Approved by order No 221 of 10.12.2024 of the Director for Administration

In force from: 10.12.2024

Real Estate Request and Incident Management

1. General

1.1 The purpose of the real estate request and incident management process (hereinafter referred to as 'the process') is to ensure the provision of services in compliance with the agreed terms, while ensuring the maintenance, reliability and safety of technical systems of the buildings. The process is designed to quickly identify, register, analyse, resolve, and close requests and incidents, ensuring problems are resolved as efficiently and promptly as possible.

2. Definitions

2.1 "**Request**" means any enquiry, request for advice, order, notification submitted through designated channels that has not yet been categorised by type.

2.2 "**Requester**" means a person who uses university buildings and premises and related assets.

2.3 "**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.

2.4 "**Incident management**" means the management and coordination of activities associated with an actual or potential occurrence of an event.

2.5 "**Incident response plan**" is a key component of incident management that includes a documented set of procedures and guidelines for assessing incident severity, escalation, notification, and implementing recovery actions.

2.6 "**Incident coordinator**" means the role assigned to a person in the event of an incident. The person in the role is responsible for managing the process of addressing and resolving high- and critical-priority incidents, including emergencies and physical security events. An incident coordinator shall ensure effective collaboration, communication and implementation of the necessary measures to resolve the incident.

2.7 "**Event**" means an occurrence detected by the monitoring system that indicates deviations from the standard operation of a building or technical systems. This may indicate a failure, security concern, or other disturbance, but does not necessarily present an immediate threat or cause a disruption.

2.7.1 Types of events:

2.7.1.1 "**Fault**" means non-compliance with the established conditions, including agreements and/or obligations that may impact the functionality or reliability of a building, item of equipment, or system. A fault might not immediately result in a failure or emergency, but it indicates that the system or piece of equipment does not perform its function as expected or operate in compliance with the applicable standards. As a rule, a fault indicates the need for further or preventive maintenance to avoid further deterioration of the problem and major disruptions.

2.7.1.2 "**Failure**" means an incident where a device or system stops functioning or does not function properly, causing disruptions to the normal operation of a building or its technical systems. If a failure occurs, it will disrupt normal operations and impact user convenience, but it will not immediately cause significant material damage or pose a direct risk to human life. However, if a failure is not resolved promptly, it can escalate into a more serious issue that may result in an accident.

2.7.1.3 "**Emergency**" means an incident that significantly disrupts the normal functioning of a building or its technical systems, requiring immediate action to prevent severe property damage or threats to human life. Emergencies include situations such as power outages, flooding, gas leaks, heating system failures, fires, or other technical failures that damage the building's infrastructure, compromise user safety, or pose a risk of environmental damage.

2.7.1.4 "**Physical security incident**" means an event that threatens the security of university buildings, premises, assets, or individuals and requires an immediate response. This includes, but is not limited to, illegal or unauthorized access to buildings or restricted areas, vandalism, burglary, physical damage to property or infrastructure, and deliberate attacks, incl. armed attacks, or other violent actions that may endanger human life or property.

2.8 Maintenance services:

2.8.1 "**Upkeep services**" means routine maintenance services carried out regularly, usually weekly, to ensure the cleanliness of the buildings and premises and keep them aesthetic and fully functional. Upkeep services involve tasks such as cleaning rooms, corridors, and common areas; removing waste; arranging furniture; and maintenance of daily used surfaces, as well as maintenance of outdoor spaces to ensure a safe, clean, and welcoming working environment. Upkeep services are an integral part of routine maintenance carried out to help prevent major failures or wear and tear and to ensure the premises are consistently ready for use.

2.8.2 "**Preventive maintenance**" means a scheduled activity agreed upon in a maintenance plan, involving the inspection, cleaning, testing, and adjustment of equipment and technical systems to ensure their optimal performance and seamless operation. Regular maintenance helps prevent failures and emergencies, extends the lifespan of systems and equipment, and ensures their safe and efficient operation. Maintenance services may involve minor routine tasks as well as comprehensive inspections and adjustments, depending on the requirements for the technical systems and equipment.

