

*Approved by the Academic Council Decision
(Protocol No. 2, 24.2025)*

Business Processes Continuity Plan

The city of Tbilisi

2025

Tbilisi, Bagebi, Tskneti Highway No. 67

www.Alterbridge.edu.ge

+995 558 198 198

E-Mail info@alterbridge.edu.ge

Article 1. General provisions.

The purpose of the Business Processes Continuity Plan of Alterbridge University LLC (hereinafter referred to as "the University") is to ensure the uninterrupted delivery of the educational process and to prevent or minimize deviations from planned operations. To this end, the teaching university identifies high-probability risks that may have a significant impact on its business processes. To reduce and eliminate these risks, procedures have been developed for the planning and implementation of preventive measures. For each of these risks, a designated team of staff members is assigned responsibility for taking appropriate action and ensuring the continued management of processes under normal operating conditions. The purpose of the Business Processes Continuity Plan is to establish a coordinated chain of actions between University leadership and personnel in the event of a crisis, ensuring a rapid and effective response to maintain the continuity of the educational process and, more broadly, the sustainability of overall university operations.

Article 1. Risk essence and its classification

1. A risk is a potentially harmful event associated with natural disasters or irrational actions by University personnel and students, which resulted in damage or destruction of University property, deterioration of the health of staff and students, harm to the ecological environment, etc.
2. The inherent nature of risks within the University is determined by their characteristic features and origin, and they are classified as follows:
 - Natural risks (floods, earthquakes, hurricanes, hailstorms, and others);
 - Functional business risks, natural (structural damage, fire, accidents, environmental pollution, ecological conditions, etc.); and technical (disruption of communication networks, data storage and recovery systems, software systems, network functionality, as well as viral and hacker attacks, etc.) (see **Annex 1**);
 - Risks associated with entrepreneurial and financial activity (bankruptcy, breach of contractual obligations, unanticipated suspension of the continuity of business processes at the University due to financial difficulties, and others);
 - Civil liability risks, which are related to the responsibility for compensating damages caused to third parties, including both legal and natural persons.
 - Pandemic, epidemic - an infectious disease whose spread poses a real threat to human life and/or health, and/or creates the need for specific regulatory measures.

3. The risk is the potential damage that may be incurred to the University in the realization of this risk. It is characterized by four major features:
- Object - University - Risk carrier;
 - Time interval;
 - Damage causing harm;
 - Damage type.
4. The grouping and prioritization of risks at the University depends not only on the frequency of their occurrence (i.e., actual damage) and the severity of their consequences, but also on influencing factors (the seismic resistance of buildings, the functionality of communication, electrical, heating, and sewage systems, the reliability of the information technology infrastructure, etc.).

Article 3. Risk Management

1. Risk management at the University is carried out by using methods, mechanisms, and tools, aimed at risk reduction.
2. The goal of business processes continuity at the University is to formalize the risk management process, namely, to develop and implement a dedicated program through which risks will be monitored and controlled.
3. Risk management at the University includes four stages:
 - Detect risks and identify them as fully as possible;
 - Analyze and evaluate the identified risks;
 - Selection of risk management strategy;
 - Practical implementation of risk management control and monitoring.

Article 4. Risk management tools.

1. The continuity plan for business processes discusses two groups of risk impact factors, referred to as "physical" and "financial" management tools:
 - Physical management tools are: Introduction and following of all safety rules, creation of firefighting conditions, strengthening building construction, minimizing hazardous routes and etc.
 - Financial instruments do not alter the likelihood or severity of an adverse event, but they reduce or entirely eliminate the financial losses incurred by the University as a result of such

events.

2. Insurance, as a risk management tool: For the university, potential insurable events include fire, explosion, lightning strike, the crash of an aircraft or any of its parts onto the insured property, etc.

