Approved by Rector's directive No 16 of 23 April 2025
Amended by Rector's directive No 17 of 29 April 2025

In force from: 29.04.2025

Rules for Information Technology Development Work

1. Purpose and scope of application

1.1 The Rules for Information Technology (hereinafter referred to as "IT") Development Work apply to IT development processes and requirements at Tallinn University of Technology (hereinafter referred to as "the university"), including the collection of development proposals, as well as the preparation of IT development orders, planning of development work, prioritization and execution and subsequent IT management.

1.2 The Rules set out the requirements for the various stages of the IT development process to ensure consistent and controlled development practices across the university. The primary aim of the requirements is to ensure the security of applications and data in accordance with the information security standard ISO/IEC 27001, which provides a framework for secure software development, system architecture, and data protection. This guarantees that software development is carried out in accordance with secure development practices, preventing potential security threats, ensuring system reliability, and protecting data.

2. Definitions

2.1 "**Information system**" means a system which stores and processes information. An information system can consist of a set of interrelated modules/applications forming a unified whole for the user.

2.2 "**Application**" means a set of various programs designed to perform specific tasks. A set of applications can form an information system.

2.3 "**IT development**" or "**IT development work**" means the process of planning, specifying the requirements, designing, programming, documenting, testing, bug fixing involved in creating and modifying information systems and applications and the management activities necessary to carry out these processes.

2.4 "**Requirements for IT development work**" means the detailed requirements for IT development work annexed to the Rules.

2.5 "**IT development proposal**" means a proposal for IT development work that can be made by any member of the university.

2.6 "**IT development project**" means a broader set of IT developments (IT development orders, small-scale IT developments) with a defined scope and time frame and with the cost exceeding 60,000 euros (VAT included), aimed at introducing or replacing an existing information system or application.

2.7 "**IT development order**" means an IT development or set of developments with a defined scope and time frame, with the cost ranging from 0 to 60,000 euros (VAT included) or with the volume of 40 hours or more if performed within the organisation by the IT Services Office, and aimed at developing a certain additional functionality, significantly modifying existing features, or technically updating a specific application or information system.

2.8 "**Small-scale IT development**" means a small-scale IT development carried out under a simplified procedure, with the cost of less than 3,000 euros (VAT included) or with the volume of less than 40 hours if performed within the organisation by the IT Services Office.

2.9 "**IT development budget**" means the financial resources allocated by the decision of the Rector for the fulfilment of development orders, implementation of IT projects and carrying out small-scale developments in the specific financial year.

2.10 "**IT management costs**" means the costs of maintaining information systems or applications (licence fees, hosting costs, administration charges), which are allocated to the budget of the IT Services.

2.11 "**IT architecture**" means the structure of an information system or application, describing the relationships between its components and their interactions with the surrounding environment. An architecture includes also system design and development standards.

2.12 "**IT management**" means the process of maintaining an information system or application in accordance with the service level agreement, incl. application hosting, maintenance, installation of updates, availability management, configuration of technical settings, implementation of information security measures, backups, restoration and monitoring as needed.

3. The participants, responsibilities and tasks in the IT development process

3.1 The information system or application owner (area director):
3.1.1 designs a roadmap of information systems and applications supporting the process or processes in the field based on the substantive and IT architecture requirements;
3.1.2 appoints a business project manager for each information system or application;
3.1.3 initiates and launches improvements, including IT development projects or development orders (with the approval of the process owner and related stakeholders);
3.1.4 allocates and ensures the necessary resources (human resources, time, financial resources) for the project (incl. IT projects and IT development orders);
3.1.5 is responsible for the successful implementation of launched projects (incl. IT projects) and IT development orders and regularly monitors the progress of the project(s);
3.1.6 is responsible for risk mapping and management.
3.1.7 If the functionality of an information system or application concerns multiple processes, the owner is the director of the area, the processes of which are affected most by the information system or application, or the area directors agree on the owner's role among themselves.

