Approved by Rector's directive No 46 of 17 November 2026

In force from: 17.11.2026

Principles for Ensuring the Continuity of Critical Services and Technical Systems at Tallinn University of Technology

1. General provisions

1.1 The purpose of this document is to establish uniform principles at Tallinn University of Technology (hereinafter 'the university') for ensuring the continuity of critical services, technical systems and physical infrastructure, as well as security of supply, with a focus on preparedness for power outages, backup power and related technical dependencies.
1.2 The document establishes:
1.2.1 the continuity levels;
1.2.2 the principles for identifying critical systems;
1.2.3 the principles governing the use of uninterruptible power supplies (UPSs), generators and other backup power solutions;
1.2.4 roles and responsibilities;
1.2.5 the general principles for financing the measures.
1.3 The document is not intended to ensure the uninterrupted operation of all systems. The purpose of this document is to ensure, on a risk basis, the safety of people, the continuity of critical services and the restoration of the university's core activities as quickly as possible in the event of disruptions or crises.
1.4 The document specifies how the university's Business Continuity Policy is implemented in the areas of technical systems and backup power. Other risks of service disruption, alternative ways of working, data backup and recovery, and the availability of staff and suppliers are addressed in the relevant continuity and incident response plans.

2. Scope of application

2.1 This document applies to the planning, development and management of measures to ensure the continuity of the university's buildings, technical systems, information systems, critical services and physical infrastructure, as well as the security of the supplies.
2.2 The document applies in particular to:
2.2.1 electrical power and backup power systems;
2.2.2 uninterruptible power supplies (UPSs) and generators;
2.2.3 server and communications rooms;
2.2.4 critical network and communications connections;
2.2.5 security, alarm and access control systems;
2.2.6 emergency notification and public address systems;
2.2.7 building automation systems;
2.2.8 specialised ventilation and cooling systems and other critical technical systems;
2.2.9 laboratories and research equipment;
2.2.10 critical teaching and research services;
2.2.11 premises and systems required to support sheltering and crisis response activities.
2.3 The document applies to all structural units of the university. The requirements applicable to partners, their responsibilities, service levels and arrangements for verifying compliance shall be set out in the relevant contracts. The need to amend existing contracts shall be assessed separately.

3. Definitions

3.1 '**Business continuity**' means the university's ability to continue its core activities or restore them following an incident or crisis.
3.2 '**Security of supply**' means, for the purposes of this document, the availability of electricity and related resources, including fuel, cooling and communications, to the extent required for the operation of critical services and systems.
3.3 '**Critical service or system**' means a service or system whose disruption could pose a risk to people, hinder crisis management or cause significant harm to the university's core activities, property, research materials or data.

3.4 '**Person responsible for a system**' means a person designated by the head of a structural unit to describe the operational need for the system and the impact of its disruption and to ensure that the requirements for the system are kept up to date. The technical administrator is responsible for the agreed technical management tasks. The designation of a person responsible for a system does not relieve the head of the structural unit of his or her responsibility.
3.5 '**Maximum tolerable downtime**' means the longest period for which a required function of a system may be interrupted without breaching applicable requirements or exceeding the impact permitted under the risk assessment.
3.6 '**Autonomy time**' means the period during which a system can operate at a specified load using backup power and other necessary resources available on site, without replenishment. The operating time dependent on additional supplies shall be documented separately.
3.7 '**Controlled shutdown**' means a predetermined sequence of actions by which a system is brought to a safe state, preventing unacceptable harm to people or the environment or damage to equipment, samples or data.

4. General principles
4.1 The university applies a risk-based approach to ensuring business continuity and security of supply.
4.2 Continuity measures shall be planned in accordance with the following principles:
4.2.1 protecting human life and health is the priority;
4.2.2 the criticality of a system or service is assessed based on the impact of a disruption, the time required for recovery, potential damage and technical dependencies;
4.2.3 continuity measures must be technically and economically justified;
4.2.4 systems are provided with an uninterruptible power supply (UPS) and generator power according to their continuity needs and applicable requirements. Where backup power for a system is required by another legal instrument, that requirement must be met regardless of the continuity level assigned to the system;
4.2.5 backup power solutions are designed based on applicable mandatory requirements and a documented risk assessment;
4.2.6 the continuity of critical systems is considered as a whole, taking into account the interdependencies between related technical systems;
4.2.7 continuity solutions must be as standardised, manageable and testable as possible;
4.2.8 continuity measures must support the continuation of the university's core activities and their recovery as quickly as possible following an incident or crisis.
4.2.9 The assignment of a continuity level, the fact that the mapping has not been carried out, or the absence of a funding decision does not relieve the university of its obligation to comply with mandatory safety requirements or reduce any obligations arising from those requirements.

