

Business Continuity Procedure

Purpose

1. This Procedure gives effect to the Business Continuity Policy by outlining the processes to be undertaken for business continuity, recovery planning and the ongoing delivery of critical business processes when incidents disrupt normal operations.

Scope

2. This Policy applies to the entire GHE entity and all staff, students and visitors.
3. The prevention of critical incidents is governed by the **Risk Management Policy**.
4. The management of critical incidents is governed by the **Critical Incident Policy**.
5. Specific protections for students in the event of a disruption that affects GHE's ability to continue to provide a course are governed by:
 - a) the **Course Teach-Out Policy**;
 - b) the **Student Fees, Charges and Refunds Policy**.

Definitions

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

Suite documents

7. This Procedure is linked to the Business Continuity Policy.

Procedure

Critical business processes

8. For business continuity purposes, critical business processes fall into one of three categories as follows:
 - a) **Safety and Security**: include activities which are necessary to maintain a safe and secure environment for all students, faculty, staff, campus visitors, and the surrounding community;
 - b) **Business Support Services**: include activities that allow the institution to maintain vital business operations, safeguard assets, and secure the financial viability of the institution. Examples of business support services include students' record management, payroll, revenue collection, accounts payable and financial reporting;
 - c) **Teaching and Learning**: include all services that directly support the academic mission of GHE. Examples include student services such as admissions and enrolment, delivery of courses and graduation services.
9. Examples of risks applicable to GHE's business continuity are outlined in Table 1.

Table 1: Business Continuity Risks

Business continuity risks	Impacted critical business processes
Loss or inaccessibility of facility	Teaching and Learning
Utility failures (power, heating, air, water)	Safety and Security Business Support Services Teaching and Learning
Infectious disease/pandemic	Safety and Security Business Support Services Teaching and Learning
Transportation to campus is unavailable	Safety and Security Business Support Services Teaching and Learning
Dependent business unit or third-party provider suffers a business disruption	Business Support Services Teaching and Learning
Loss of registration as an education provider	Teaching and Learning
Serious non-compliance/Show Cause/Conditions on Registration	Teaching and Learning
Unavailability of employees (serious injury/death/sudden resignation)	Safety and Security Business Support Services Teaching and Learning
Critical software unavailable (client server or web)	Safety and Security Business Support Services Teaching and Learning
Computer hardware failures	Safety and Security Business Support Services Teaching and Learning
Replacement cost or delay for equipment/hardware and office assets	Business Support Services Teaching and Learning
Vital records destroyed or unavailable to access	Business Support Services
Data corruption or theft including cyber attack	Safety and Security Business Support Services
Insufficient business continuity and disaster recovery planning causing inappropriate response time	Safety and Security Business Support Services Teaching and Learning

Business Impact Analysis

10. The Operations Director will ensure that business continuity requirements are assessed on an annual basis, and/or following a serious incident, via a Business Impact Analysis (BIA) for each category outlined in Table One.
11. The BIA will be developed and renewed with input from the managers of each area and must include the following:
 - a) recovery time: the length of time a business process could be unavailable before the impact reaches an unacceptable level;

- b) financial and intangible impacts: includes impacts such as the interruptions of cash flow into the institution, the costs of mitigating a disaster, financial penalties for failing to meet contractual obligations, in addition to intangible consequences such as those dealing with safety of students and staff, the level of quality maintained by academic and research programs, and public image and reputation;
- c) application dependencies: modern business applications are commonly dependent on information technology resources, such as systems, software, data, and personnel. The business impact analysis should consider the interdependencies of institutional processes;
- d) priority for recovery: assessment of the priority for recovery for each business process or function (High/Medium/Low).

12. BIAs will be reviewed and in place for the start of the academic calendar year.

Business Continuity Plan

13. The Business Continuity Plan (BCP) identifies and documents existing workarounds and continuity arrangements should a business continuity risk impact on GHE's operations.

14. The BCP is developed by the Operations Director in response to BIAs and updated as required to ensure currency. The BCP must include actions and resourcing for:

- a) short-term continuity of service provision (usually 0-30 days dependent on the disruption);
- b) business recovery (process for ensuring a return to business as usual).

15. The BCP must:

- a) identify the resources required to ensure timely restoration of a minimum acceptable level operations. At a minimum these include people (specialist and support); IT infrastructure; information and data (hardcopy and electronic); office and specialist equipment; facilities and accommodation; internal dependencies and/or interfaces (e.g. other business units); external dependencies and/or interfaces (e.g. suppliers, contractors, customers, competitors and regulators etc.);
- b) include a communications strategy which should identify who needs information, what information is needed, how that information can be provided, what constraints on its provision might exist and who has the authority to approve the communications;
- c) be documented in such a way that it is of practical use in a disaster and that it fulfils business, regulatory, training and audit requirements;
- d) be updated to reflect any changes to business functions and activities, key dependencies, facilities and supporting infrastructure etc.

Testing and review

16. The Operations Director must ensure that testing of the effectiveness of the Business Continuity Plan is undertaken at least once every two years. This may take the form of one of the following types of testing:

- a) scenario based testing;
- b) transfer of some critical functions to the offsite location to confirm the feasibility of the plan;
- c) transfer of all critical functions for an extended period to the fall-back location; and/or
- d) communications testing.

17. The Operations Director will monitor and review the results of testing with a view to improving performance.

18. Every seven years the Operations Director will seek an independent review of all policy, procedure and plans relating to business continuity and recovery, or sooner should risk management processes identify a significant change in GHE's risk profile.

Recording and reporting

19. The Audit and Risk Committee has responsibility for the monitoring and review of business continuity planning for GHE on behalf of the Board of Directors.
20. The Operations Director will report the following to the Audit and Risk Committee:
 - a) the outcomes of developing the Business Impact Analyses;
 - b) Business Continuity Plans and any significant updates;
 - c) any disruptions to continuity and remedial actions.
21. The Audit and Risk Committee will report instances and recommendations to the Board of Directors.

Roles and responsibilities

22. The Board of Directors is responsible for the oversight and governance of risk management, including business continuity.
23. The Audit and Risk Committee is responsible for the monitoring and review of risk management, including business continuity planning.
24. The Operations Director is responsible for:
 - a) the management of business continuity planning, including reporting any incidents to the Audit and Risk Committee, and the overarching implementation of the plan on an as needs basis;
 - b) the testing and review of the Business Continuity Plan and all associated policies and procedures;
 - c) the management of all records arising from this Procedure.
25. Managers of business areas are responsible for completing a Business Impact Analysis for their area and its submission to the Operations Director.
26. 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.

Associated information

Related Internal Documents	Business Continuity Policy Course Teach-Out Policy Critical Incident Policy Enrolment Policy Governance Framework Risk Management Policy Student Fees, Charges and Refunds Policy Student Wellbeing, Orientation and Support Policy Glossary of Terms
Related Legislation, Standards and Codes	<i>Tertiary Education and Quality Standards Agency Act 2011</i> <i>Higher Education Standards Framework (Threshold Standards) 2021</i> TEQSA Guidance Notes: <i>Corporate Governance</i> , Version 2.4 <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>
Date Approved	1 May 2020
Date of Effect	1 May 2020
Date of Review	June 2026
Approval Authority	Board of Directors
Policy Custodian	Chief Executive Officer
PinPoint DocID	2681

Change history

Version Control	Version 1.2	
Change Summary	15-Apr-20	V1.0 Draft approved by Board of Directors (BoD) 1 May 2020
	23-July-20	V1.1 Administrative updates
	9-Oct-23	V1.2 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>