Approved by order No 108 of 2 May 2024 of the Director for Administration

In force from: 2.05.2024

Management of requests, incidents, events and problems

Table of Contents

1 General provisions

The purpose of the process for managing requests, events, and incidents (hereafter referred to as 'the process') is to deliver services to users under agreed conditions and resolve any errors that arise as soon as possible.
The process includes activities such as defining, recording, diagnosing, resolving, and closing requests, incidents, and events to ensure a swift and high-quality resolution process.

2 Request types

"**Request**" means any enquiry, request for advice, order, notification that has not been previously categorised by type.
"**Requester**" means a user, member of the university staff, a partner or any other person who uses the university's services or information systems.
"**Event**" means any notification of service component failure or alert detected by the monitoring system that can compromise data confidentiality, integrity, or availability. Events trigger requests.
The types of requests are as follows:

- **Incident** – an unexpected event that impairs or reduces the quality of service or causes a service disruption, which results in or creates a significant risk of compromising the availability, integrity and/or confidentiality of data and/or other assets.
    - **Cybersecurity incident (cyber incident)** – a special type of incident related to a successful or unsuccessful attempt or attack to destroy, alter, disable, steal or gain unauthorized access to or make unauthorized use of an IT asset.
    - **Data breach** – a special type of incident involving a breach of security, accidental or unlawful destruction, loss, alteration, unauthorised access to or disclosure of personal data transmitted, stored or otherwise processed.
    - **Presentation equipment incident** – a specific type of incident involving an unexpected malfunction or failure of presentation equipment.
- **Service request** – a request to obtain information, advice, access, a specific service, or a new resource.
    - **Procurement of IT Resources** – a service request form, the aim of which is to acquire suitable software or hardware components.
    - **Access rights** – a service request form intended to get access to an information system or any other IT asset.
    - **User account orders** – service request forms used to place orders related to user accounts.
    - **Computer and learning workstation** – service request forms for ordering various services related to computer workstations, including setup and support for computer labs, auditorium computers (operating systems, shared solutions, email and distribution lists, printers).
    - **Orders related to mobile and landline phones** – service request forms for ordering a range of services related to mobile and landline phones.
    - **Network and servers** – service request forms for ordering network setup and server-related services.
    - **Presentation equipment solutions** – a service request form for ordering various presentation equipment solutions for auditoriums and meeting rooms.
    - **AV technical services for events** – a service request form to order audio and video technical support (audio and video solutions) for events.
    - **IT development proposal** – a proposal for IT development work that can be made by any member of the university.

- **Problem** – the underlying cause of one or more incidents, service quality degradation, or the risk of future incidents and service quality degradation.
    - **Known bug** – a problem with an identified and documented cause, along with a temporary and/or permanent solution.

The response and resolution times of requests are the following:
Response time is the amount of time it takes to address a request, i.e. the time it takes for a Helpdesk employee to review a request, categorise and prioritise the request and designate an assignee.
Response times in various channels during working hours

- The response time for requests received via email or in JIRA is 180 minutes.
- The response time for requests received by phone is up to 5 minutes.

First response time is the amount of time it takes for an initial response to be provided after a request is made. First response time measures how long it takes for an agent (Helpdesk employee) to respond to a customer support request. First response time for all requests is up to 24 hours, i.e. up to three working days.
Resolution time is the time it takes to resolve a request or reply to an enquiry. The resolution time depends on the complexity and priority of the request.

