Procedure

2026-10-27

Registration number: MIUN 2026/1985

Procedure for Business Continuity Management

Published: 2026-10-27

Decision-makers: Vice-Chancellor Anders Fällström

Responsible function: Security Coordinator

Administrator: Lars Hägglund

Date of decision: 2026-10-27

Period of validity: For the time being

Last review: 2026-10-27

Summary: The rules of procedure regulate responsibilities, roles and work processes for continuity management at Mid Sweden University in accordance with Ordinance (2022:524) on state authorities' preparedness. The procedure complements the University's procedure for crisis organization and aims to create the conditions for the operations to maintain critical functions in the event of disruptions or interruptions.

Previous versions: Newly established

Table of contents

Introduction **3**
Purpose **3**
Scope **4**
Responsibilities and roles **4**
Vice-Chancellor 4
University Director and Deans of Faculty 4
Heads of Department and Heads of Divisions 5
Digitalisation and service 5
System owner 6
Employees and other professionals 6
Business continuity management work process **6**
Identify critical activities 7
Plan for disruptions 7
Act during disruptions and interruptions 8
Practice and develop the ability 8
Follow-up and review **9**

Procedure for Business Continuity Management

Introduction

Continuity management aims to ensure that operations can be maintained in the event of disruptions or interruptions, in peacetime crisis situations and in the event of elevated preparedness. For Mid Sweden University, this is important because education, research and administrative processes are largely dependent on human resources, premises, information, digital systems, communication and internal and external deliveries.

Continuity management is a central part of a systematic and risk-based approach to crisis and contingency planning. The work includes identifying critical operations, planning for disruptions, practicing and testing the ability, and continuously following up and improving working methods and measures. The administrative procedure supports the Agency’s work in accordance with Ordinance (2022:524) on state authorities’ preparedness and forms part of the University’s system of internal governance and control.

Through this systematic work, the university should be able to maintain its mission in education, research and collaboration even in the event of serious disruptions that affect the university's operational capacity.

Purpose

The purpose of the procedure is to clarify responsibilities, roles and working methods in the work with continuity management at Mid Sweden University. The rules of procedure shall help ensure that critical operations can be maintained in the event of disruptions affecting operations and create conditions for operations to act in a coordinated manner in the event of disruptions and interruptions affecting priority business processes, systems, resources and dependencies.

The administrative procedure has been developed to support Mid Sweden University's planning and implementation of measures to maintain business

continuity in accordance with Ordinance (2022:524) on state authorities' preparedness. The work will be coordinated with the University's risk and vulnerability analysis (RSA), crisis management planning, information security work and (if necessary) planning for heightened preparedness.

Scope

The rules of procedure apply to the entire Mid Sweden University and cover business processes, resources, information as well as the systems, services and other dependencies on which the university is dependent to conduct education, research and administrative functions.

The rules of procedure shall be applied in the process of planning for and maintaining business continuity in the event of disruptions or interruptions that may affect the University's ability to conduct priority activities.

Responsibilities and roles

Vice-Chancellor

The Vice-Chancellor has overall responsibility for ensuring that there are conditions for comprehensive and effective work with continuity management and preparedness, and that the work is organised and followed up at university-wide level.

University Director and Deans of Faculty

The University Director and Deans of Faculty are responsible for:

- set out the overall direction and priorities for business continuity management;
- ensure that the work is integrated into the university's governance and management,
- monitor the ability and need for improvement measures.

Heads of Department and Heads of Divisions

Heads of department and heads of divisions are responsible for:

- ensure that its own operations plan for and are prepared to maintain research, training and administrative processes in the event of disruptions or interruptions (including but not limited to IT disruptions);
- identify mission-critical processes;
- determine which activities should be prioritised in the event of disruptions;
- decide on the transition to alternative ways of working for business processes in the event of disruption of digital systems.