3.2 The process manager (contracting authority):
3.2.1 carries out day-to-day management and development of the process, monitors user feedback;
3.2.2 makes proposals to the area director for initiating IT development projects and orders;
3.2.3 formulates the objectives, success criteria and indicators and coordinates them with the beneficiaries (users, participants in the process); prepares a project work plan and other necessary documentation;
3.2.4 plans and carries out operational restructuring or organisational changes when necessary, and manages their implementation (this includes informing stakeholders and explaining the need for and content of the changes, making sure that the organisation is prepared to adopt the resulting deliverables;
3.2.5 ensures that the goals of IT development projects are achieved by complying with the quality, time and budgetary objectives; takes preventive or corrective measures where necessary, informs the area director and the process owner of the risks and obstacles;
3.2.6 keeps all documentation related to the process (incl. regulations, process models, indicators, manuals) up to date.

3.3 The business project manager (the contracting authority's project manager):
3.3.1 is responsible for defining the roadmap or life cycle of an information system or application based on the substantive need and in alignment with the IT architecture;
3.3.2 ensures the consistency and integrity of functional IT developments across an information system or application;
3.3.3 provides the process manager regular overviews of IT developments and informs the area director or process owner as necessary;
3.3.4 monitors the implementation of the budget allocated to the information system or application;
3.3.5 processes new IT development proposals in cooperation with the process manager and prepares IT development orders and terms of reference;
3.3.6 organises analysis (the business project manager carries out analysis himself/herself, orders the analysis from a development partner or arranges it in another way) and, if necessary, conducts market research to find the most suitable solution in terms of functionality;
3.3.7 manages IT projects, IT development orders and small-scale IT developments and makes sure that the objectives are achieved; prepares an IT development plan in cooperation with the process manager, IT project manager and other related parties;
3.3.8 is responsible for the success and risk management of an IT project;

3.3.9 is responsible for managing and updating the project documentation of the application or information system;
3.3.10 organises the data protection impact assessment and information security risk assessment and ensures its compliance with the requirements;
3.3.11 is responsible for organising functional testing and validation during the IT development process. A successfully passed test is a prerequisite for accepting IT development work;
3.3.12 is responsible for preparing and/or updating manuals;
3.3.13 participates in negotiations regarding the service level agreement held with the IT management service provider;
3.3.14 compiles the part of functional requirements of the procurements of IT development work, IT development partners and IT management; organises purchasing of licences and software services in cooperation with the IT Services.

3.4 The superuser:
3.4.1 provides daily support to the users of the information system or application;
3.4.2 is responsible for provision of training to the users and IT Helpdesk and ensuring the availability of manuals;
3.4.3 manages application or information system settings (incl. configures workflows, etc.);
3.4.4 proposes additional IT developments, supplements the terms of reference, business analysis and IT development orders if necessary;
3.4.5 is responsible the timely management of the rights of access to the application or information system and, in cooperation with the process manager, develops the principles for granting access;
3.4.6 manages data in the information system or application, i.e. the information assets; fulfils the obligations placed upon a superuser based on the Information Security Policy.

3.5 The IT project manager:
3.5.1 coordinates the implementation of IT development work in cooperation with the IT development partner;
3.5.2 breaks down IT development orders into smaller tasks or work packages, if necessary;
3.5.3 prepares a schedule for fulfilling an IT development order in cooperation with the IT development partner, ensures its fulfilment and provides the business project manager an overview of its progress in the agreed form;
3.5.4 coordinates with the business project manager the use of the approved budgetary resources and is responsible for staying within the allocated budget;
3.5.5 is responsible for managing the technical documentation of the information system or application;
3.5.6 organises procurement of IT developments, IT development partners and IT management services and is the person responsible for carrying out procurements; compiles the parts of non-functional requirements and IT management components for procurements and integrates them with the functional requirements received from the business project manager into a unified document;
3.5.7 performs or organises system analysis;
3.5.8 ensures compliance of IT development work with the requirements for architecture and information security;
3.5.9 is responsible for developing UX/UI design in cooperation with the IT development partner, the business project manager and future users;
3.5.10 is responsible for non-functional testing;
3.5.11 accepts IT development work from an IT development partner and with the approval of the business project manager orders the system manager to install updates;
3.5.12 is responsible for negotiating and concluding a service level agreement.