- Fire - an open fire that independently expands after its appearance from the fireplace, in a different place or spontaneously crossed this place;
- Explosion - a sudden devastating occurrence of the gas or steam pressure, rapid chemical reaction of the unsustainable system, followed by the dismantling/breakdown of the outer walls of the object. Reservoir (boiler, pipeline and etc) explosion is considered an event during of which the reservoir walls are so damaged that will result in balancing of internal and external pressure. If the explosion occurs within the reservoir, due to the rapid chemical reaction, the damage will be compensated in case of immutability of the reservoir walls;
- Natural disasters - earthquakes, hurricanes, storms, hail, floods, heavy snowfall, rainstorms;
- Water disruption - Sudden breakdown of water pipes, heating, fire extinguishing, sewage systems; Water invasion from neighboring facilities, groundwater output;
- Inflicted damage by third parties - theft, robbery, pillage, unlawful act by third parties. Under these conditions, insurance covers the insured building-facilities only when forcible entry methods are used, in case of such obvious signs of entering the place and the insured objects are lost or damaged after this action.

Article 5. Evaluation of risk environment

1. The risk environment assessment in the university implies the following basic requirements:
 - The management process should not be difficult;
 - We do not have to think about developing a precise mechanism for risk evaluation, as it is not applicable;
 - Risks must comply with the competence of employees, who are responsible for their management;
 - Risk management requires responsibility and accountability.
2. To identify risks, the university may use a range of general methods:
 - Structural approach;
 - Inviting experts;

- Analysis of previous failure;
- Controlling questionnaire;
- Analysis of the potential source of risk.

3. To assess the risk environment correctly, it is necessary to define risks. Determining the boundaries of acceptable and unacceptable risks is the determination of risk inclination.

Main objectives:

- Identify priority risks;
- Each employee of the university should understand what risks he/she should receive and how to manage it;
- Establishment of the culture of risk.

Article 6. Risk Assessment Stages

1. At the university, the risk assessment stage consists of two levels:
 - Collection of information;
 - Detecting threats or incidents.
2. To ensure the effective execution of this activity, the university establishes a business continuity working group, which collects statistical and financial data for the purpose of qualitative and quantitative risk assessment and, in case of necessity, conducts direct inspection of the layout of the threat.

Article 7. Business Continuity Planning

Business continuity planning is a dynamic and process, which gives possibilities to changes of circumstances and / or risks adaptation and ensures further development of security.

The university's business continuity plan primarily serves to ensure the safety of individuals. At the following stage, building / facilities protection and implementation of appropriate protective measures and, finally, protection of the organization's infrastructure and critical business processes, which provides the teaching / learning processes and operation of information systems in continuous mode. For the purpose of effective implementation of business continuity management, according to the Rector's legislative act, which determines members, their rights and duties, instructions and action plans for different situations. Based on the above:

To ensure business continuity, an emergency response team/management unit has been established with the following composition:

- a. Head of the emergency response team – rector
- b. Deputy head of the emergency response team for evacuation matters – head of the finance department
- g. Deputy head of the emergency response team for material and technical supplies – head of the material and technical supply department.

d. Assistant to the Head of Emergency Staff for Communication and notifications – head of the information technology department;

e. Head of Fire-Rescue Group - Head of Protection and Security Service;

6. Business Continuity Management team meets at least once a semester to discuss the business continuity plan and make appropriate changes.

7. Business continuity plan is kept in electronic and reprinted format.

8. The business continuity plan is reviewed and approved by the decision of the head of the Emergency Situations.

Business Continuity Plan

Risk category: Natural disasters

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Earthquake	Medium	Major	The building's seismic resistance is ensured	5 days	Security Service	Access to infrastructure	Rector Security and Safety Department Finance Department

