

Business Continuity Policy

October 2025

Approving authority:	Audit and Risk Committee
Consultation via:	Global Director of Governance and Legal Services, BCP Global Working Group, University Executive
Approval date:	4 September 2025
Effective date:	1st October 2025
Review period:	Every two years from the date of approval
Responsible Executive:	University Secretary and Vice-Principal (Governance and Operations)
Responsible Office:	Assurance and Legal Services

POLICY

HERIOT-WATT UNIVERSITY
Business Continuity Policy

Section	Content	Page
1	Introduction	3
2	Purpose	3
3	Objectives	4
4	Scope	4
5	Incident Management Policies	5
	5.1. On-Campus Incidents	5
	5.2. Off-Campus Incidents	5
6	Roles and Responsibility	5
	6.1. Gold & Silver Team	5
7	Requirements for Review, Updates and Simulations	5
8	Insurance	6
9	Confidentiality	6
10	Glossary	7
11	Further Help and Advice	8
12	Policy Version and History	8

POLICY

1. INTRODUCTION

‘Business Continuity is the capability of an organisation to continue delivering products and services within acceptable time frames at predefined capacity during a disruption’ (ISO 22313:2020 Security and Resilience – Business Continuity Management Systems).

This policy outlines the University’s framework for responding to severe or major disruptions to operational activities supporting learning and student experience, research, and day-to-day administrative functions across the University. This includes activities at specific campuses and/or Group functions. It aims to assist the University in identifying critical activities which require to be maintained with the minimum of disruption to the operations of the University, alongside supporting the capacity to address incidents which have occurred and to resume normal operations within agreed timeframes.

2. PURPOSE

The Business Continuity Policy has been developed to provide a framework for Business Continuity Planning (BCP) at all campuses and establish roles and responsibilities for management and oversight of BCP incidents. The University aspires to be compliant with the global ISO 22313:2020 standard on Security and resilience - Business continuity management systems, therefore this policy has been developed with that consideration.

The BCP Policy has been developed within a broader framework consisting of:

- the values, vision, culture, mission, and goals of the University;
- the University’s governance and reporting structures;
- legal, regulatory, and other requirements applicable to the University;
- associated incident management plans, including on-campus Emergency Incident Management Plans, the IS Disaster Recovery Plan, Communication strategies, and the Reputational Incident Management Plan.

3. OBJECTIVES

The University’s strategy for the development and maintenance of Business Continuity (BC) plans addresses the following broad objectives:

- Develop BC plans that minimise the inevitable disruption caused by a BCP incident whilst supporting the business to restore the University's resources, infrastructure, and services as close to their original state.
- Identify and prioritise the University's critical services and resources using a consistent and reliable Business Impact Analysis (BIA) process.
- Create effective contingency strategies for critical services (as determined by the BIA process) using a risk-based approach to be included in the BC plans.
- Develop incident management procedures that are efficient and practical for use and which merge seamlessly with BC plans.
- Develop BC plans that are appropriate, regularly reviewed, available to the relevant internal audience, easy to follow, and understand.
- Provide regular training and simulations to all staff with direct BCP responsibility to ensure relevant staff better understand their roles in BCP situations.
- Regularly assess the efficacy and suitability of the University's Business Continuity Plans, considering any relevant changes including to the University's structure and services plus changes to legal and regulatory requirements.
- Promote awareness of BCP throughout the University, including raising awareness of the BCP Policy, and plus ensuring BCP concerns are incorporated into relevant strategic and operational decision making.

4. SCOPE

- The University's BC plans encompass all campuses and Group functions.
- Underpinning Business Impact Assessments address the five key BCP resources - People, Campuses/Buildings, Systems, Data, and Suppliers/Partners, and consider the potential disruption caused by the loss of one or more of these resources over a range of timeframes.
- BC plans apply to all university staff, students and activities, including learning, teaching, research, and Professional Services.
- The University has relevant Emergency Incident Management plans in place. EIM is in place at all campuses for on-campus incidents and is co-ordinated by Safeguarding Services. EIM is also in place for off-campus incidents (e.g. reputational and travel incidents) is co-ordinated by Assurance and Legal Services.
- Once an incident has concluded, the University's BCP is invoked, where applicable, supported by the Assurance and Legal Services team (ALS).

- All BCP incidents are managed by a Gold or Silver team, dependent on the severity of the incident, and which have defined memberships of relevant senior managers.
- ALS support the coordination of response activities during the disruption and then the recovery of impacted assets or services during that period, liaising with IS on any of their disaster and recovery plans, plus engaging with the Communications team to ensure there is effective and timely communication to all staff and students.

5. EMERGENCY INCIDENT MANAGEMENT PLANS:

5.1. ON-CAMPUS INCIDENTS:

The on-campus Emergency Incident Management Plans at Heriot-Watt University provides a comprehensive framework for handling on-campus emergencies, ensuring that incidents are managed efficiently and effectively, and links to the University's broader BCP when necessary.