3 Resolving requests

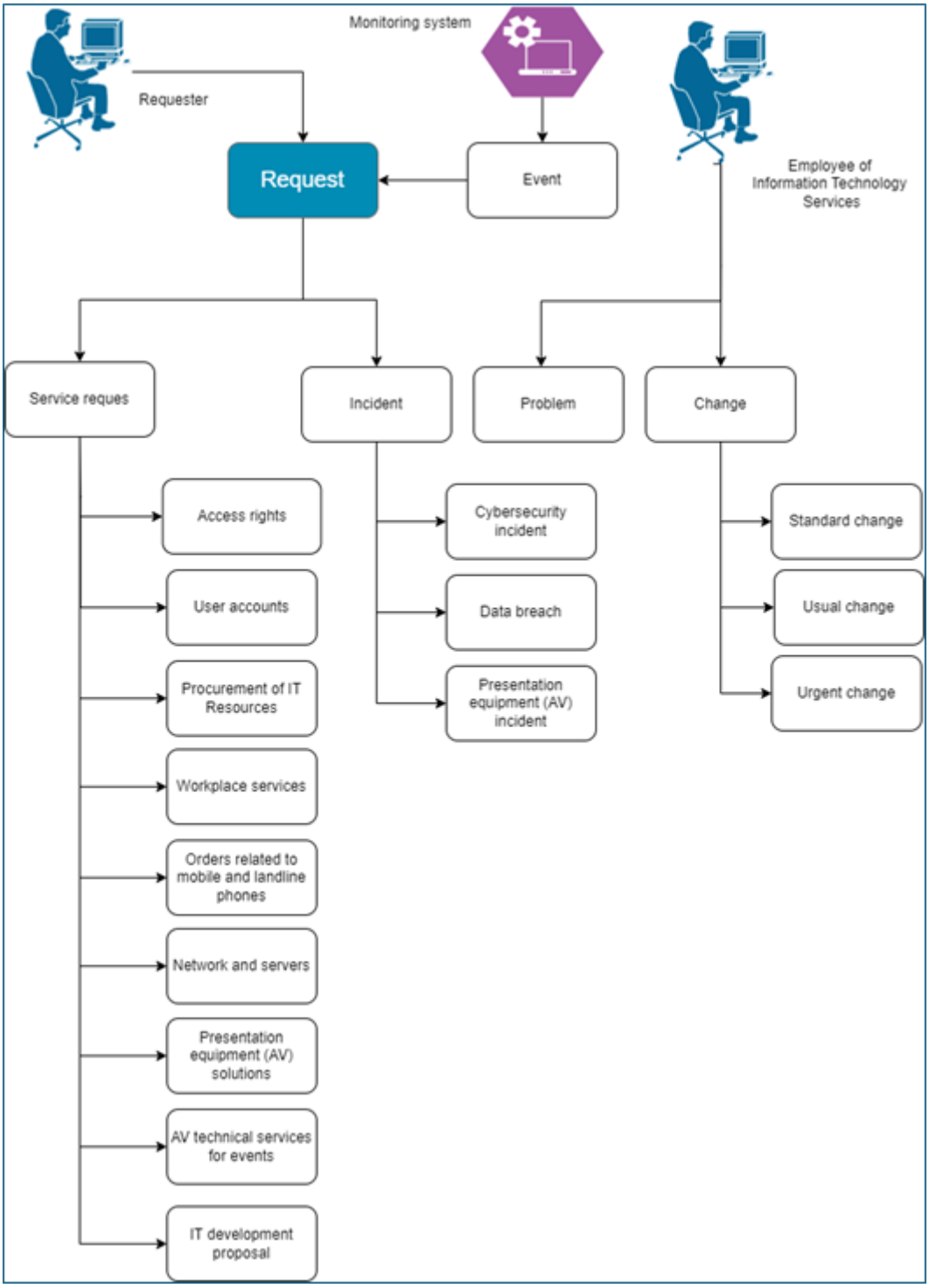

Figure 1 Resolving requests

3.1 Channels for submitting and recording requests

Users can submit their requests through the following channels: the JIRA support portal, email, phone, using the walk-in service. All user requests must be recorded in the Jira ticket management portal. Requests submitted through the JIRA support portal or via email to helpdesk@taltech.ee are automatically recorded. Requests submitted by phone or using the walk-in service shall be recorded by the Helpdesk specialist.

For any request, the person's name or username and the content of the request shall always be recorded in the JIRA ticket management system.
Events received through the monitoring system are also recorded as requests.

3.2 Responding to requests and providing a first response

The response time during working hours starts from the moment a request is registered. The response time for tickets registered outside working hours starts the following working day.
An IT Helpdesk employee shall respond to any registered request within 180 minutes during working hours and shall conduct **an initial analysis** and/or **error detection.** The Helpdesk employee shall categorise and prioritise the request and designate an assignee of the request.
During working hours, the Helpdesk specialist shall provide a first response to the requester regarding his/her request within 24 hours, i.e. three working days.