Landslide	Low	Minor	<p>Immediate evacuation of students and staff to designated safe areas, in accordance with the evacuation plan;</p> <p>Contacting the relevant local and central government authorities to request assistance with response coordination.</p>	3 days	Security Service	Access to infrastructure	<p>Rector</p> <p>Security and Safety Department, Finance Department, Doctor</p>
Fire	Medium	Major	<p>Compliance with fire safety regulations;</p> <p>Equipping server and network infrastructure rooms with fire protection systems to prevent damage from high temperatures or fire;</p> <p>Immediate evacuation of students and staff to designated safe areas, in accordance with the</p>	3 days	Security Service	Access to infrastructure	<p>Rector</p> <p>Security and Safety Department, Finance Department, Doctor</p>

			<p>evacuation plan;</p> <p>Contacting the relevant local and central government authorities to request assistance in organizing response efforts.</p>			
Floods, mudflow	Medium	Moderate	<p>Immediate evacuation of students and staff to designated safe areas, in accordance with the evacuation plan;</p> <p>Contacting the relevant local and central government authorities to request assistance in organizing response efforts.</p>	2 days	Security Service	<p>Access to infrastructure</p> <p>Rector</p> <p>Security and Safety Department,</p> <p>Finance Department,</p> <p>Doctor</p>

Hurricane	Medium	Minor	Immediate relocation of students and staff to designated safe areas, in accordance with the evacuation plan; Engaging relevant local and central government authorities to request support in organizing response operations.	2 days	Security Service	Access to infrastructure	Rector Security and Safety Department, Finance Department, Doctor
-----------	--------	-------	--	--------	------------------	--------------------------	--

Risk category: Technology

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Cyber- attack (information infrastructure hacking or virus attacks)	Medium	Major	Monthly antivirus inspection;		Information Technology Department and Material and Technical	Access to reserve servers	Information Technology Service

					Support Department		
Termination of Internet Services	Medium	Moderate	Wireless Internet access or service purchase. from alternative Internet services suppliers	24 hours	Information Technology Department and Material and Technical Support Department	Availability of internet service	Information Technology Service
Disruption of telephone service	Medium	Moderate	securing alternative sources	24 hours	Information Technology Department and Material and Technical	Availability of internet service	Information Technology Service

Support
Department

Risk category: Operational

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Targeted damage to infrastructure: Damage to building	Low	High	Considering the quality and frequency of the damage	Considering the extent of the damage	Security and Safety Department, Finance Department, Doctor	Accessibility of the administrative building	Head of Finance Department
Loss or destruction of equipment and supplies	Low	Moderate	Monthly inspection	1 day	Security and Safety Department, Finance Department, Doctor	access to equipment, supplies	Head of Finance Department

Loss or destruction of movable property	Low	Moderate	Monthly inspection	1 day	Security and Safety Department, Finance Department, Doctor	access to educational inventory	Head of Finance Department
---	-----	----------	--------------------	-------	--	---------------------------------	----------------------------

Risk category: Outflow of high percentage of employees (dismissal, suspension of labor relations, due to unforeseen causes)

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Academic Staff	Low	High	Related to working conditions	5 working days	Rector	Temporary replacement, vacancy	Rector
			Rapid response to problems			Announcing	
Invited personnel	Low	Moderate	Related to working conditions	5 working days	Rector	Temporary replacement, vacancy	Rector
			Rapid response to problems			Announcing	
			Response				
Administrative personnel	Low	High	Encouragement, recognition, and promotion related to working conditions	2 weeks	Rector	Temporary replacement, vacancy	Rector

			Related			Announcing	
			Rapid response to problems, paid leave days,				
			Individual				
			flexible work schedule				
Support staff	Low	Moderate	Recognition and promotion related to working conditions	10 days	Rector	Temporary replacement, vacancy	Rector
			Related			Announcing	
			Rapid response to problems, paid time off, and individualized, flexible work arrangements				

Risk category: Termination of utility services (electricity, heating, water)

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Electricity	Low	Moderate	Backup power supply through an autonomous electricity generation system;	1-5 days		Ensuring power supply (backup generator)	Head of Finance Department

Electricity supply on the premises of Alterbridge

periodic inspection of systems;

Protection of network and server infrastructure through the use of surge protection and uninterruptible

power supply systems;

Ensuring the storage of backup copies of created, processed, and used information;

The existence of security mechanisms

provided by the relevant company,

based on contractual agreements,

to protect stored information.

