

(LEPL) Iakob Gogebashvili Telavi State University



Business Process Continuity Plan

Reviewed at the meeting of the Academic Board: Protocol N13 14. 03. 2018

Reviewed at the meeting of the Academic Board: Protocol N 28 30.11.2023

Chair of the Academic Board, Rector /Shalva Tchkadua/

Approved at the meeting of the Representative Council: N 5 14.03.2018

The amendments are approved at the meeting of the Representative Council: N21 01.12.2023

Chair of the Representative Council: / Manana Gharibashvili /

Telavi
2018

(LEPL) Iakob Gogebashvili Telavi State University

Business Process Continuity Plan

The Business Process Continuity Plan is a document that reflects the changes in the environment that affect LEPL Iakob Gogebashvili Telavi State University (hereinafter referred to as TESAU). The document is fully in line with TESAU business continuity policy. The Business Process Continuity Plan (hereinafter-„BCP") is very important for the smooth functioning of any organization. BCP is able to restore and continue business processes in crisis situations.

University administration at any time, including in case of significant or minor delay in processes, is obliged to ensure the continuity of educational and organizational processes.

The objectives of BCP are:

- Identify key functions and critical activities, including the resources they need;
- Develop a plan and identify the necessary resources to return to the usual process in the shortest possible time;
- Ensuring business continuity process during emergencies, with appropriate resources (restoration of operational processes in the catalytic situation).

BCP covers three main areas:

- **Maintaining** a safe academic environment for all students, employees and the surrounding community, communications, data storage and recovery, software systems, network access.
- **Learning, teaching and research** - academic and other institutional processes; All programs and services that directly contribute to the implementation of the mission of the University.
- **Actions in support of business activities** in relation to resources ☐ - which will allow TESAU to maintain business activities, protect human resources, property and ensure the financial viability of the institution.

BCP is treated as a "live" process and consists of the following components:

- **Incident management system**, which includes management, coordination and control of critical situations;
- **Analysis of the impact of business**, which includes the maximum wait of the university as an educational institution;
- **Risk assessment**, which determines the degree of danger caused by various events for the University;

- **Risk management**, which includes written and publicly disseminated strategies to restore important functions, activities outlined for working groups and contact details of those responsible.
- **Updating the plan**, which means constantly updating the plan and constantly introducing to the staff (both academic and invited staff, as well as administrative and support staff) and students.

The Incident Management System is one of the first to be managed by the university, which serves to provide uninterrupted services to TESAU staff and students and increase the productivity of staff. All the levels of the university are involved in the incident management system and are obliged to cooperate with all structures in case of minor delay, and on a wide scale, e. g. work with the emergency management service in times of danger.

Business Impact Analysis - determines the estimated time of delay for the university and ensures the maintenance of a safe environment for everyone during this period. Groups working on the business continuity process set specific goals and determine costs to create a safe environment for students and co-workers. In addition, actions are carried out that help maintain the property, financial condition and mission of the university.

Risk assessment, which ensures the determination of the degree and severity of potential hazards as a result of technical and natural catastrophes, which negatively affects TESAU.

The threat is assessed in terms of the ability to influence TESAU.

Risk management is a single, continuous and specific action plan used to reduce risks in case of danger. The team responsible for the implementation of BCP evaluates the risks in terms of public safety, after which the team carries out a set of actions to prevent expected delays and reduce risks (Mitigation).

An essential component of risk management is the procedures to be implemented during risk realization and the response provided by the incident plan. It is necessary to inform employees, students, other persons in TESAU and determine the real time determined for the restoration of processes.

Plan update - by taking into account the experience, BCP should be updated annually depending on the change/needs of business processes, regularly checking existing strategies, and systematically informing staff and students.

In order to coordinate the implementation process of BCP, a team is created, which includes: Head


of Administration (Leader), Deputy Rector, Deputy Head of Administration, Head of Material Resources Service, Head of Financial Service, Head of Public Procurement Department, Automated Education Management Systems Administrator, Human Resource Management Manager, Head of Public Relations Service.

