Approved by order No 65 of 20 March 2025 of the Director for Administration

In force from: 20.03.2025

Change Management Rules

1. General

1.1. The aim of the change management process is to ensure that changes to information systems and other IT assets are implemented in a planned and controlled manner. An efficiently controlled change management process ensures that all changes are properly documented, reviewed and the parties involved are informed. It also enables the identification and mitigation of potential risks, minimising errors related to changes and ensuring the organisation's smooth and efficient operation.

1.2. The Change Management Rules apply to all university information systems and IT assets, ensuring their reliability, security, and sustainability. The Rules are generally aligned with the principles and terminology of the Information Technology Infrastructure Library (ITIL), ensuring adherence to international best practices in change management.

2. Types of changes

2.1. An operational task or routine task is a repetitive activity related to IT services that does not impact the operation of information systems or services and does not require completion of the change management process. Such activities may include, for example, installing a workstation for a user or applying standard firewall rules based on approved procedures. Since operational tasks or routine tasks do not impact service availability or end-user experience, they are not recorded as changes.

2.2. A standard change is a pre-approved, low-risk and frequently implemented change that follows a pre-defined and tested procedure. Since a standard change has minimal impact on an information system or service, it does not require separate approval, but its recording is mandatory. Examples include routine software updates, the impact of which has been tested and is known. A normal change is a change that is neither a standard nor an emergency change and requires evaluation and approval prior to implementation. A normal change can have a moderate to high impact on an information system, which is why its risk level is assessed during the change management process. For example, this could involve the implementation of a new software module, changes to server or network configurations affecting multiple systems, or system upgrades that have a significant impact on users.

2.3. An emergency change is an urgent change required to address a critical incident or mitigate a significant risk, the failure of which could lead to major disruptions in the operation of the university's information systems or services. Such changes include, for example, the immediate deployment of a critical security patch or system recovery following a technical failure or security breach.

3. Change management process

3.1. Normal changes

3.1.1. Creating and submitting a normal change request ticket

3.1.1.1. A normal change management process is initiated by an employee of the university's Information Technology Services or an owner of the IT asset, who shall submit a request for change (RFC) via the Help Center (JIRA work management solution). A request must be submitted at least three business days before the change is implemented to allow adequate time for assessment and approval.

3.1.1.2. A request for normal change must include the following information:

3.1.1.2.1. A description of the change, its priority, impact and risk assessment - what will be changed and why is it necessary? What is the criticality rating (e.g. critical, high, medium) of the change, and how will it affect information systems, services and users? How will the change help improve services, security, or work processes? What are the potential risks, and how will they be mitigated?

3.1.1.2.2. Implementation, rollback and testing plan – how will the change be implemented? What are the steps, schedule, and resources required? What is the rollback plan if the change needs to be reversed? How will the change be tested, and how will its success be evaluated?
3.1.1.3. Testing and validation – how has the change been tested and how will its success be evaluated?

3.1.2. Approving a request for normal change

3.1.2.1. The initiator of a normal change prepares a request for change and submits it to the owner of the IT asset for approval. The asset owner is responsible for evaluating the impact of the change to ensure it complies with the organisation's technical, business, and information security requirements and does not cause unexpected risks.
3.1.2.2. If a change significantly impacts information systems, services, or users, the asset owner may involve additional stakeholders to ensure compatibility with all related systems and processes.

3.1.3. Reviewing a request for a normal change, preparing and approving a schedule

3.1.3.1. One a request for a normal change is submitted and approved by the asset owner, it will be forwarded to the change manager for review. The change manager (Head of the IT Helpdesk Division) verifies that the request meets the process requirements, is properly formatted, all necessary approvals have been obtained, and a risk assessment has been completed.
3.1.3.2. If the request is incomplete or missing critical information, it will be returned to the change initiator for revision. The change manager is not responsible for the substantive accuracy or technology rationale of the change but ensures that the requirements for the change management process are met, and all necessary information is provided. The change initiator and asset owner are responsible for the substantial accuracy, necessity, and technical feasibility of the change. They must ensure that all technical and commercial aspects have been well considered before submitting the request.
3.1.3.3. If a normal change meets all requirements, it is added to the change schedule in JIRA. The change manager is also responsible for scheduling changes to prevent the overlap of major changes and avoid system overload.
3.1.3.4. The change implementer and asset owner are responsible for planning and preparing the change implementation process in accordance with the approved schedule. Preparation involves allocating necessary resources, assigning tasks, testing, and planning the technical implementation to ensure a smooth and successful implementation process.