2.8.2.1 "**Extraordinary maintenance**" means an unscheduled, exceptional maintenance service, ordered by an employee of the Real Estate Office to address an unexpected issue. This type of maintenance is carried out when an unexpected issue arises, requiring resolution to ensure the optimal functioning of a system or piece of equipment and to prevent potential failure. Extraordinary maintenance services are often time-critical, aiming to prevent more serious problems, failures or emergencies and may involve immediate inspection, repair or replacement of a piece of equipment or system.

2.8.3 "**Service request"** means a request to obtain information, advice, access, a service, or anything else in the area of real estate management.

2.8.4 **Management and maintenance services** – service request forms used to order maintenance and upkeep of buildings and premises, including the purchase and repair of furniture and window coverings, disposal of hazardous waste, moving service, nameplates and signage, specialised cleaning services and to request changes to the intended use or registry data of the premises.

2.8.5 **Security and access services** – service request forms used to order building security and access management solutions, including the installation of security and fire safety systems, as well as arrangement of event security and parking.

2.8.6 **Indoor climate and technical systems services** – service request forms used to order maintenance and configuration of indoor climate and technical systems of buildings, including renovation of ventilation, cooling, electrical and lighting systems.

2.8.7 **Transport and logistics services** – service request forms used to order a range of transport and logistics services, including moving services, gases and excise-free spirits, as well as taxi and car rental services.

2.8.8 **Construction and repairs** – service request forms used to order the construction and repairs of buildings, including small-scale repairs, interior design services, as well as large-scale construction and design projects.