5. Continuity levels
5.1 The university applies a common safety baseline to each building or part of a building and determines whether systems and services require additional protection at level 1 or 2. The safety baseline is not an alternative to levels 1 and 2. It comprises mandatory safety requirements, essential safety functions required for the use of the building and the functions necessary to prevent significant damage to the building.
5.2 The continuity level is determined using a risk-based approach, taking into account the impact of a disruption, the maximum tolerable downtime, the required level of operation and technical dependencies. Where a system is subject only to the baseline safety requirements, this shall be recorded separately in the system inventory. Assignment to level 1 or 2 does not diminish the safety baseline requirements.

6. Safety baseline
6.1 A minimum level of safety shall be ensured in all buildings in active use to support their safe use and enable an effective response to a crisis. This includes evacuation, fire safety, emergency notification, essential access, minimum security and bringing the building to a safe state.
6.2 As a rule, the safety baseline covers the following:
6.2.1 fire safety and alarm systems;
6.2.2 evacuation and emergency lighting;
6.2.3 essential access control systems;
6.2.4 the minimum functionality required of surveillance and security systems;
6.2.5 emergency notification systems;

6.2.6 essential safety functions of building automation systems;
6.2.7 server and communications rooms forming part of the central IT infrastructure and their critical equipment;
6.2.8 critical communications and network equipment;
6.2.9 cooling required for the operation of server rooms, communications rooms and UPS rooms;
6.2.10 heating system functions necessary to prevent the building from freezing and suffering resulting damage;
6.2.11 electrical distribution components required for the operation of baseline systems;
6.2.12 other technical systems essential to the operation of baseline systems.
6.3 Backup power for baseline systems shall be provided through compliant and standardised solutions, taking into account applicable legislation, including fire safety requirements, and the technical requirements of the systems. Where the existing infrastructure of a building does not permit the required backup power to be provided, the necessary technical modifications shall be planned and implemented, and the temporary safety measures required until their implementation shall be specified.
6.4 The safety baseline requirements and compliance with them shall be documented for each building or part of a building, specifying the maximum tolerable downtime and required operating time for each relevant system.

7. Level 1 – critical and essential systems and services
7.1 Level 1 covers systems and services that must continue to operate during a disruption because their interruption could:
7.1.1 pose a risk to people's lives or health;
7.1.2 hinder the organisation of incident or crisis response;
7.1.3 interrupt the operation of the university's critical services;
7.1.4 cause significant or irreversible damage to property, research or data;
7.1.5 cause a significant interruption to work, place a substantial burden on recovery efforts or disrupt the university's teaching and research activities.
7.2 Level 1 may include:
7.2.1 research equipment of significant or critical importance;
7.2.2 irreplaceable or exceptionally valuable research samples and materials, as well as critical experiments and data;
7.2.3 systems whose continued operation is necessary to prevent more extensive damage.
7.3 Level 1 systems shall be capable of operating for at least 24 hours from the start of a power outage, covering the designated critical loads, using a generator or an equivalent backup power solution and taking into account the maximum tolerable downtime assigned to the system.
7.4 A UPS shall be used where a system cannot tolerate the interruption caused by switching to generator power or requires an uninterrupted power supply for a safe shutdown.
7.5 The assessment of the ability to operate for at least 24 hours shall take into account the critical load, the energy requirements of the system and its supporting systems, the actual capacity of the backup power solution and the adequacy of the necessary resources.
7.6 The assessment shall determine the autonomy time achievable with the resources available on site. Where the required operating capability depends on additional supplies of fuel or other resources, the need for such supplies and the arrangements for securing them shall be documented. The need for the ability to operate for at least 72 hours and the options for ensuring it shall also be assessed.

8. Level 2 – systems requiring a controlled shutdown
8.1 Level 2 covers systems and equipment that do not require a long-term backup power supply, but require protection against power fluctuations and brief power outages or a controlled shutdown to prevent damage, data loss or unstable operation.
8.2 Level 2 may include:
8.2.1 sensitive laboratory and measuring equipment;
8.2.2 audiovisual and presentation equipment;
8.2.3 local IT equipment;
8.2.4 equipment used for experiments;
8.2.5 research equipment that requires a safe shutdown;
8.2.6 other sensitive equipment and systems.

