

F. No. 29-12/2025-S&S
Government of India
Ministry of Education
Department of Higher Education
S&S Section

Shastri Bhawan, New Delhi

Dated: 14th July, 2025

To,

VCs and Heads of all CFHEIs

Subject: - Security of Vital Installations – reg.

Sir/Madam,

It is to bring to your notice that as per the threat assessment by Central Security Agency, some terror groups along with their local supporters may carry out sabotage and terror activities targeting Vital Installations including Higher Educational Institutions (HEIs), which are strategically vulnerable.

2. In this regard, HEIs are requested to strengthen the security protocols of their physical assets and may also consult the local police and civil administration to ensure fool proof security.

3. In this regard, dos and don'ts to be followed at the institutional and individual level in the HEIs has been put together by culling out the same from the Security Manuals of GoI and the same may be complied with on priority basis.

(A) PHYSICAL SECURITY MEASURES:-

- i. All officials and employees must display their ID cards not only at the time of entry into the office but keep displaying it during the entire period of stay in the office building.
- ii. Security personnel may frisk and check bags/briefcases of all employees and visitors at the time of entry and/or exit, regularly or occasionally (surprise checks) depending on the requirement. Wherever possible, X-ray Scanners should be installed.
- iii. Security personnel may search and frisk visitors and their belongings depending on the requirement.
- iv. Thorough checking of the material taken in or out of the building, especially in bags or envelopes, should be carried out to ensure that no office items are being taken away unauthorisedly.
- v. Entry of casual labourers in the building for carrying out civil works should be based on proper pass by the reception or security staff. Advance passes of validity period upto maximum 3 days may be issued on the request of contractor and/or a designated officer.
- vi. Guarding Arrangement: - There must be provision of adequate guards, both by day and by night, to prevent the entry of unauthorised persons to the premises. In addition, there should be patrolling of the premises during night hours and during day hours where guards are not deployed. CCTVs may be installed wherever required with a dedicated CCTV monitoring control room round the clock.
- vii. A contingency plan for dealing with any emergency situation like fire, earthquake, flooding, etc., should be prepared for every building by the Security Officer concerned and its copy should be kept with the stakeholders.

Contd...p/2-

- viii. The security vetting of vendors, especially new vendors supplying services, materials & products needs to be rigorously undertaken.
- ix. Ensure 100% serviceability and availability in sufficient numbers of security and safety related equipment besides ensuring urgent repairs, procurement and stockings.
- x. A 24/7 operational control room may be established for continuous situational update and communication with relevant stakeholders (state police, district authorities, civil Defence, and Border Guarding Forces and Coast Guard/ Indian Navy).

(B) CYBER SECURITY MEASURES:-

- i. Cyber Security guidelines for Government Entities available at <https://cert-in.org.in/PDF/guidelinesgovtentities.pdf> and CERT-IN "Technical Guidelines on Software Bill of Materials (SBOM)" (CISG-2024-02) need to be implemented.
 - ii. Increase surveillance and monitoring in and around the installation through foot patrol, waterfront patrol, continuous monitoring through CCTVs cameras by the Security Agencies guarding the Institute.
 - iii. Access control of the Institution needs to be further strengthened with strict protocol for temporary visitors, foreigners, contractual and contingency staff. The pending police verification certificates of employees / contractual employees needs to be expedited. The access control for the interim period before the receipt of PVC needs to be strictly followed.
 - iv. Strict enforcement and monitoring of social media policies, protocols on sharing of official information on unsecured communication network and individual of the departments may be ensured.
 - v. The management, chief security officer, Chief Information Security officer of the Institute may watch for deviant/ suspicious/ abnormal behaviours and informed the relevant authorities. Incidents of security breaches, cyber-attack, sighting of drones. trespassing, observance of suspicious vessels/boats may immediately be reported to the local police and nearest central security agencies.
3. DOs and DON'Ts for Security, Telecommunication and Social Media Uses in respect of Officers, Employees, students, etc., of Institution is annexed.

Yours faithfully,

-sd-

(S. E. Rizwi)

Joint Secretary to Govt. of India

Tele- 011- 23383872

Copy to:

- 1. PPS to Secretary (HE), MoE.
- 2. All BHs of Department of Higher Education.

Copy for information to: Shri R. Kumar, Under Secretary, MHA.