3.1.4. Notifying of a change

3.1.4.1 The change manager (Head of the IT Helpdesk Division) is responsible for notifying of normal changes, ensuring that all affected parties receive timely and adequate information about the impact and schedule of the changes. Notification will be sent through designated communication channels. The extent and level of detail of the notification is determined by the complexity and impact of the normal change. The change manager selects the most effective notification method to ensure clear communication and preparedness of all involved parties.

3.1.5. Implementing a normal change and rolling back

3.1.5.1. A normal change is implemented following a previously approved implementation plan that outlines the schedule, activities, and responsible parties involved in the process. A normal change should be scheduled to minimise its impact on information systems, services, and users, ensuring as seamless transition as possible.
3.1.5.2. The change implementer is responsible for executing a normal change, ensuring that all activities are performed according to the implementation plan and schedule. During implementation, the system status should be monitored in real time, progress must be documented, and automated monitoring solutions should be used, when possible, to quickly detect any deviations. After implementing a change, the change implementer must monitor system and IT asset performance to ensure stability and promptly address any problems that arise.
3.1.5.3. If a normal change causes unexpected problems or does not produce the desired result, a pre-defined and tested rollback plan is implemented. The rollback criteria must be defined in the request for change and its execution is considered based on the system's status and business requirements. The decision to initiate a rollback is made by the change implementer, based on the criteria outlined in the request for change. If a change impacts critical systems or if there is

uncertainty about the need for a rollback, the change implementer must consult with the asset owner.

3.1.5.4. All activities associated with the implementation of a normal change and rollback shall be documented and, if necessary, escalated to the relevant parties. Affected parties shall be informed of the status of the change and any potential deviations to ensure clear communication and quick resolution of any potential problems.

3.1.6. Declaring a change successful and closing it

3.1.6.1. A normal change is considered successful if it has been implemented according to the approved implementation plan and the information systems and IT assets are functioning as expected. If the change implementer is certain that the change was successful, the normal change ticket is marked as completed, and an automatic notification is sent to the involved parties, confirming the successful completion of the change.

3.1.6.2. For normal changes with high impact, an additional evaluation period may be implemented before final closure, during which the stability of the system is monitored to ensure that the change has achieved the desired result without any unexpected side effects. At the end of the evaluation period, an additional review shall be conducted, if necessary, and the final impact of the change, along with the results achieved, shall be documented.

3.1.6.3. If a normal change fails to produce the desired result or causes unexpected problems, and a rollback plan has been implemented, the normal change ticket will remain open. In this case, further analysis shall be conducted to identify the cause of the problem and to plan a new change based on the findings.

3.2. Standard and emergency changes

3.2.1. Standard changes

3.2.1.1. Standard changes are pre-approved, low-risk and repeated changes for which a task or work order has already been defined in a JIRA project related to an IT asset. Since the details of the change and the required activities are outlined in the task description, no separate documentation on the change is created. The initiator of a standard change fills in the required change-related fields in the JIRA ticket, ensuring that the change is recorded and visible in the change calendar, thus enabling better planning and traceability without excessive administrative burden.

3.2.1.2. The change implementer is responsible for implementing the change and documenting it in a JIRA task, ensuring that the procedures and key details are accurately recorded after implementation. Related documentation shall also be updated, as necessary. If a standard change fails or unexpected problems occur, the situation is evaluated, and if needed, the change is escalated to an incident.

3.2.2. Emergency changes

3.2.2.1. Emergency changes are carried out in response to critical incidents and are typically linked to an existing incident ticket in JIRA. Once a change is implemented, the change implementer or incident resolver records the details in the same ticket, outlining what was changed and the method used for implementation. If needed, the documentation for related systems is updated to ensure the change can be easily found and tracked later, without the need for a separate change ticket.

3.2.2.2. If an emergency change was initiated due to a system failure or security risk, the change manager or asset owner may initiate a follow-up analysis to determine how similar incidents can be prevented in the future.