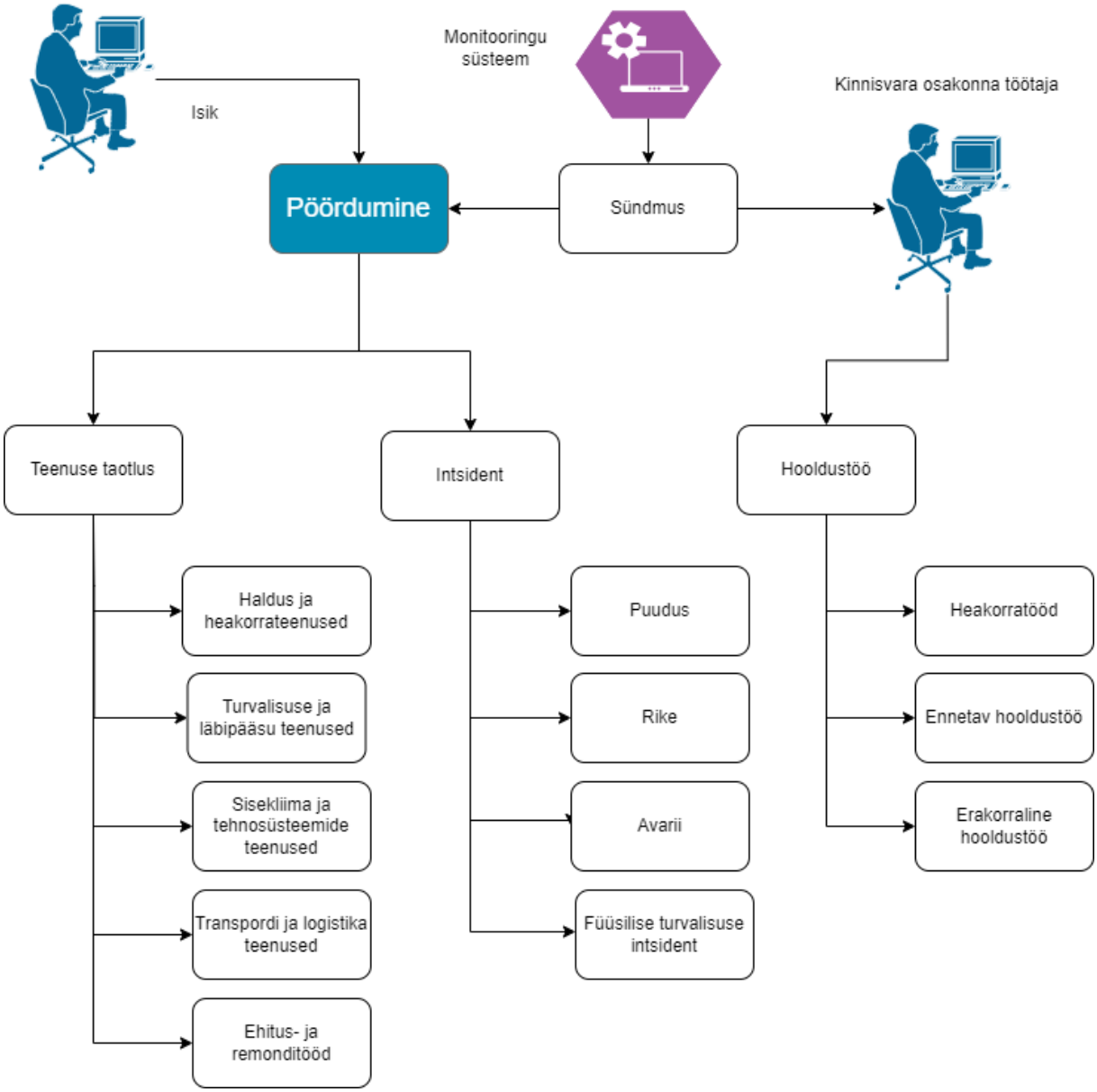

Figure 1 Requests to the Real Estate Office

2.9 The response times are the following:

2.9.1 **Response time** is the amount of time it takes for a Real Estate Office employee to review a request, categorise and prioritise the request and designate an assignee. During working hours, the requests received via email or JIRA shall be addressed within 1 working day.

2.9.2 **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 a Real Estate Office employee to respond to a customer support request after a request is made. First response time is up to three working days.

2.9.3 **Resolution time** is the time it takes to resolve a request or reply to an enquiry. Resolution time depends on the complexity and priority of the request.

3. Resolving requests

3.1 Channels for submitting and recording requests

3.1.1 Requests and incidents can be registered through the JIRA support portal, via email (murekontor@taltech.ee), or by calling the Security Division at 620 2112 (registration by phone is only used in the case of physical security incidents and emergencies, such as urgent or high-impact incidents). All requests and incidents are recorded in the JIRA ticket management system. Each request registered in the JIRA system must include the requester's name or username, along with a detailed description of the issue.

3.2 Responding to requests and providing a first response

3.2.1 The response time during working hours starts from the moment a request is registered. A Real Estate Office employee shall respond to a request. Events reported outside of working hours will be addressed on the next working day, except for physical security incidents and emergencies, to which the university's Security Division shall respond immediately.
3.2.2 A Real Estate Office employee shall respond to any registered request within 8 hours during working hours and shall conduct **an initial analysis** (excluding physical security incidents and emergencies, for more details see Incident management). The Real Estate Office employee shall categorise and prioritise the request and designate an assignee of the request. The Real Estate Office employee shall provide the first response to the requester regarding his/her request within three working days.

Table 1 Prioritising requests

		Impact			
		More than 50 persons affected, there is a risk of major financial loss (exceeding 100,000 euros) or a threat to human life	11–50 persons affected, there is a risk of significant financial loss (10,000–100,000 euros) or a serious threat to health	2–10 persons affected, there is a risk of minor financial loss (1,000–10,000 euros)	1 person affected, there is a risk of minimum financial loss (up to 1,000 euros)
Urgency	Highly urgent (threat to human life)	Critical	High	Moderate	Moderate
	Urgent (threat to health)	High	Moderate	Moderate	Low
	Medium	Moderate	Moderate	Low	Low
	Low	Moderate	Low	Low	Low