(S. E. Rizwi)

Joint Secretary to Govt. of India

Tele- 011- 23383872

(I) GENERAL SECURITY DOs AND DON'Ts:

DOs

- a. Do read and ensure that your staff have read all security standing orders and instructions relating to contacts with foreigners, etc.
- b. Do ensure at all time the physical security of- (i) your room, (ii) your documents (iii) your selves and almirahs (iv) your seals (v) your operating and duplicate keys.
- c. Do ensure that on closing down for the day, nothing to prejudice security is left lying about in your office even for a short while.
- d. Do make sure of the identity of a visitor first and then give him just what he needs to know to discharge his duty.
- e. Do ensure that all your employees have been properly verified before reemployment.
- f. Do ensure that all classified waste paper is burnt/shredded daily under adequate supervision.
- g. Do report at once to your Supervisory of Departmental Security Officer if you observe any breach of security in your office.

DON'Ts

- a. Do not keep your eyes and ears closed. If everyone is on the lookout for breaches security is assured.
- b. Don't hesitate to have the identity of an unknown visitor established before you pass on any classified information to him.
- c. Don't leave your room with secret papers lying on your desk. Lock them up if you leave your room even for a short while.
- d. Don't take official documents home. If you have to, don't forget that the burden of their security is your personal responsibility.
- e. Don't have classified maps, graphs, charts, photographs etc. displayed open on the walls in your office. Keep them covered or locked.
- f. Don't encourage rumour and garrulity by anyone. On the contrary suppress these firmly.
- g. Do not put your neck out by signing receipts for secret papers without scrutiny.
- h. Don't forget to destroy all drafts, rough notes, spare copies, Steno's notes, carbon papers etc. when you get fair copy ready.
- i. Don't leave your room unlocked at any time.
- j. Don't discuss sensitive subjects and/or classified information on the phone which is a public service.

(II) TELECOMMUNICATION SECURITY DOs AND DON'Ts:

DOs

- a. Do remember that telephone is a public service and not a secret service.
- b. Do remember that the enemy is keen to obtain sensitive information, which you may divulge inadvertently.
- c. Do ensure that no sensitive information is passed over on telephone.
- d. Always check the identity of the Caller, before entertaining the call.
- e. Be polite and courteous while talking over the telephone.
- f. Do not get nervous if a caller identifies himself/herself as a superior officer, especially so if you cannot identify him/her. Do take the number and call back after informing your senior officer.

- g. Do ensure that 2 telephones instruments having an external communication facility has the following pasted on it in bold letters :
"Identify the Caller before giving any Information".
- h. Do ensure that all sensitive telephones are fitted with 'Caller ID' facility.
- i. Bring to the notice of your senior officer if you find any infringement of instructions on security of telephones.
- j. Keep your conversation brief and to the point.

DON'Ts

- a. Do not discuss official matters over telephone and other social media platforms with friends/family members and unauthorized persons on any telephone i.e official/ residence/mobile.
- b. Do not discuss any classified information on the telephone.
- c. Do not disclose the whereabouts/movements of officials of your set- up, Senior officers/VIPs/VVIPs to unauthorized/ unidentified callers. Do not disclose important events/dates to anyone on the telephone, in case you are not sure about the person at the receiving end.

(III) SOCIAL MEDIA USAGE DOs AND DON'Ts:

DOs

- a. Make sure that the family and friends are also sensitized on the risks involved in Social Media, as they too possess sensitive information at times. Be sure to protect the privacy of your family and friends, as carefully as your own.
- b. Ensure location services and geo-tagging features are off and switched on, only when required.
- c. Avoid using location services and geo-tagging features while utilizing Social Media sites.
- d. Be aware of who can see your account. Keep the setting to private and keep the content appropriate.
- e. Use adequate protection measures for domestic Wi-Fi connections.
- f. Remember that anything posted on the electronic media once, even by accident cannot be ever recalled or deleted. Once posted, it is permanent.
- g. Carefully consider the implications of making friends, linking, following or accepting requests from unknown persons.
- h. Do remember that there's no such thing as a "private" social media site. Archival systems save and store information even if you delete a post.

DON'Ts:

- a. Do not share classified information obtained through the official channel or otherwise.
- b. Do not reveal exact posting and nature of work if you are posted in a sensitive Ministry/Department/Organisation.
- c. Do not activate Geo-tagging features when accessing social media sites from place of work.
- d. Don't use the Government emblem, insignia, etc. in your posts.
- e. Do not share anything through a non-authorised platform even if it is unclassified or innocuous like manpower issues, promotions, local orders, etc., which may give an opportunity to the adversaries in gathering intelligence.
- f. Do not unnecessarily post addresses, telephone numbers, bank details etc. as these could make you, your friends and family a target.