4. Roles and responsibilities

Role	Responsibilities and liability
Change initiator	Prepares a request for normal change in JIRA, detailing the purpose, impact, and risk assessment of the change, and submits it to the asset owner for approval. Ensures that a request is properly formatted and includes all required information.
Owner of the information system or IT asset	Assesses the effects of a normal change on business, technical, user experience, performance, and information security aspects. Verifies that the change meets the organisation's requirements and, if needed, involves other relevant parties.
Change manager (Head of the IT Helpdesk Division)	Verifies that the request for normal change complies with process requirements and that all necessary approvals have been obtained. Adds the change to the schedule in the JIRA work management solution, coordinates scheduling, and notifies the relevant parties. Ensures ongoing monitoring and continuous improvement of the change process.
Change implementer	Implements a normal change according to the approved implementation plan and schedule. Monitors the system status, tracks the progress of the change implementation, and uses monitoring tools as needed. If needed, initiates a rollback plan and updates the documentation.

5. Supervision

The change manager carries out consistent supervision of the change management process, ensuring continuous monitoring and improvement. The change manager regularly assesses the effectiveness of the change management process and ensures its alignment with the organisation’s needs.

ANNEX 1 Examples of types of changes

1. **An operational task or routine task** is a repetitive activity related to IT services that has no impact on the operation of information systems or services and does not require the completion of the change management process. These tasks follow pre-approved procedures and are an integral part of standard IT administration and user support.
   1.1. Examples of operational or routine tasks:
      1.1.1. Installing a user's workstation with standard software.
      1.1.2. Applying standard firewall rules.
      1.1.3. Updating printer drivers on workstations by the Helpdesk.
      1.1.4. Resetting the email account password upon a user's request.
      1.1.5. Daily monitoring and management of backups.
      1.1.6. Conducting regular log analyses and monitoring.
      1.1.7. Creating a new user account and assigning standard permissions in AD or another identity management system.
2. **A standard change** is a pre-approved, low-risk and frequently implemented change that follows a pre-defined and tested procedure. Since a standard change has minimal impact on an information system or service, it does not require separate approval, but its recording is mandatory. A standard change is recorded and managed in JIRA, where the change initiator fills in the required change-related fields. This ensures proper planning and traceability in the change calendar.
   2.1. Examples of standard changes:
      2.1.1. Routine software updates with a tested and known impact (e.g., Windows security patches, Office 365 updates).
      2.1.2. Renewing standard service certificates (e.g., renewing a TLS certificate for a web server).
      2.1.3. Archiving and clearing logs in accordance with the retention policy.
3. **A normal change** is a change that is neither a standard nor an emergency change and requires evaluation and approval prior to implementation. A normal change can impact the operation of systems and services, which is why its risk level is assessed during the change management process. A change is recorded in JIRA, where it is reviewed, approved, and scheduled.
   3.1. Examples of normal changes:
      3.1.1. Implementing a new software module in a business-critical system (e.g., adding a new functionality).
      3.1.2. Modifying a server or network configuration that impacts multiple systems.
      3.1.3. System upgrades that significantly impact users (e.g., an ERP system upgrade).
      3.1.4. Integrating a new system or service into the existing IT infrastructure.
      3.1.5. Reconfiguring services to optimise resource usage (e.g. improving database performance).
      3.1.6. Migrating cloud services (e.g., moving a database to AWS or Azure).
4. **An emergency change** is an urgent change required to address a critical incident or mitigate a significant risk. The failure to resolve an incident can lead to major disruptions in the operation of the university’s information systems or services. Since emergency changes are implemented as a quick response, they are typically recorded as an incident ticket in JIRA.
   4.1. Examples of emergency changes:
      4.1.1. Deploying promptly a critical security patch (e.g., in addressing a newly discovered zero-day vulnerability).
      4.1.2. Restoring a system following a major technical failure (e.g., recovering a corrupted database).
      4.1.3. Quickly replacing a server when a critical hardware component unexpectedly fails.
      4.1.4. Quickly implementing firewall rules to mitigate a network or ransomware attack.
      4.1.5. Temporarily blocking users’ access to a system due to security threats.