

Campus and Facilities Management Procedure - Security

Purpose

1. This Procedure gives effect to parts of the Campus and Facility Management Policy in outlining the requirements and processes for maintaining a safe campus environment.

Scope

2. This Procedure applies to the GHE campus and any activities undertaken on campus.
3. Provisions for online security are outlined in the Campus and Facilities Management Procedure – Information Technology.

Definitions

4. Definitions for key terms are presented in the Glossary of Terms which may be accessed on the GHE website at <https://www.globalhe.edu.au/policy>

Suite documents

5. This Policy is linked to the following suite documents:
 - a) Campus and Facilities Management Policy;
 - b) Campus and Facilities Management Procedure – Information Technology;
 - c) Campus and Facilities Management Procedure – Space and Capacity.

Procedure

Security personnel

6. Security personnel are based on the GHE campus to respond rapidly to security incidents, emergency situations and threats. Their visible presence serves to assure students and staff of a safe workplace, and to deter offenders.
7. Information about how to contact security personnel, and in what circumstances, is provided to students and staff through all key communication channels such as the GHE website, posters and stickers around the campus and through induction and orientation programs.

Appointment of a provider

8. GHE uses a third-party security service provider for all campus security.
9. The appointment of the security service provider will be undertaken via a competitive tender process, renewed every two years, with selection based on:
 - a) previous experience;
 - b) cost;
 - c) level of services;
 - d) references including all due diligence checks such as police checks, insurances and licenses to provide the services contracted.

10. The tender process is managed by the Operations Director. Tenders are considered by a panel consisting of:
 - a) the Academic Director;
 - b) the Chief Executive Officer;
 - c) an independent member of the Audit and Risk Committee or Board of Directors.

Role of security personnel

11. Security personnel are:
 - a) required to be on campus during opening hours and manage appropriate access to students, staff and visitors;
 - b) entitled to request students, staff and visitors to provide their identification, and ask individuals to leave the premises where they fail to do so;
 - c) required to maintain a logbook to record activities such as search and patrolling, visitors' information, deliveries, shift logs, incidences logs, and security personnel attendance logs.
12. Security personnel will call police when there is a physical threat to people on campus, or individuals do not comply with a request to leave the campus. They will also call an ambulance when there is a medical emergency.
13. Security personnel will be present at functions and events where security is required.
14. Senior managers (Academic Director, Operations Director) are responsible for advising IIBIT IT Services of any extraordinary security requirements, on or off campus, at least two weeks prior to the event.

Back-up arrangements

15. In addition to specific security personnel, a Fire Warden is appointed who will cooperate with the Chief Fire Warden assigned for the building in which the GHE campus is situated (see **Human Resources Framework**).
16. In the event of a non-emergency critical incident staff and students can contact a trained Fire Warden who in turn may call the security personnel if required.

Closed-Circuit Television (CCTV)

17. Closed-circuit television (CCTV) systems are installed in key areas such as entrances and exits and appropriate signs are placed at key positions and in proximity to the area under surveillance.
18. Once the recording capacity of the CCTV system is exceeded, overwriting will commence so that at any given time, the CCTV footage will extend only to that previous period of time which represents the relevant system's recording capacity.
19. Upon request, CCTV footage is provided to law enforcement agencies, such as the Police, if it is necessary for a law enforcement activity.
20. IIBIT IT Services is responsible for the installation and management of CCTV systems.

Other campus security measures

21. Staff are responsible for ensuring their office is locked when not in use and confidential documents are stored in a cabinet that has a lock.
22. Advice on security-related matters may be sought at any time from senior managers in InfoTech Professionals under the Shared Services Agreement.

Building access

23. Access to areas on campus is controlled by means of locks and keys and/or electronic access control systems, which are managed by IIBIT IT Services and Facilities Management.

24. Requests for master keys or lift access cards require the approval from IIBIT IT Services and Facilities Management or the Operations Director.
25. IIBIT IT Services and Facilities Management maintains a register with the issue of all keys and access cards.
26. Access is revoked in the event of staff leaving the organisation or upon the request of the original approver.

Roles and responsibilities

27. The Board of Directors is responsible for the overall governance of this Procedure.
28. The Operations Director is responsible for:
 - a) the management and implementation of this Procedure;
 - b) the maintenance of any records that arise from this Procedure.
29. Security personnel are responsible for the safety and security of the campus and its occupants.
30. The Manager, Quality and Compliance is responsible for:
 - c) ensuring compliance with this Procedure;
 - d) ensuring that staff are adequately notified of the existence of this Policy and the related procedures;
 - e) benchmarking GHE policy and standards with those adopted elsewhere in the tertiary sector;
 - f) the monitoring of information available from the review of records relating to the implementation of this Procedure.
31. All staff are responsible for becoming familiar with and complying with this Procedure.

Associated information

Related Internal Documents	<p>Campus and Facilities Management Policy Campus and Facilities Management Procedure – Information Technology Campus and Facilities Management Procedure – Space and Capacity Business Continuity Policy Critical Incident Policy Financial Framework Human Resource Framework Teaching and Learning Plan Records and Data Management Policy Risk Management Policy Strategic Plan Student Complaints, Grievances and Appeals Policy Student Non-Academic Conduct and Misconduct Policy Glossary of Terms</p>
Related Legislation, Standards and Codes	<p><i>Tertiary Education and Quality Standards Agency Act 2011</i> <i>Higher Education Standards Framework (Threshold Standards) 2021</i> TEQSA Guidance Notes: <i>Wellbeing and Safety</i>, Version 1.2 <i>Education Services for Overseas Students Act 2000</i> <i>National Code of Practice for Providers of Education and Training to Overseas Students 2018</i> <i>Work Health and Safety Act 2012 (SA)</i></p>
Date Approved	25 September 2020
Date of Effect	25 September 2020
Date of Review	June 2026
Approval Authority	Board of Directors
Policy Custodian	Chief Executive Officer
PinPoint DocID	2953

Change history

Version Control	Version 1.1	
Change Summary	4-Sept-20	V1.0 Draft approved by Board of Directors 25-Sept-20
	9-Oct-23	V1.1 administrative updates following TEQSA registration

Warning - Document uncontrolled when printed! The current version of this document is maintained on the GHE website at <https://www.globalhe.edu.au/policy>