3.3 Processing and closing a request
3.3.1 A Real Estate Office employee categorises a request based on its type and content, conducts an initial analysis, and may request additional information from the requester if needed. The employee resolves the request himself/herself or creates a subtask, assigning it to the appropriate person by sending the description and any additional information.
3.3.2 In cases where a partner resolves a request, the Real Estate Office employee who assigned the request to a partner is responsible for resolving the request.
3.3.3 Requests are resolved based on their priority. Requests shall be resolved as quickly as possible. All actions are documented in JIRA as soon as possible after being carried out. The documentation shall provide enough detail to ensure clarity and provide a clear understanding of the actions taken and the rationale behind the decisions upon subsequent review.
3.3.4 The request owner shall mark a request as resolved 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 Real Estate Office employee. If a request cannot be resolved immediately, it will be assigned an appropriate status, such as 'paused,' 'unresolved,' or another relevant status to accurately reflect its current status. Clearly defining the status ensures clarity, as well as facilitates later tracking and reopening of the request if needed.
3.3.5 Once a request is resolved, the final resolution process shall be documented.

4. Incident management
4.1 A 24-hour security service is provided to prevent and resolve physical security incidents and emergencies across all university buildings and locations. The Security Division serves as the primary

coordinator for physical security incidents and emergencies (excluding faults and failures, which are addressed through the standard request resolution process).

4.2 Identifying an incident

4.2.1 At the university, incidents can be reported by anyone who detects disruptions in the normal functioning of buildings, technical systems, or breaches in security. Incidents can be identified in several ways:

4.2.1.1 persons' observations – physical failures (e.g., water leaks, power outages) or security breaches (e.g., unauthorized persons in buildings) may be identified by occupants of the premises or staff;

4.2.1.2 monitoring systems – the automated monitoring and surveillance devices of the university's buildings and systems, such as alarm systems, security cameras, fire alarms, and server and technical system monitoring tools can automatically alert to violations or potential threats;

4.2.1.3 the Security Division – the Security Division may identify incidents during regular patrols or based on information provided by surveillance equipment.

4.3 Responding to and prioritising an incident

4.3.1 Urgent and high-impact incidents affecting physical security or involving emergencies must be reported immediately to the Security Division, available 24 hours a day, by calling 620 2112. The Security Division coordinates the implementation of initial measures and, if needed, notifies the relevant specialists or the Emergency Response Centre.

4.3.2 Minor incidents, such as faults and failures, should be reported through the designated service channels, e.g. via the Jira support portal or via email at murekontor@taltech.ee.

4.3.3 In case of an attack, fire, or other emergency, the Emergency Response Centre shall be contacted first by calling 112, after which the Security Division shall be informed by calling 620 2112.

4.3.4 Emergency action guidelines for all persons at the university are available at safety.taltech.ee. These guidelines provide detailed steps and recommendations on how to respond in various critical situations, ensuring both safety and effective action.

4.3.5 When an incident is identified, whether by a university employee, student, visitor, security patrol, or automatic monitoring system, the Security Division shall promptly verify the received information. If needed, immediate measures shall be taken to mitigate the impact of the incident and prevent damage. The incident is then prioritised, and an incident response plan is activated based on established procedures (e.g., fire, explosion, attack, etc.). Should the incident require, the Emergency Response Centre shall be notified by calling 112.

4.3.6 Based on the nature and priority of the incident, the Security Division forwards the information to the designated contact person in the Real Estate Office's incident response list. The first person contacted by the Security Division shall assume the role of incident coordinator. The coordinator is responsible for resolving the incident and ensuring that the necessary specialists or contracting parties are involved to resolve it as quickly and efficiently as possible.

4.3.7 Priorities are determined based on the urgency of the requests. (Table1 Prioritising requests).

4.4 Resolving an incident

4.4.1 An incident coordinator is responsible for ensuring that all relevant parties are involved in resolving the incident (this applies to physical security incidents or emergencies; other incidents are addressed through the standard request resolution procedure), and for ensuring that the incident is resolved as quickly as possible and with minimal damage. The coordinator also ensures that all affected parties are notified and manages communication.

4.4.2 Notifications must be written in clear and correct Estonian and English, providing sufficient information about the incident's scope, further instructions, and the estimated resolution time. The incident coordinator selects the appropriate notification channels based on the nature of the incident. If the public has to be notified due to the scope of the incident, the incident coordinator will coordinate the messages with the Marketing and Communications Office who is responsible for public communication.