5.2. OFF-CAMPUS INCIDENTS:

The management of off-campus incidents at Heriot-Watt University, which may include reputational or travel issues related to students, employees, or university facilities, is guided by a comprehensive Incident Management process, and also links to the University's broader BCP when necessary.

6. ROLES AND ACCOUNTABILITIES

The overall accountability for BCP arrangements sits with the University Secretary, who is authorised to invoke the Business Continuity Plan when required. In the Secretary's absence, delegated individuals may invoke the BCP, as detailed in the BCP document. This accountability includes ensuring that there are satisfactory BC plans in place to address the range of possible incidents with clear accountabilities for management of responses to individual incidents.

There are Gold and Silver response teams, as set out below, which are made up of applicable senior members of the management team, and who are responsible for managing individual incidents based on their severity. Assurance and Legal Services is responsible for supporting the development and maintenance of suitable BC plans across the University, with underpinning BIAs in place, and that simulation testing of BCP takes place on a 2-year cycle with follow up actions implemented.

6.1. GOLD & SILVER TEAMS

In the event of a specific BCP incident, the University has clearly defined Gold and Silver teams, with defined membership of applicable senior management team members, who would respond to any strategic or operational incidents, both on and off campus. The Gold team is responsible for BCP responses which would impact the University at a strategic level, whilst the Silver team deals with operational incidents.

7. REQUIREMENTS FOR REVIEW, UPDATES AND SIMULATIONS

The BC plans and underpinning BIAs are reviewed and updated at least every two years, or when there are significant changes to the University's structures or business. In addition, training and testing is carried out in form of BCP simulation exercises with management to test responses and identify actions for improvement. This work ensures satisfactory BC plans are in place, and associated procedures remain valid and effective, and are consistent with the University's BCP objectives.

Regular internal audit and other external reviews are also conducted from time-to-time to assess the effectiveness of the BC plans, and all actions for improvement are followed up as required.

8. INSURANCE

The University maintains appropriate Business Interruption insurance at its campuses to provide coverage for loss of income and increased costs of working.

9. CONFIDENTIALITY

The University's BC plans are held in confidence and are only shared with relevant members of the senior management team, given the nature of the information held and data confidentiality requirements.

10. GLOSSARY

Heriot Watt Group	HW Group	Means those entities associated with the University whether by ownership of shares or otherwise and which the Court determines should form part of the Heriot-Watt Group for the purposes of the Charter and Statutes, and which are listed in the Ordinances
Business Continuity	BC	The capability of the university to continue delivery of products or services at acceptable predefined levels following a disruptive incident
Business Continuity Plan	BCP	Documented procedures that guide universities to respond, recover, resume, and restore to a pre-defined level of operation following disruption. Typically, this covers resources, services and activities required to ensure the continuity of critical business functions.
Business Impact Assessment	BIA	Assessment of the impact of disruption to five key BCP resources: people, buildings/campus, data, systems, and suppliers/partners over a variety of timeframes.
Disaster Recovery Plan	DR	Ability of the IT elements of the University to support its critical business functions to an acceptable level within a predetermined period of time following a disaster.
Incident		Events that have the potential to cause significant disruption to normal operation. For example, - a fire or flood that stops the operation of all or part of the campus. - a disruption in the supply chain that affects the universities' ability to function. - severe weather that stops staff from getting to work. - disease outbreak that causes a large number of student or staff absences.
Incident Management		Process for responding to unplanned events and recovery of normal operation state.
Staff		All persons employed by the University or by any member of the Heriot-Watt Group and applicable contractors/temporary staff/volunteers.
Student		Persons pursuing a programme of study at the University.
Premises		Buildings, together with its land and outbuildings, which are occupied by any member of the HW Group.

Infrastructure		The basic physical and organisational structures and facilities (e.g., buildings, roads, and power supplies) are needed for the University's operation.
IT Systems		All electronic data processing, information, recordkeeping, communications, telecommunications, account management, inventory management and other computer systems (including all computer programs, software, databases, firmware, hardware, and related documentation) and Internet websites.
Data and Records		Facts and statistics collected for reference, research, or analysis.
Supplier		An external organisation that provides a product or service to the University.
Business as Usual	BAU	Normal execution of standard functional operations within the University.
Lesson Learned		A brief exercise conducted at the end of a BCP incident to identify elements that worked well and areas for improvement, which can be incorporated into future plans.

11. FURTHER HELP AND ADVICE

For further information and advice about this Policy and any aspect of records management and information governance, contact:

Assurance and Legal Services Division
 Governance and Legal Services
 Email: assurance@hw.ac.uk

12. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V. 1.0	4 September 2025	Audit and Risk Committee	First published version