Table1 Prioritising requests

		Impact			
		More than 50 users affected	10 to 50 users affected	up to 10 users affected	1 user affected
Urgency	Critical	Critical	High	Medium	Medium
	High	High	Medium	Medium	Low
	Medium	Medium	Medium	Low	Low
	Low	Medium	Low	Low	Low

3.3 Resolving and closing a request

When possible, the Helpdesk resolves the request and if the Helpdesk cannot resolve it, the ticket will be forwarded to the appropriate person for resolution depending on the type and content of the request. In addition, the Helpdesk specialist shall conduct **initial analysis**, ask supplementary information from the user as needed, and provide the description of the fault identification before forwarding the ticket.
In cases where a partner resolves a request, the university's contact person who registered the ticket remains responsible for processing the request until it is closed.
Requests are resolved according to their priority level. Requests shall be resolved as quickly as possible. **All actions taken to resolve a request must be documented in the JIRA portal at the time they are performed** or as soon as possible thereafter, providing sufficient detail to facilitate understanding upon subsequent review.
The assignee shall mark a request as resolved in the tool immediately after it is resolved. For a request to be considered resolved, the requester's issue must be resolved, and this must be validated by a Helpdesk employee.
Once the request is resolved, the final resolution process shall be documented. If a resolved request has not been marked as resolved in the tool, the Head of the Helpdesk Division has the right to close the ticket.

4 Description of the incident management process

Incident coordinators are heads of the divisions of the IT Services Office who are responsible for ensuring effective resolution of high-priority and critical incidents and managing all related communications. The incident coordinators are as follows:

- Head of the IT Helpdesk Division (by default);
- Head of the IT Infrastructure Division;
- Head of the IT Development Division;

- Chief Information Security Officer (by default, in the case of information security incidents)
- Head of the IT Services Office.

4.1 Identifying an incident

- Identifying an incident in different roles
    - A user who identifies that an information system or other IT asset is not functioning as expected. The user shall notify the IT Helpdesk as soon as possible using various contact channels and, if possible, take appropriate measures to mitigate the damage caused by the incident or to prevent its impact from spreading.
    - A monitoring event that notifies the Helpdesk of a potential incident.
    - An employee of the IT Services Office who identifies that an information system or other IT asset is not functioning as expected. The employee of the IT Services Office shall notify his/her immediate superior and/or the IT Helpdesk of the incident as soon as possible.

4.2 Responding to and prioritising an incident

- **Scenario 1** – when a user detects an incident and reports it to the Helpdesk, or the Helpdesk employee detects an incident
    - Incidents detected and reported by a user as well as technical monitoring events are recorded by the IT Helpdesk.
    - Responding to an incident follows a process similar to resolving requests. First, the request is categorised as an incident, an assignee is designated, and the request is linked to a specific information system or IT asset.
    - The assignee conducts an initial analysis and error detection, requesting additional information from the user if necessary.
    - The assignee contacts the administrator of the relevant information system (or another related party) to verify the functioning of the solution.
    - Once the incident is confirmed, the assignee will prioritise the incident.
        - Low- to medium-priority incidents are assigned to a Helpdesk employee. If the Helpdesk can resolve the incident, it will not be forwarded, and the assignee will resolve the incident independently. The assignee shall inform the business project manager and superuser of the information system, or the owner of the relevant IT asset about the incident.
        - In the case of high-priority or critical incidents, the Head of the Helpdesk Division will be appointed as the coordinator (if the Head of the Helpdesk Division cannot respond, the incident will be assigned to the next coordinator in the list).
    - If multiple requests are received for the same incident, the Helpdesk employee will link them to the main incident ticket.
- **Scenario 2** – when an incident is detected by an employee of the IT Services Office:
    - The employee who detects an incident shall notify his/her immediate superior and/or the IT Helpdesk of the incident as soon as possible.
    - The immediate superior shall conduct an analysis in collaboration with the employee. The immediate superior contacts the system administrator (or another related party) to verify the functioning of the solution.
    - Once the incident is confirmed, the immediate superior will prioritise the incident.
        - If the priority is low to medium, it will be registered in the IT Helpdesk and forwarded to the person who can resolve it. The assignee shall inform the

business project manager and superuser of the information system, or the owner of the relevant IT asset about the incident.

- In the case of a high-priority or critical incident, the immediate superior will act as the coordinator. If the incident requires the immediate superior's direct involvement in the resolution process, coordination will be delegated to another available immediate superior (incident coordinator). The incident coordinator will record the incident in the Helpdesk system and notify the Helpdesk, the business project manager, the superuser of the information system, or the owner of the relevant IT asset about the incident.

- If multiple requests are received for the same incident, the Helpdesk employee will link them to the main incident ticket.