Information
Technology
Service

Heating	Low	Moderate	Annual inspection of the heating system, shut-off and control valves	1 day	Material and Technical Support and Security Services	Heating provision	Head of Finance Department
			Equipped with device				
Water	Low	Moderate	Check the water pipes when needed	1 week	Security service, material and technical support service	Provision of water	Head of Finance Department
			Shutter/startup				
			Equipped with device				

Risk category: Financial and Legal

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Lack of tuition fees	Medium	High	payment	1 month	Finance Department	Finding additional resources	Head of Finance Department
			Constant monitoring				
			of payment				
	Medium	Moderate	Increase in income	1 year		Additional resources	

Limited availability of grants and funding					Finance Department	finding	Head of Finance Department
Taxes	Low	High	flexible, effective mechanisms	1 week	Finance Department	Additional resources	Head of Finance Department
			use			finding	

Risk category: Pandemic/Epidemic

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Specific or online learning/work modalities, the need for distance regulation, and the requirement for building access control.	Medium	High	Implementation/enforcement of necessary regulations, Procurement/upgrade of relevant equipment, staff training, and deployment of online platforms	10 days	Legal Department, Finance Department, Information Technology Department, Educational Process Management Department,	Access to infrastructure and information	Rector

Physician,
Material and
Technical
Support
Department,
Security
Department,
Quality
Assurance
Department

Risk category: Fines and penalties,

Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Administrative	Low	High	Control of the work performed	3 days	Lawyer	Finding additional resources	Head of Finance Department
			Strengthening				
Tax penalties	Low	Major	Consultation with auditors	8 months	Lawyer	Finding additional resources	Head of Finance Department
other	Low	High		5 months	Lawyer	Finding additional resources	Head of Finance Department

Legal disputes	Medium	High	In a timely manner properly perform	Several weeks	Lawyer	Act accordingly	Head of Finance Department
Risk category: Breach of Contract							
Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Technical Service	Low	High	Constant communication	3 months	Lawyer	Finding additional resources	Head of Finance Department
Educational services	Low	High	Constant communication	2 weeks	Lawyer	Additional resources finding	Rector
Risk category: Strategic - authorization / accreditation							
Risk	Probability (high, medium, low)	Impact (minor, moderate, major)	Preventive action	Disruption Period	Responsible unit/person	Action	Evaluation
Accreditation	Low	High	Compliance with standards	1 year	Evaluation Assurance Service,	Transfer under the student mobility rule Program update	Rector

					Program Coordinator		
					Dean		
Authorization	Low	High	Compliance with standards	1 year	Evaluation	Transfer under the student mobility rule	Rector
					Assurance Service,	Submission of the monthly authorization application	
					Program Coordinator		
					Dean		

<ul style="list-style-type: none"> ▪ Earthquake; ▪ Landslide; ▪ Fire ▪ Floods, mudslides ▪ Storm; ▪ Other types of technogenic and natural disasters; ▪ Pandemic/Epidemic 	<ul style="list-style-type: none"> ▪ Cyber- attack (information infrastructure hacker or virus attacks); ▪ Interruption of telephone and internet services; ▪ Protection of processed information in services and systems 	<ul style="list-style-type: none"> ▪ Targeted damage to infrastructure: Damage to the building, loss / destruction of equipment, supplies, movable items; ▪ Outflow of high percentage of employees (dismissal, suspension of labor relations, due to unforeseen causes); ▪ Interruption of utility services (electricity, heating, water) 	<ul style="list-style-type: none"> ▪ Decline in income; ▪ payments; ▪ Fines and penalties; ▪ Legal disputes; ▪ Violation of lease agreements 	<ul style="list-style-type: none"> ▪ Authorization / accreditation loss
--	--	---	---	--