BCP strives to create a flexible system to prevent or reduce the following risks. Such risks are:

- Destruction / loss of buildings;
- Destruction / loss of ICT or other data;
- Personnel injury/death/non-appearance at work;
- Loss of other technologies/equipment/equipment, internet, power supply, etc.;

To achieve the goal, three phases are separated, depending on the objective (Recovery Time Objective -RTO) basis of the recovery time using the RTO table:

- Emergency phase (priority 1 - immediate reaction 0-24 hours)
- Continuous phase (priority 2 - intermediate solution 1-7 days)
- Recovery phase (priority 3 - return to normal mode > 7-28 days)

Operational Risk	Tasks for Improving Operational Risk	
Information Technology	Control mechanisms	Determination of risk assessment and risk indicators
Human factor	Standards Implementation	Introduction of an integral database of losses, analytical tools, continuous improvement of software
Processes/Systems	Constant control/ monitoring	Preventive management
External factors	<p>Types of loss; Date of detection of losses; Violation/error; Accident scene; Accident time and frequency; The volume of loss; The cause of the occurrence of risk; The relationship between various causes, places and events; Operational risk category; Source of information.</p> 	
Legal/procedural errors		
	<p>Registration; Control/detection; Decision-making; Statistical analysis; Simulation; Evaluation.</p>	

The main operational risks of TESAU include:

(The amendment is approved at the meeting of the Representative Council: Protocol N 21 01.12.2023)

1. Risks associated with compliance with educational standards;
2. Risks associated with access to financial resources;
3. Risks associated with human resource management;
4. Cessation of utilities;
5. Risk associated with damage to training and material resources;
6. Risks associated with information technology, technical equipment, laboratory equipment and internet services;
7. Risks associated with force majeure situations;
8. Risks associated with reputation and brand awareness.

Scheme 1: Plan of Operational Risk Factors, Mechanisms of Control over these Factors and Preventive Measures - Business Process Continuity Plan:

Risk Assessment						
N	Risk Name	Probability of happening (high, medium, low)	Influence on university activities (high, medium, low)	Prevention and control mechanisms	Ways to Improve/Preventive Measures	Responsible
1. Risks related to compliance with educational standards						
1.1.	Termination of accreditation of educational programs	low	Medium	Possession of information related to the accreditation standards of educational programs	Alignment of educational programs with accreditation standards	University and faculty quality assurance services; Program Workers
1.2.	Loss of university authorization	low	high	Possessing information related to HEI authorization standards	Constant monitoring of compliance with the authorization standards of the University; Monitoring of the Strategic and Action Plans of the University and Determination of Change Needs	Rector; Head of Administration; Quality Assurance Service; Faculty Workers; Departments
2. Risks associated with access to financial resources						

2.1.	Increase in new and/or additional financial obligations caused by legislative changes	low	high	Constant monitoring of taxes	Assessment of financial condition and changes	Head of Administration; Financial-Material and Public Procurement Service
2.2.	Increase in financial liabilities caused by administrative, tax penalties and legal disputes	low	high	Constant monitoring of taxes; Constant control of legal obligations	Assessing the financial situation and making changes;	Head of Administration; Financial-Material and Public Procurement Service; Legal Office
2.3.	Reduction of the number of university students	low	high	Constant monitoring of student contingent and revenues;	Labor Market Research; Correct information and advertising campaign	Administration; Departments
2.4.	Risk associated with the unexpected costs	Medium	Medium/High	Constant monitoring	Implementation of appropriate measures to eliminate the risk associated with unforeseen costs	Administration; Financial and Material Resources Management and Public Procurement Service
3. Risks associated with human resource management						
3.1.	Decrease / outflow of the number of academic staff	low	high	Affiliation, incentives, flexible salary system, etc. – Involvement of academic staff in a professional development scheme	Temporary replacement of academic staff with relevant qualifications,- Announcing a competition for the position.	Human Resources Management Service, Deputy Rector

3.2.	Reduction / outflow of the number of invited personnel	low	Medium	Incentives, offering a flexible workload scheme, flexible payroll system, etc. – Engaging invited personnel in a professional development scheme	Temporary replacement of personnel with relevant qualifications, Announcing a competition for a position/inviting new staff.	Human Resources Management Service, Deputy Rector
3.3.	Reduction / outflow of the number of administrative and support personnel	low	Medium	Use of methods provided by the Human Resources Management Policy (incentives, flexible workload and payroll system, etc.)	Distribution of work among existing employees, temporary replacement of personnel with relevant qualifications, announcement of a competition for the position	Head of Structural Unit - Human Resources Management Service
4. Termination of utilities						
4.1.	Electricity Termination	low	Medium	University System wiring monitoring	Providing an alternative source of electricity	Material resource Specialist
4.2.	Heating system damage	low	Medium	Inspection of heating system before the start of the season (twice a year)	Implementation of relevant measures	Heating System Superintendent
4.3.	Termination of water supply	low	Medium	Quarterly inspection of water supply	Implementation of relevant measures	Water Supply Technician
5. Risk associated with damage to training and material resources						

