Campus and Facilities Management Procedure – Information Technology

Purpose

1. This Procedure gives effect to parts of the Campus and Facilities Management Policy in outlining the requirements and processes for the provision and maintenance of a secure information technology infrastructure.

Scope

2. This Procedure applies to the management of all GHE's technology assets. These include but are not limited to:
   a) technology aspects of library collections and services;
   b) the Learning Management System (LMS);
   c) hardware and software to support teaching and student learning;
   d) hardware and software to support administration and key business processes;
   e) the Student Management System (SMS);
   f) the records management system;
   g) website infrastructure;
   h) electronic communication systems.

Definitions

3. 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

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

Procedure

Access control

5. All users of GHE information technology must be authorised to access relevant resources and systems to ensure that access is regulated and that unauthorised access attempts are detected and prevented.
6. Access control comprises identification, authorisation and authentication.

Identification

7. All users of GHE information technology are assigned a unique Windows Active Directory account which will enable their controlled access to relevant resources and systems.

8. IT systems and applications that are not managed centrally via Windows Active Directory are expected to follow the same requirements for access management.
9. Login details may never be shared under any circumstances and users are responsible for all actions taken under their sign-on.

Authorisation

10. Senior managers (Academic Director, Operations Director) are responsible for authorising appropriate access to their domain-specific resources/systems to enable staff to perform their duties.
11. IIBIT IT Services are provided through the Shared Services Agreement is responsible for enabling the required access.
12. Senior managers (Academic Director, Operations Director) will inform IIBIT IT Services of any staff exits or terminations so their access can be revoked.

Authentication

13. Access to non-public information technology resources and systems will be achieved by a combination of unique login ID and password.

Passwords

14. User accounts are created with a random password and users are required to change upon initial login.
15. All user accounts passwords must be changed before the expiry period of 180 days.
16. Users can register for the online self-service password management portal to change or reset their forgotten password.

Password standards

17. Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
18. Password must be at least eight characters in length and contain characters from three of the following four categories:
    a) uppercase characters (A through Z);
    b) lowercase characters (a through z);
    c) base 10 digits (0 through 9);
    d) non-alphabetic characters (for example, !, @, #, $, %).
19. Passwords must not be identical to the previous two passwords.
20. User accounts are temporarily locked-out if a wrong password is used in more than five logon attempts.
21. Once a user account is locked out, it remains locked for one hour or until the user resets their password in the password reset portal. Users can also reset passwords by contacting the IT Service Desk.
22. Users must under no circumstances reveal their account password.

Data security

23. All electronically held information should be stored in network locations or systems which are regularly backed up and in the event of a system failure can be retrieved from an existing backup. Specific procedures in relation to data security, including asset disposal, are specified in the **Records and Data Management Policy**.

Server security

24. The server room must be secured with appropriate locks and must be kept locked at all times. Access should be restricted to relevant information technology staff only.
25. A CCTV camera must be placed in a location that can capture images of persons accessing the server room.

Use of the internet and email

26. Use of the internet and email is integral to the educational activities of staff and students. Reasonable personal use of the internet is permissible providing users do not:
    a) participate in online activities that are likely to bring GHE into disrepute, create or transmit material that may be defamatory or incur liability for GHE;
    b) visit, view or download any illegal or inappropriate material;
    c) knowingly introduce any form of computer virus into GHE's network;
    d) hack into unauthorised areas;
    e) download any material belonging to third parties, unless permitted under an agreement or licence;
    f) use the internet for personal financial gain or illegal or criminal activities;
27. When using GHE email users must not:
    a) create, retain or distribute any material that includes offensive or abusive comments based on any attributes protected under equal opportunity and discrimination legislation (see *Associated Documents*), or that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, defamatory or libellous and as outlined in the **Student Diversity and Equity Policy**, the **Student Sexual Assault and Sexual Harassment Policy** or the **Human Resources Framework**;
    b) engage in any activity that is likely to be a breach of copyright, licence provisions or intellectual property rights.

Damage or disruption

28. Any damage or disruption to any of GHE's digital facilities or resources must be reported to the IIBIT IT Services as soon as possible.

Breaches

29. Individuals who become aware of, or are personally subject to, any improper use of the internet or email at GHE may make a complaint or seek assistance under the following:
    a) for students the **Student Complaints, Grievances and Appeals Policy** or the **Student Sexual Assault and Sexual Harassment Policy**, depending on the nature of the incident;
    b) for staff, grievance procedures in the Human Resources Framework.
30. Any student alleged to have misused digital resources at GHE will be investigated under the **Student Non-Academic Conduct and Misconduct Policy.**
31. Any staff alleged to have misused digital resources at GHE will be investigated under the Staff Code of Conduct and Grievance Resolution mechanisms in the **Human Resources Framework**.

Roles and responsibilities

32. The Board of Directors is responsible for the overall governance of this Procedure.
33. Senior managers (Academic Director, Operations Director) are responsible for:
    a) the management and implementation of this Procedure;
    b) the maintenance of any records arising from this Procedure.

34. Senior managers are responsible for authorising appropriate access to their domain specific resources/systems.
35. The Manager, Quality and Compliance is responsible for:
    a) ensuring compliance with this Procedure;
    b) ensuring that staff are adequately notified of the existence of this Policy and the related procedures;
    c) benchmarking GHE policy and standards with those adopted elsewhere in the tertiary sector; and
    d) the monitoring of information available from the review of records relating to the implementation of this Procedure.
36. All staff are responsible for becoming familiar with and complying with this Procedure.

Associated information

Related Internal Documents	Campus and Facilities Management Procedure – Information Technology Campus and Facilities Management Procedure – Security Campus and Facilities Management Procedure – Space and Capacity Business Continuity Policy Critical Incident Policy Financial Framework Human Resources Framework Learning Resources Collection and Review Policy Records and Data Management Policy Risk Management Policy Strategic Plan Student Complaints, Grievances and Appeals Policy Student Non-Academic Conduct and Misconduct Policy Student Sexual Assault and Sexual Harassment Policy Student Wellbeing, Orientation and Support Policy Teaching and Learning Plan Work-Integrated Learning Placement Policy Glossary of Terms
Related Legislation, Standards and Codes	*Tertiary Education and Quality Standards Agency Act 2011* *Higher Education Standards Framework (Threshold Standards) 2021* TEQSA Guidance Note: *Technology-Enhanced Learning,* Version 1.2 *Education Services for Overseas Students Act 2000* *National Code of Practice for Providers of Education and Training to Overseas Students 2018* *Age Discrimination Act 2004* (Cth) *Australian Human Rights Commission Act 1986* (Cth) *Disability Discrimination Act 1992* (Cth) *Disability Standards for Education 2005* (Cth) *Equal Opportunity Act 1984* (SA) *Racial Discrimination Act 1975* (Cth) *Sex Discrimination Act 1984* (Cth) *Work Health and Safety Act 2012 (SA*) *Workplace Gender Equality Act 2012* (Cth)
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	2952

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