- **Scenario 3** – when an incident is detected by the head of a division or the Head of the IT Services Office.
  - The head shall conduct initial analysis.
  - The head contacts the system administrator (or another related party) to verify the functioning of the solution.
  - Once the incident is confirmed, the head will prioritise the incident.
    - If the priority is low to medium, it will be registered in the IT Helpdesk and forwarded to the person who can resolve it. The assignee shall inform the business project manager and superuser of the information system, or the owner of the relevant IT asset about the incident.
    - In the case of a high-priority or critical incident, the head will act as the incident coordinator. If the incident requires the head's direct involvement in the resolution process, coordination will be delegated to another available head (incident coordinator). The incident coordinator will record the incident in the Helpdesk system and notify the Helpdesk, the business project manager, the superuser of the information system, or the owner of the relevant IT asset about the incident.
  - If multiple requests are received for the same incident, the Helpdesk employee will link them to the main incident ticket.

Table2 Prioritising incidents

	More than 50 users affected	10 to 50 users affected	up to 10 users affected	1 user affected
Information system criticality – 3	Critical	High	Medium	Medium
Information system criticality – 2	High	Medium	Medium	Low
Information system criticality – 1	Medium	Medium	Low	Low
Information system criticality – 0	Medium	Low	Low	Low

Incident priority is the product of the following variables:

- Information system criticality (described in the JIRA service catalogue)
- The request scope is determined by the person who registers the request based on the information provided and the number of users affected.

If an incident has resulted in financial damage, it is classified at least as a **high** priority.
An information security incident is always classified at least as high priority. If an impact on the service(s) is identified, or if the assignee makes a corresponding decision after assessing the situation, the case is escalated to critical status.

4.3 Resolving an incident

- In the case of low- or medium-priority incidents the assignee , or in the case of high-priority or critical incidents, the incident coordinator will establish a common information flow with relevant parties to resolve the incident or inform them of the circumstances, using the appropriate communication channels.
- The assignee or coordinator of the incident shall ensure that all necessary parties are able to resolve the incident within the established resolution time.
- If necessary, the assignee or coordinator of the incident shall arrange notifications for affected users. The notification shall include information on the incident, its scope and the estimated time of resolution. As a rule, the notifications are sent by the IT Helpdesk Division.
- Notifications sent to users must be written in proper Estonian and English and include sufficient information about the incident's scope, instructions for next steps, and an estimated resolution time. The assignee or coordinator of the incident shall choose the appropriate communication channels based on the nature of the incident.
- In cases where the incident must be communicated to the wider public, the incident coordinator shall obtain approval of the Marketing and Communications Office, who will inform the public.
- In the event of an information security incident, the Chief Information Security Officer shall be notified, who will decide on the need for and extent of informing the partners.

Table 3 Incident resolution times

Priority level	Incident resolution time during working hours
Critical	4h
High	8h
Medium	24h
Low	48h

4.4 Closing an incident and follow-up

- An incident will be closed either when the ticket is resolved or when it cannot be resolved. When an incident is closed, the reason for closing shall be documented in the relevant ticket.
- The assignee of the incident shall prepare an incident report in Jira no later than 5 working days after the start of the incident.
- The Chief Information Security Officer reviews the incidents and their resolutions, providing recommendations for future improvements.
- For follow-up analysis, incidents recorded so far must be categorised as follows:
    - **human error (human risk)**, caused by persons, incl. theft and unauthorised activities (such as fraud, misdemeanour, breach of labour law, lack or loss of key staff, acts or omissions of the staff that may result in reputational damage if disclosed, actions taken by employees due to lack of knowledge (inadequate training);
    - **process error (process risk)**, caused by various deficiencies in processes, shortcomings in documentation and contracts, non-compliance with legislation, expiration of the university’s internal regulations;

- **system error (system risk)**, caused by issues related to IT or other systems, such as investment in or lack of investment in technology, shortcomings in development and implementation, inadequate capacity and volume accounting, system disruptions and outages, security and information security vulnerabilities;
- **external error (external risk)**, caused by external factors, such as criminal activity, external service providers, lawsuits, pandemics, disasters, infrastructure disruptions, political risk, surveillance, activity in foreign countries or cross-border provision of remote services, risks associated with the customers consuming the products and services, risks stemming from customer negligence or behaviour;
- **physical error (physical risk)**, caused by physical factors, such as physical hazards related to buildings and equipment, structural and environmental hazards (e.g. bars, fences), mechanical risks (such as locks and sprinklers), electronic systems (alarm and video surveillance systems), and procedural aspects (e.g. manned guarding).