Security Coordinator

Security coordinators are responsible for coordinating the University's business continuity management and ensuring connection to RSA, crisis management and contingency planning. This includes:

- managing the business continuity planning methodology, templates and requirements;
- coordinate the planning, follow-up and review of business continuity plans for priority activities;
- ensure that business continuity is based on the RSA and agreed priorities;
- planning, coordinating and following up training and practice related to continuity and preparedness;
- coordinate follow-up and learning from disturbances, exercises and reviews.

Digitalisation and service

Digitalization and service is responsible for:

- support business continuity management activities related to digital dependencies, including through templates and processes;
- ensure that the digital infrastructure is planned and managed with the conditions to deal with disruptions and disruptions;

- coordinate and manage the university's prioritization of IT systems in the event of major disruptions or interruptions,
- follow up and contribute to the development of the work on the continuity of digital infrastructure, systems and services.

System owner

System owners are responsible for:

- ensure that IT systems and digital services within the system group have business continuity plans and are managed so that disruptions or interruptions can be managed;
- require storage, backup and information management so that information can be handled securely and in the long term;
- decide on the transition to alternative or manual working methods within the system in the event of disruption;
- collaborating with the business on prioritization of disruptions and restoration of systems.

Employees and other professionals

Employees and others working at Mid Sweden University are responsible for following decided alternative ways of working in the event of disruptions or interruptions, and for helping to ensure that operations can be conducted on the basis of the priorities decided upon. It also includes being involved in developing our capacity for continuity, including participating in exercises.

Business continuity management work process

Continuity work shall be carried out systematically and include the following elements.

Identify critical activities

The operations shall identify which parts of the operations are critical for the University to be able to maintain its mission in the event of disruptions affecting prioritized business processes. This shall include:

- identify mission-critical processes and functions;
- identify dependencies on information, skills/staff, premises, systems, infrastructures and the supply chain;
- assess the impact of reduced functionality or disruption of business processes, information and digital systems;
- consider RSA and other risk assessments as a basis for what is critical and which measures should be prioritised;
- determine the prioritisation of operations and systems in case of disruptions.

Plan for disruptions

The business shall plan for how the business can be maintained in the event of disruptions affecting prioritized business processes and resources. This shall include:

- business continuity plans are in place for business-critical processes (including necessary system support) and communicated with stakeholders;
- alternative or manual ways of working may be used in the event of interruption;
- dependencies to external suppliers are identified and managed (e.g. contractual requirements, alternative supply routes and contact routes in case of disruption);
- tolerable downtimes or unavailability are established for mission-critical functions and systems;
- prioritisation in the restoration of operations and systems can be made on the basis of identified needs;

- information security and information protection are also maintained in alternative or manual ways of working.

Act during disruptions and interruptions

In the event of disruptions and interruptions that affect the University's ability to conduct prioritised operations, the operations must be able to maintain critical functions through coordinated management of incidents, continuity measures and crisis management. This includes:

- decisions to activate business continuity plans or introduce alternative ways of working are taken within the framework of normal business and system responsibilities;
- prioritisation of activities and systems forms the basis for decisions on measures to be taken in the event of disruption;
- Continuity management is coordinated with the University's incident management and crisis organisation,
- conditions are in place to return to normal working methods after a disruption or interruption.

Practice and develop the ability

The ability to handle disruptions and interruptions that affect operations shall be developed and monitored regularly. This includes:

- exercises are carried out to test business continuity plans and the ability of the organisation to cope with disruptions and disruptions;
- experiences from exercises and incidents are documented;
- identified improvement measures are taken care of in the further work,
- business and system continuity plans are regularly reviewed and updated in the event of changes in the business, organisation, system or risk picture. In connection with updates, a new version shall be communicated to those concerned.

Follow-up and review

Continuity work must be followed up continuously through checks, documentation and compilations. The security coordinator is responsible for compiling the results of the follow-ups carried out, which gives an overall picture of the status of the continuity work within the university.

The results of the follow-up shall be used as a basis for improvement measures and further development of the business continuity work. The rules of procedure and related plans/procedures shall be reviewed regularly and updated as necessary, for example in the event of changes in operations, organisation, risk profile or governing requirements.