8.3 Level 2 systems shall be supplied with UPS power through the building's central UPS system, taking into account the protection needs of the equipment, the power capacity required and the operating time needed for a safe shutdown.
8.4 A local UPS may be used only as a justified exception where the use of the central UPS system is not technically feasible or the technical requirements of the equipment call for a separate solution. The exceptions shall be approved by the Real Estate Office.
8.5 For level 2 systems, the conditions for a controlled shutdown, the person responsible for the shutdown and his or her substitute, and the time required to carry it out shall be specified. Where an automatic shutdown is not possible, the person responsible or his or her substitute shall be available within the required time in accordance with the response arrangements set out in clause 13.5.

9. Principles for identifying critical systems and planning backup power solutions
9.1 Critical systems shall be identified and documented based on the impact of a service disruption, and the equipment, premises, data and personnel required for the operation of the service, as well as its technical dependencies. The price or type of equipment alone does not determine its continuity level.
9.2 UPS, generator and other backup power solutions shall be designed and arrangements for their management agreed between the unit responsible for the system, the Real Estate Office and the Information Technology Services, according to their respective areas of responsibility. Solutions affecting electrical infrastructure or conditions in the premises shall be approved by the Real Estate Office, and those affecting IT or communications infrastructure shall be approved by the Information Technology Services.
9.3 UPS solutions shall be designed as centralised, standardised systems, taking into account the needs of all continuity levels and the required capacity reserve. A local UPS may be used only as a justified exception where the use of the central UPS system is not technically feasible or the technical requirements of the equipment call for a separate solution. Exceptions shall be agreed with the Real Estate Office.
9.4 The person responsible for the system shall describe its continuity needs and the impact of a disruption. Based on this information, the system shall be assessed in cooperation with the relevant persons responsible for technical matters against the criteria for the continuity levels set out in this document. The required continuity level shall be approved by the Real Estate Office.
9.5 Where the required capability has not yet been established, the shortfall, temporary measures, the person responsible for addressing the shortfall and the deadline for doing so shall be recorded in the register of critical systems and loads. A temporary deviation shall be accepted by the manager responsible for the relevant area, unless otherwise provided in other university regulations. Non-compliance with a mandatory safety requirement cannot be accepted; where necessary, the use of the system or premises shall be restricted.
9.6 When planning backup power solutions, the following shall be taken into account:
9.6.1 the capacity to maintain and test the solutions;
9.6.2 the availability of monitoring and alerting capabilities;
9.6.3 technical compatibility;
9.6.4 the capacity of the electrical and other technical systems;
9.6.5 the principles governing responsibility and funding;
9.6.6 ensuring the reliability and continuity of backup power for critical systems, including during maintenance of the backup power solution or in the event of the failure of an individual component;
9.6.7 the impact of noise and exhaust emissions from generators on the building and its occupants.
9.7 The purpose of UPS systems is to:
9.7.1 protect systems against power fluctuations and brief power outages;
9.7.2 keep systems operating until the generator starts;
9.7.3 enable a controlled shutdown of systems.
9.8 Generator power is used to ensure the continuity of designated critical systems and services during prolonged power outages. Generator power is also used as a backup power supply for technical systems with high power demands where connecting them to a UPS or providing the required backup time through a UPS is not technically or economically feasible. Such systems include sprinkler pumps, firefighting lifts, heating substations, large cooling units and smoke extraction ventilation systems.
9.9 The generator solution shall be selected based on the criticality of the system, the level of risk, technical feasibility and cost. Backup power may be provided by:
9.9.1 a fixed generator;

9.9.2 a mobile generator that can be made available and brought into operation within the system's maximum tolerable downtime. Where a generator is shared, priorities for its use shall be established, taking into account the possibility that buildings may need it at the same time;
9.9.3 another technically justified backup power solution.
9.10 When planning backup power solutions for critical systems, reliance on a single power source or component whose failure or maintenance could interrupt the operation of a system shall be avoided. Where necessary, power shall be provided to critical systems through independent or redundant backup power solutions.

