Approved by Rector's directive No 12 of 20 March 2025

In force from: 20.03.2025

Business Continuity Policy

1. General

1.1. The Business Continuity Policy defines the fundamental principles of business continuity at Tallinn University of Technology (hereinafter referred to as "the university") and establishes the specific conditions, bases, and principles for ensuring business continuity. The goal of the Business Continuity Policy is to define the university's strategic approach to ensuring business continuity.
1.2. The university implements a business continuity management system that includes risk management (incl. risk identification, analysis, evaluation, and treatment), incident and crisis management (incl. integrated monitoring solutions), disaster management, and business continuity monitoring.
1.3. The aim of the business continuity management system is to strengthen the university's resilience against disruptions in core activities (incl. research and development, teaching, and business operations) by enhancing preparedness for potential incidents and crises, minimising their impact, and ensuring quick restoration of normal operations. The business continuity management system is closely interconnected with both information and physical security.
1.4. The purpose of the Policy is to establish the principles and processes for ensuring business continuity, define the required roles, and assign responsibilities. The Policy has been developed with consideration of the university's internal and external context, as well as its key stakeholders, including employees, students, and partners.
1.5. The Policy applies to all the university's structural units, employees, students, and partners involved in the university's activities or utilising the university's resources. The Policy has been developed in alignment with the Quality Concept of Tallinn University of Technology and the ISO 27001 international standard.

2. Definitions

2.1. "**Business continuity"** means the university's ability to carry out its core operations without disruption or to swiftly restore them in the event of incidents or crises. Managing business continuity requires implementation of a structured approach by the organisation, i.e. the establishment of a business continuity management system (BCMS).

2.2. Risks

2.2.1. "**Risk management"** means a set of coordinated activities to manage an organization depending on the risks. Risk management is conducted in accordance with the university's risk management policy, with specific adjustments made based on the type of risks within the context of business continuity (e.g., information security risk management focuses on information systems and IT assets, by addressing risks related to the confidentiality, integrity, and availability of information).

2.3. Incidents and crises

2.3.1. "**Incident**" means an unplanned event that undermines or reduces service quality, causes service disruptions, endangers human life, causes material damage or harms the reputation of the university.
2.3.2. "**Crisis**" means a highly hazardous situation that impacts the university, its members, and their activities, causing damage (including property, reputation and/or other damage) to the university or its members that cannot be resolved using standard operations and resources.
2.3.3. "**Incident and crisis management**" means the management and coordination of activities associated with an actual or potential occurrence of an incident or a crisis.
2.3.4. "**Incident and crisis response plan**" means a key component of incident and crisis management that includes a documented set of procedures and guidelines for assessing incident or crisis severity, escalation, notification, and implementation of recovery actions.

2.4. Disaster management

2.4.1. "**Disaster management**" means a systematic process for addressing the consequences of incidents and crises.

2.4.2. “**Disaster recovery plan**” means a plan that outlines how an organisation can resume normal operations, disrupted by an incident or crisis, within a specified time period and budget by utilising physical, technical, procedural, and human resources.

3. Scope of application

3.1 The business continuity management system applies to all of the university's information systems, physical assets and services that support its core processes.

4. Principles for maintaining business continuity

4.1. A key element in maintaining business continuity is the mapping of the university’s assets.
4.2. As regards business continuity, the focus is primarily on processes and the recovery of associated components, such as services and information systems.
4.3. Business continuity has been integrated into the responsibilities of current employees.
4.4. All business continuity plans are based on risk analysis and include relevant risk management measures to ensure continuity and resilience.
4.5. Business continuity is maintained using existing financial and human resources, with additional resources allocated as needed based on reasoned requests (incl. those resulting from identified risks).
4.6. Regulations, guidelines, and procedures related to business continuity are approved through the standard decision-making process.
4.7. Business continuity requires consistent testing and training.
4.8. As part of the business continuity process, regular audits and corrective actions are carried out to ensure continuous improvement of the system.
4.9. All business continuity plans and guidelines are documented, regularly reviewed, and updated as needed.

