strictly prohibited.

8.7. Data Protection and Privacy

- **Sensitive Data:** Student records, exam data, personal identification data, and financial data may be encrypted and access-controlled.

Data Retention: Data should be retained only as long as necessary and then securely disposed of.

- **Compliance:** Adhere to the Indian IT Act 2000 (and amendments), UGC and AICTE guidelines on data and digital safety.

8.8. Incident Response and Recovery

- A documented **Incident Response Plan** must be in place.
- The CSC shall investigate and take action on any breach or cyber incident.
- Regular mock drills and audits to be conducted.

8.9. Training and Awareness

- Periodic cyber security awareness sessions for students, faculty, and staff.
- Inclusion of basic cyber hygiene in student induction programs.
- Workshops in collaboration with CERT-In or other government bodies.

8.10. Policy Review and Updates

This policy shall be reviewed annually or as needed in light of emerging threats, technological changes, or legal mandates.

8.11. Enforcement and Penalties

Violations of this policy may lead to disciplinary action including suspension of access, academic penalties, or legal action in accordance with institute rules.