5.1.	Damage to training buildings	low	Medium	Inspection of buildings by the expert bureau; Permanent inspection of buildings by university administration	Implementation of preventive measures to eliminate the threat	Head of Administration; Financial and Material Resources Management and Public Procurement Service;
5.2.	Damage to other auxiliary buildings	low	Medium	Inspection of buildings by the expert bureau; Permanent inspection of buildings by the university administration;	Implementation of preventive measures to eliminate the threat	Head of Administration; Financial and Material Resources Management and Public Procurement Service;
5.3.	Damage to the library building	low	high	Permanent inspection of the building	Implementation of preventive measures to eliminate the threat	Head of Administration; Head of the Library; Financial and Material Resources Management and Public Procurement Service;
5.4.	Damage to working rooms	low	low	Weekly inspection of rooms	Implementation of preventive measures to eliminate the threat	Head of Administration; Financial and Material Resources Management and Public Procurement Service;
5.5.	Damage to study auditoriums and laboratories	low	low	Weekly inspection of auditoriums and laboratories	Implementation of preventive measures to eliminate the threat	Head of Administration; Financial and Material Resources Management and Public Procurement Service; Lab specialists

5.6.	Documentation (including archive)	low	high	Security Assurance	Carrying out preventive measures to eliminate the threat; Ensuring safe storage of documents	Head of Administration; Stationery
6. Risk associated with information technology, technical equipment, laboratory equipment and Internet services						
6.1.	Computer and other devices	low	high	Constant monitoring of computer and other devices;	Planning financial and technical measures necessary for repair and renewal	Financial and Material Resources Management and Public Procurement Service; Office of Information Technologies
6.2.	Laboratory Equipment & Supplies	low	high	Constant monitoring of laboratory equipment and supplies	Planning financial and technical measures necessary for repair, refurbishment and filling supplies	Financial and Material Resources Management and Public Procurement Service; Faculty Administration; Lab specialists

6.3.	Termination of the Internet connection	low	high	Intensive monitoring of networks	Determining the internal cause of termination of the Internet connection by eliminating the internal cause; Informing the supplier of the company's termination and ensuring their response	Office of Information Technologies
6.4.	Software disruption	Medium	high	Constant monitoring of server devices and hosting	Updates, antiviruses, data backups, cybersecurity	Information Technology Service; Electronic Systems Administrator Supplier Company
7. Risks associated with force majeure situations						
7.1.	Risk of natural disasters (floods, storms, hurricanes, earthquakes)	Medium	high	Arrangement of infrastructure: informing staff about behavior during natural disasters;	Evacuation from the building; Sending a notification to the Emergency Situations and Emergency Service;	University Administration; Emergency Response Coordinator
7.2.	Fire	Medium	high	Arrangement of firefighting infrastructure	Evacuation from the building; Call a fire team	University Administration; Fire Safety Response Coordinator
7.3.	Terrorist acts	low	high	Arrangement and strengthening of protection and security mechanisms	Evacuation from the building; Sending a notification to the Emergency Situations and Emergency Service;	University Administration; Emergency Response Coordinator

7.4.	Restrictions caused by viruses and the pandemic	Medium	high	Familiarization/consideration of state recommendations	Readiness to switch to remote format of training and workers	University Administration; faculties; services.
8. Risks associated with reputation and brand awareness						
8.1.	Low Recognition of the University	low	high	Constant contact with stakeholders	Information Campaign Production	Administration; International Service of International Development and Public Affairs
8.2.	Negative sentiment towards the university	low	high	Constant monitoring of the satisfaction of the interested parties	Information Campaign Production	Administration; International Service of International Development and Public Affairs
8.3.	Negative media reactions	low	high	Constant monitoring of media outlets	Permanent contact with the media	Administration; International Service of International Development and Public Affairs