10. Assessment of continuity needs
10.1 When planning a new laboratory, system, device or item of research equipment, the structural unit shall obtain the approval of the Real Estate Office for the proposed solution before finalising the technical specifications, initiating a procurement procedure or entering into any other binding commitment.
10.2 As part of the approval process, the continuity needs and technical requirements of the proposed solution, the adequacy of the existing infrastructure and the life-cycle costs of the solution shall be assessed. Compliance with the agreed requirements shall be verified before the solution is brought into use.
10.3 The following shall be involved in assessing continuity needs, according to their respective areas of responsibility:
10.3.1 the structural unit responsible for the system or equipment, which shall describe the operational need and the impact of a disruption;
10.3.2 the Information Technology Services, where IT or communications infrastructure is affected;
10.3.3 other relevant parties, depending on the nature of the solution and the safety and funding issues involved.
10.4 The assessment shall determine, among other things:
10.4.1 the continuity level of the system or equipment;
10.4.2 the potential impact of a disruption;
10.4.3 the need for UPS protection, a controlled shutdown or generator power;
10.4.4 the capacity of the existing electrical and technical infrastructure and the impact of the proposed solution on it;
10.4.5 the availability of the premises, utilities and technical conditions required to establish the backup power solution, such as space for installing the UPS and batteries, space for switchgear, cooling, ventilation and possibilities for installing cable routes;
10.4.6 maintenance, monitoring and testing needs;
10.4.7 the principles governing the funding of the solution and responsibility for it.

11. Roles and responsibilities
11.1 The organisation of business continuity and security of supply at the university is based on role-specific responsibilities.
11.2 The area director shall organise continuity planning and the consideration of resource needs in his or her area and decide on priorities within the scope of his or her authority.
11.3 The head of a structural unit shall designate persons responsible for systems and arrange for the continuity needs of their unit to be documented and the necessary measures to be implemented.
11.4 Within its area of technical responsibility, the Information Technology Services is responsible for:
11.4.1 the continuity of critical IT, communications and network systems;
11.4.2 assessing the technical criticality and dependencies of the IT infrastructure in cooperation with the units responsible for the services;
11.4.3 defining the technical requirements for UPS systems and backup power solutions for IT systems and agreeing on management responsibilities with the Real Estate Office;
11.4.4 ensuring that monitoring and alerts for IT systems function properly;
11.4.5 coordinating, through the Business Continuity Division, the implementation of the Principles for Ensuring the Continuity of Critical Services and Technical Systems at Tallinn University of Technology, and developing and updating a common methodology.
11.5 The Real Estate Office is responsible for:
11.5.1 ensuring the continuity of the technical systems of buildings;
11.5.2 planning and managing generators, electrical infrastructure and building automation systems;
11.5.3 organising technical maintenance, testing and operation;

11.5.4 ensuring the minimum level of safety in buildings;
11.5.5 approving the required continuity level;
11.5.6 arranging the technical review and approval of new laboratories, systems and equipment that affect a building's technical infrastructure or conditions in its premises.
11.6 For each shared solution, the Real Estate Office and the Information Technology Services shall document the division of management responsibilities, including responsibility for the UPS, batteries, generator, electrical connections, cooling and monitoring. Persons competent in the relevant fields shall be involved in matters concerning fire safety and occupational safety.
11.7 Heads of structural units and the persons they designate as responsible for systems are responsible for:
11.7.1 assessing the criticality of the systems, equipment, laboratories and research equipment in their areas of responsibility;
11.7.2 assessing the continuity needs of systems and equipment required for the safe operation of work processes, and determining and implementing the necessary measures in cooperation with the relevant persons responsible for technical matters, in accordance with the university's Occupational Health and Safety Management Regulations;
11.7.3 describing the continuity needs, potential impacts of disruptions and required operational capability of the systems and services in their areas of responsibility, and providing and keeping up to date the information needed for this purpose;
11.7.4 arranging the proper maintenance, regular inspection of equipment and systems serving premises within their areas of responsibility, and keeping them in good working order, in accordance with the documented division of management responsibilities. Management of a building's central technical systems shall be carried out by the Real Estate Office in accordance with its area of responsibility.
11.7.5 arranging for plans for new laboratories, systems, equipment and research equipment to be submitted to the Real Estate Office for approval in good time, in accordance with clause 10.
11.8 The Real Estate Office is responsible for the technical planning and approval of continuity solutions that affect a building's technical infrastructure or conditions in its premises, involving the Information Technology Services and the relevant structural unit as necessary.