4.4.3 To resolve an incident, the staff of the Security Division and the contact persons in the incident response list are authorized to enter the facility without prior notice. If a room is marked with a hazard sticker (e.g., chemicals, explosion risk, high voltage), the building manager, the room supervisor, or the contact person of the structural unit must be contacted before entering.

4.5 Closing an incident and follow-up analysis

4.5.1 Once the resolution of an incident (physical security incident or emergency) has been completed and all necessary actions have been taken, the incident coordinator is responsible for closing the

incident. The coordinator shall make sure that all the activities related to the resolution are documented and inform the parties involved that the incident has been resolved. If the solution is unsatisfactory, the incident may remain open until the issue is fully resolved. The following activities must be completed before an incident can be closed:
4.5.1.1 documentation: all actions taken to resolve the issue, the parties involved, and the outcomes shall be thoroughly documented in the JIRA ticket management system or another relevant platform.
4.5.1.2 notification: all involved parties and affected persons shall be informed that the incident has been resolved. If necessary, additional notifications shall be prepared to inform them of preventive measures to be implemented in the future.

4.6 Follow-up analysis of security incident and emergency responses

4.6.1 Once an incident (physical security incident or emergency) is closed, a follow-up analysis is conducted to evaluate the cause, the resolution process, and any preventive measures to be implemented in the future. The lessons learned from the follow-up analysis should be incorporated to improve future procedures and guidelines. The follow-up analysis is conducted by the incident coordinator in collaboration with the Real Estate Office and other relevant parties involved in the incident. Key aspects of a follow-up analysis:
4.6.1.1 the cause of the incident: What was the root cause of the incident? Was it due to a technical failure, an external factor, or a procedural error?
4.6.1.2 resolution effectiveness: Did the incident response process and procedures function as expected? Were the necessary resources quickly available and properly allocated;
4.6.1.3 communication: Did all parties involved receive adequate information, and was the communication effective?
4.6.1.4 corrective actions: What corrective actions can be implemented to prevent similar incidents in the future or minimize their impact?

4.7 Incident report

4.7.1 Based on the follow-up analysis results, an incident report is prepared, which includes:
4.7.1.1 the date, location of, and time required to resolve the incident;
4.7.1.2 the cause of the incident and the actions taken to resolve it;
4.7.1.3 the parties and specialists involved in the resolution process;
4.7.1.4 the follow-up actions and recommendations to prevent similar incidents in the future;
4.7.1.5 the lessons learned and potential changes to procedures for improving incident management.
4.7.2 The final report helps evaluate whether all necessary measures were implemented effectively and serves as a foundation for future preventive actions and procedural improvements.

5. Carrying out maintenance work

5.1 Routine maintenance work

5.1.1 The Real Estate Office concludes procurement contracts for building and system maintenance services and appoints a responsible person to coordinate maintenance activities according to the established maintenance schedule. Users will be notified of maintenance work at least two weeks in advance, and the work will be coordinated with the building manager.

5.2 Extraordinary maintenance work

5.2.1 Extraordinary maintenance work not included in the maintenance schedule must be coordinated with the building manager. The building manager shall notify the involved parties about the work to be carried out and, if needed, arrange temporary access or interruptions of work.

5.3 Granting access rights to external persons for upkeep and maintenance work

5.3.1 External persons are granted the necessary access rights to fulfil their contractual obligations.
5.3.2 To carry out upkeep and maintenance work, the person responsible for fulfilling the contract specifies the required access rights and levels of the contracting party, considering the nature of the contract (depending on whether the person is an operational staff member or a person carrying out routine maintenance) and submits a request to the Security Division to create user group(s).
5.3.3 If the person is carrying out routine maintenance, access rights are granted only for the duration of the work. The request for access rights must be submitted at least three business days prior to the start of maintenance work.
5.3.4 The person responsible for the implementation of the contract submits requests for access rights of the contracting parties and keeps records of the access cards.

6. Supervision

The Head of the Real Estate Office regularly monitors the implementation of the real estate request and incident management and resolution procedure, ensuring that all operations are conducted in line with established procedures and guidelines.