5 Problem management

The purpose of problem management is to resolve issues related to information systems, minimizing the impact of incidents and problems on services, including:

- to implement measures to prevent incidents and problems;
- to implement measures to reduce the likelihood of recurring incidents;
- to minimize the impact of unavoidable incidents;
- to identify the root causes of incidents.

To prevent incidents and mitigate their impact, the business project manager of the information system or the owner of an IT asset shall proactively identify problems through service monitoring, continuous incident analysis, and risk assessment.
The problem management process is directed by the problem manager, who is responsible for ensuring its effectiveness and optimal functioning.

5.1 Defining a problem

When incidents with the same root cause are detected, the person who detected the incident creates a problem ticket in JIRA and assigns it to the IT project manager responsible for the information system. An incident record must not simply be reclassified as a problem, instead, a separate problem record should be created. A problem must be defined as clearly as possible, providing a detailed description of the problem, its scope, the suspected root cause, and its priority level.
Problems are classified into four priority levels: critical, high, medium and low. Problems are prioritised based on the business criticality of the service, the priority level of the incidents causing the problem, and the impact on the business process. If necessary, the final priority of the problem will be agreed between the IT project manager and the business project manager/superuser of the information system. The factors that help to determine the priority levels based on the impact of the problem include the following:

Priority level	Impact of the problem	Maximum resolution time
Critical	The core functionality of a critical information system is non-operational, resulting in ongoing service disruptions or data loss	< 1 month
High	A secondary functionality of a critical information system is non-operational, potentially causing recurring disruptions and interrupting, but not halting, business processes.	< 3 months
Medium	A secondary functionality of a critical information system is non-operational, potentially causing disruptions that partially interrupt business processes and cause inconveniences, but work is not halted.	< 6 months

Low	The problem does not have a significant impact on information systems and does not affect business processes.	> 6 months

5.2 Problem definition and analysis

- Once the problem has been initiated and assigned to the IT project manager, the project manager shall review the definition of the problem and provide additional details. If, upon reviewing the details, it is determined that there is no actual problem, the problem should be closed. If the problem definition is unclear, the assignee must clarify and specify the problem definition.
- During the investigation of a problem, its causes are identified, and temporary solutions are provided to mitigate the impact until the necessary fixes or changes can be implemented. While developing a temporary solution, the problem solver shall outline the necessary actions to quickly and effectively mitigate or eliminate the impact of the problem. The IT project manager oversees the implementation of the temporary solution in accordance with the planned activities and schedule.
- Based on the previously collected information, it should be clear which component of the information system caused the problem, allowing the resolution team to begin investigating the root cause and developing a solution. Throughout the solution development process, the nature of the problem is analysed, with the aim of finding a proper and lasting solution.
- **Known bug** is a problem with an identified and documented cause, along with a temporary and/or permanent solution. If it is a known bug, the problem owner shall enter an appropriate note in the problem management tool.
- The assignee of the problem, in collaboration with the resolution team, determines the necessary activities to address the problem (including communication with all relevant parties) and documents these in the problem ticket.
- If a new problem is identified during the resolution process, a new ticket must be registered. The monitoring component of the information system must also be analysed, and if improvements are needed, these should be implemented, and the IT Helpdesk should be notified thereof.
- If the risk is accepted and the temporary solution is deemed satisfactory, or if a permanent fix is not feasible/resources are not available, the problem is closed with the approval of the information system or IT asset owner.

5.3 Resolving and closing a problem

A solution is the understanding of how to resolve a problem definitively and permanently. A solution is implemented according to the activities and deadlines established by the problem resolution team and is summarised in the problem ticket. A solution is implemented following the change management process, and the tickets are linked.
When marking the problem as resolved, a summary or general assessment should also be included. When closing a problem, the decision is documented as follows:

- **Not a bug** – a detailed justification of the assessment is also required.
- **Resolved** – the implemented solution has eliminated the root cause.
- **Known bug** – a workaround has been identified, the risk is accepted, and the decision to close the problem without implementing a permanent solution has been approved by the asset owner.
- **Not resolved** – the risk is accepted, and a solution to the problem cannot be identified due to a lack of resources and/or because it is not feasible; the decision to close the problem without implementing a solution has been approved by the asset owner.

6 Supervision

The Head of the Helpdesk Division shall exercise regular supervision over the request, incident and problem management process, ensuring that upon closing a request, all relevant information has been collected, all parties have been notified, and any necessary follow-up analysis (in the case of incidents) has been conducted and attached to the request ticket.