12. Funding principles

12.1 Funding for the following continuity measures shall be included in the university's budget and budget strategy by the structural unit responsible for the relevant service or infrastructure, in accordance with the university's Financial Regulations and Rules for the Use of Assets:
12.1.1 continuity measures required to meet the safety baseline;
12.1.2 the university's central critical safety, security, communications and IT systems;
12.1.3 central technical systems and infrastructure;
12.1.4 university-wide continuity solutions.
12.2 The costs of providing additional continuity protection for equipment, a laboratory or research equipment specific to a structural unit shall generally be planned in the budget of the unit or project concerned, based on a substantiated need and the conditions governing the use of the funding source. Funding decisions shall be made in accordance with the university's budgeting and decision-making procedures.
12.3 For a solution serving multiple units or financed jointly, the allocation of investment and ongoing costs, the funding sources and the person responsible for managing the solution shall be determined in writing before any commitments are made. The allocation of costs shall take into account the use of the solution and the substantiated needs of the units.
12.4 Continuity measures and investments shall be prioritised based on the continuity levels assigned to systems and the deficiencies identified.
12.5 When a funding request is submitted, the full life-cycle costs of the solution shall be taken into account, including design, installation, adaptation of premises and technical systems, maintenance, testing, monitoring, battery replacement, fuel, training and decommissioning.
12.6 The unit responsible for the system shall submit a substantiated statement of need, a cost estimate and a schedule. The Real Estate Office and the Information Technology Services shall identify and consolidate the needs relating to their respective infrastructure. The Finance Office shall be involved in matters concerning budgeting and funding sources in accordance with the Financial Regulations.

12.7 Where funding for the necessary measures is not available, a funding request, together with a proposed solution and temporary measures, shall be submitted to the person authorised to make the decision.
12.8 Technical approval and the assignment of a continuity level do not replace a funding decision. Likewise, the availability of funding or a funding decision does not replace the required technical approval.

13. Maintenance, testing and response to disruptions

13.1 Regular maintenance, testing and technical inspection of UPS systems, generators and other continuity solutions shall be documented and organised in accordance with applicable requirements, manufacturers' instructions and system-specific maintenance and testing plans.
13.2 To ensure the continuity of critical systems, the technical administrator shall, in accordance with the documented division of management responsibilities, arrange regular checks of:
13.2.1 the operational capability of UPS systems;
13.2.2 the condition of batteries;
13.2.3 the ability of generators to start;
13.2.4 the operation of monitoring and alerting systems;
13.2.5 the ability to restore critical systems.
13.3 The functioning of critical systems shall be checked in accordance with a risk-based testing and exercise plan. The plan shall specify the frequency and scope of the checks, the persons responsible, the safety measures and the criteria for evaluating the results. In addition to individual items of equipment, the checks shall cover the service delivery chain, including the UPS, generator, transfer to backup power, cooling, communications, alerts and recovery. The results, deficiencies, improvement measures, persons responsible and deadlines shall be documented.
13.4 Disruptions shall be addressed and operations restored in accordance with the university's Business Continuity Policy and the relevant incident response and crisis plans.
13.5 The instructions for each system shall specify the procedures for reporting a disruption, switching to backup power, carrying out a controlled shutdown and restarting the system. The availability of responsible persons shall be ensured in accordance with agreed arrangements for responding during working hours, while on call or under a contract, including outside working hours and during a power or communications outage.
13.6 Before a system is restarted, the technical administrator shall check that the system and its supporting systems are ready for operation. Where the use of a system or premises has been suspended because of a hazard, use may resume once the hazard has been eliminated and a competent person in the relevant area of safety has given his or her approval.

14. Implementing provisions and annexes

14.1 This document shall be applied together with the documents governing the organisation of business continuity, crisis management, real estate management, information security and information technology services at the university.
14.2 For the implementation of this document, at least the following shall be prepared and kept up to date:
14.2.1 system-specific operating, shutdown and restoration instructions;
14.2.2 the necessary checklists and test results;
14.2.3 documented risk assessments and the information on which they are based;
14.2.4 the register of critical systems and loads, in accordance with Annex 1;
14.2.5 maintenance and testing plans.
14.3 The Business Continuity Division of the Information Technology Services shall arrange for this document to be reviewed at least once a year and whenever significant changes occur. The document shall be updated as necessary, and amendments shall be approved in accordance with the university's applicable procedures.
14.4 Annex 1 forms an integral part of these Principles.
14.5 An action plan does not alter the required level assigned to a system. Breaches of mandatory requirements shall be addressed without delay; other measures shall be implemented in accordance with the approved action plan.
14.6 The Real Estate Office shall, in cooperation with the Information Technology Services and the relevant structural units, arrange the initial assessment provided for in Annex 1 and enter its results in the register of critical systems and loads no later than 31 December 2028.