5. Business continuity objectives

5.1. To enhance the university's resilience against disruptions in core operations and ensure a sense of security for its members.
5.2. To implement a risk-based approach to identify and evaluate business continuity risks, and to apply appropriate measures to mitigate them.
5.3. To develop preparedness for potential incidents and crises.
5.4. To minimise the impact of incidents and crises.
5.5. To ensure the rapid recovery of normal operations

6. Organisation and management of business continuity

6.1. The business continuity manager:
6.1.1. is responsible for planning, developing, implementing the business continuity management system and keeping it up to date;
6.1.2. leads the business continuity team, ensuring methodological consistency, effective team operations, regulatory adequacy, and accessibility of regulations for the university community;
6.1.3. coordinates the activities of the business continuity team, ensuring the smooth operation of the team and achievement of the goals;
6.1.4. provides guidance on preparing business continuity and disaster recovery plans, as well as incident and crisis management frameworks;
6.1.5. continuously improves the business continuity management system based on the results of monitoring and testing of the business continuity management system;
6.1.6. regularly conducts training sessions and information campaigns to raise awareness of business continuity principles and practices across the university;
6.1.7. regularly conducts business continuity training sessions and mock drills to test and improve business continuity and disaster recovery plans, ensuring the university’s readiness for various crisis scenarios;
6.1.8. organises assessments of the university’s crisis preparedness based on monitoring results and case analyses and ensures regular updating of the business continuity plan;
6.1.9. analyses and assesses potential incidents or crises and provides relevant recommendations;
6.1.10. consistently focuses on raising awareness among members of the university community, ensuring they are prepared to respond effectively to potential threats;

6.1.11. remains independent and objective in relation to the person being inspected when conducting inspections, making observations and conclusions, providing recommendations, and communicating results;
6.1.12. ensures effective collaboration and communication on business continuity matters among all relevant stakeholders.

6.2. The process owner (area director, i.e. member of the Rectorate):

6.2.1. ensures business continuity planning, allocation of resources for preventive measures, and preparedness within his(her area of responsibility to effectively manage crises and incidents;
6.2.2. coordinates risk management and the implementation of preventive measures within the assigned area of responsibility.

6.3. The head of sector (the head of a structural unit):

6.3.1. manages risk assessment, business continuity planning, implementation of preventive actions, and analysis of monitoring results within his/her area of responsibility;
6.3.2. ensures that all business continuity measures and activities within his/her area of responsibility comply with applicable policies and procedures;
6.3.3. ensures that business continuity activities are integrated into daily work procedures and that all employees are aware of their roles and responsibilities in maintaining business continuity;
6.3.4. is responsible for resolving incidents within his/her sector.

6.4. The business continuity team (network)

6.4.1. The team is led by the business continuity manager.
6.4.2. The team consists of heads of sectors and process managers who are consistently engaged in business continuity planning and communication.
6.4.3. The business continuity team is responsible for coordinating risk management related to physical threats, cyber and reputational crises, as well as for developing regulations, preventive measures, and conducting incident analysis.
6.4.4. Members of the business continuity team receive training and participate in exercises to ensure they are prepared to coordinate the university community's response during crises and incidents.

6.5. The crisis manager

6.5.1. The role of the crisis manager is fulfilled when a crisis situation occurs, following a pre-defined process (crisis plan) until the crisis is resolved.
6.5.2. The crisis manager is responsible for managing crisis resolution within his/her specific area (physical threats, cyber crises, or other sector-specific crisis) and organising initial recovery activities based on established disaster recovery plans.
6.5.3. The crisis manager is responsible for coordinating the actions required to resolve crisis situations.
6.5.4. The crisis manager is responsible for communication with all relevant parties during a crisis, including engaging the Marketing and Communications Office.
6.5.5. The crisis manager follows the framework for action established in the crisis plan and coordinates the crisis resolution process accordingly.
6.5.6. The crisis manager is authorised to give orders to the members of the university community during a crisis to ensure effective resolution of the crisis and maintain security. The crisis manager is authorised to use the university's physical, technical, and human resources within the limits set by the Rector to resolve the crisis. Resources must be used in accordance with the terms established in the crisis plan.
6.5.7. When necessary, the crisis manager requests additional resources from the Rectorate, providing a rationale for their required use.
6.5.8. The crisis manager conducts a post-crisis assessment and submits a report detailing the resolution actions, decisions, and resource usage.

6.6. The incident coordinator (process manager, head of a sub-unit)

6.6.1. The role of the incident coordinator is fulfilled when an incident occurs, following a pre-defined process until the incident is resolved.
6.6.2. The role of the incident coordinator is primarily performed by the heads of sub-units of structural units/process managers (as specified in the sectoral order).
6.6.3. The incident coordinator ensures the effective resolution of high-priority and critical incidents.
6.6.4. The incident coordinator is responsible for managing communication related to the incident.
6.6.5. The incident coordinator escalates the incident to a crisis if necessary.
6.6.6. The incident coordinator ensures that all incidents are resolved in accordance with established procedures and that key lessons are documented and applied.

7. Supervision

7.1 Supervision over the implementation of the business continuity policy shall be conducted by the Internal Audit Office in accordance with its work plan, but not less frequently than once every three years.