14.7 Based on the initial assessment, the Real Estate Office shall, in cooperation with the Information Technology Services and the relevant structural units, prepare an action plan to address the deficiencies and submit it to the Director for Administration for approval no later than 31 December 2029. The action plan shall specify the measures, the persons responsible, implementation deadlines and funding needs.
14.8 The Real Estate Office shall, in cooperation with the Information Technology Services and the relevant structural units, submit to the Director for Administration at least once a year an overview of the implementation of the action plan and any unresolved deficiencies, together with proposals for amending the action plan where necessary.

Annex 1 Procedure for mapping critical systems and loads

1. The Real Estate Office shall coordinate the mapping of business continuity needs for critical technical systems, equipment and rooms in each building, in cooperation with the technical staff responsible in the Information Technology Services and the relevant structural units.

2. The purpose of the mapping is to:

2.1 identify the building's critical systems and loads;
2.2 assess their business continuity needs in the event of a power outage or other crisis;
2.3 determine the applicable baseline requirements and any additional continuity level required;
2.4 select the necessary backup power solution (a UPS, generator or other solution);
2.5 plan the required investments and assign responsibilities.

3. Assessment of buildings

3.1 Each building shall be mapped separately.
3.2 The assessment shall consider at least the following:
3.2.1 systems essential for building safety and crisis preparedness;
3.2.2 critical equipment and services associated with the use of the building, the disruption of which would cause significant harm;
3.2.3 equipment that requires only protection against power fluctuations or a controlled shutdown.

4. Identifying critical loads and determining the required level of business continuity

4.1 A list of critical loads shall be drawn up for each building.
4.2 The list shall include all critical loads identified in the building and the systems required to ensure safety functions, including the following, where installed:
4.2.1 fire safety and alarm systems;
4.2.2 evacuation and emergency lighting;
4.2.3 access control and security systems;
4.2.4 emergency notification systems;
4.2.5 essential safety functions of building automation systems;
4.2.6 server and communications rooms;
4.2.7 cooling, ventilation and heating systems;
4.2.8 laboratories and research equipment;
4.2.9 equipment requiring a controlled shutdown.
4.3 For each load, the applicable baseline requirements shall be documented and, where additional protection is required, level 1 or 2 shall be specified. If no additional level is required, "baseline only" shall be recorded. The required level and the capacity currently available shall be recorded separately.
4.4 The continuity requirements of each critical load shall then be assessed and an appropriate backup power solution selected. For this purpose, at least the following shall be documented:
4.4.1 location;
4.4.2 person responsible;
4.4.3 power demand and, where necessary, starting load;
4.4.4 maximum tolerable downtime
4.4.5 dependencies on other systems;
4.4.6 proposed backup power solution;
4.4.7 minimum required service level and order of restoration;
4.4.8 shutdown conditions and duration, and availability of the person responsible for responding;
4.4.9 the operating time achievable using on-site resources, as well as the resources needed to maintain operation where it depends on an external supply or service, their availability, delivery and implementation times, and arrangements for maintaining operation in the event of a large-scale outage.
4.5 When selecting a backup power solution, the following shall be assessed in particular:
4.5.1 the required UPS runtime;
4.5.2 the need for a controlled shutdown;
4.5.3 the loads to be supplied by a generator;
4.5.4 the required autonomy time;
4.5.5 the suitability of a shared or building-specific generator solution.
4.6 Actual measurement data shall be used where possible. For a shared solution, simultaneous loads, spare capacity and the impact of a failure affecting multiple systems shall be assessed. A shared solution shall be selected if its reliability and risk mitigation measures enable it to meet the requirements of the systems concerned.

5. Documentation of the mapping results

5.1 The mapping results shall be documented in a central register of critical systems and loads, using the university's register of premises or another information system designated for this purpose. Access to technical diagrams, information on vulnerabilities and contact details shall be granted on the basis of the need arising from work duties and in accordance with the university's information security and information management requirements.

5.2 The register shall contain the results of the assessment of the continuity requirements of critical systems and the required improvement measures. The detailed structure and data fields of the register shall be determined as part of the organisation of work.

5.3 The information in the register shall be checked to ensure that it is up to date at least once a year and after any significant change, incident or test that affects the recorded capability. The unit responsible for a system shall ensure that the information on its operational needs and criticality is kept up to date. The Real Estate Office and the Information Technology Services shall keep the technical information on the infrastructure they manage up to date.