3.6 The IT architect:
3.6.1 develops the IT architecture principles, manages the architecture of the university's IT solutions, creates the corresponding component diagrams and approves the designed architecture based on the agreed principles and the existing IT architecture. For approval, involves an IT infrastructure information security expert to confirm that the solution complies with security requirements;
3.6.2 makes sure that the architecture of IT systems is designed in compliance with IT architecture principles and manages the data architecture across information systems and applications;
3.6.3 prepares the preliminary IT architectural design for IT development orders and IT projects if necessary.

3.7 The IT development partner (an external partner or the IT Services):
3.7.1 executes IT development orders approved by the IT project manager;
3.7.2 performs work in accordance with the IT architecture principles, data protection and information security requirements;
3.7.3 is responsible for achieving the agreed outputs and goals; monitors the progress of an IT project, makes sure that the goals of the IT project are achieved by complying with the quality, time and budgetary objectives and takes preventive or corrective measures if necessary;
3.7.4 mitigates and manages risks upon fulfilling IT development orders;
3.7.5 adheres to the best practices in the field, including the OWASP Secure Coding Practices, to ensure code security and compliance with information security standards;
3.7.6 when using third-party software, the developers must ensure it is sourced exclusively from trusted and official providers, and that its licensing complies with the university's policies and requirements. Prior to software integration, security checks and risk assessments must be performed to identify potential vulnerabilities. Software and its components must also be regularly updated, and security patches must be applied to maintain system security and stability;
3.7.7 makes sure that reports are submitted to the IT project manager in the agreed form;
3.7.8 delivers the work completed in the framework of IT development orders.

3.8 The system manager:
3.8.1 is responsible for installing and managing servers and information systems, applying security patches and updates, and ensuring system continuity;
3.8.2 is responsible for the implementation of the service level agreement of an application or information system;
3.8.3 manages environments related to IT development of an information system or application (the development, testing and production environments);
3.8.4 installs updates to the information system or application based on the instructions of the IT project manager;
3.8.5 manages settings and makes technical adjustments related to the information system or application if necessary;
3.8.6 ensures the implementation of information security requirements and fulfils the requirements set for an information asset administrator in the Information Security Policy;
3.8.7 compiles and updates the technical documentation, including recovery manuals, of an information system or application and performs regular recovery testing from backups;
3.8.8 installs the monitoring tool as required and ordered by the IT project manager;
3.8.9 cooperates with the IT infrastructure team;
3.8.10 maps technical risks and proposes improvements.

3.9 The IT development manager:
3.9.1 leads the IT development process;
3.9.2 processes IT development proposals;
3.9.3 processes and approves IT development orders and terms of reference;
3.9.4 provides advice to parties involved in an IT development order;
3.9.5 ensures that IT development orders are consistent with the organization's goals;
3.9.6 prepares a budget proposal for IT developments;
3.9.7 plans the execution of IT development orders in cooperation with the business and IT project managers;
3.9.8 provides advice to parties involved in an IT development order to ensure that the solutions being developed are consistent with the organisation’s goals;
3.9.9 is a member of the IT development steering group;
3.9.10 appoints IT project managers and system administrators for information systems and applications.

3.10 The IT development steering group:
3.10.1 is responsible for prioritizing IT development orders and IT projects and submits an IT development budget proposal to the Rectorate for approval;
3.10.2 decides on the initiation, implementation and termination of IT projects;
3.10.3 receives reviews and monitors the progress of IT development orders and IT projects;
3.10.4 makes proposals to improve the IT development process if necessary;
3.10.5 The IT development steering group is led by the head of the IT Services Office.

3.10.6 The IT development steering group consists of all the heads of the administrative and support structure units (except for the FinEst Centre for Smart Cities, AI & Robotics Estonia (AIRE)), the IT development manager and the head of the IT Services. Business and IT project managers are involved in the steering group if necessary.

4. The IT development process

4.1 The university's IT development process is based on the Secure Software Development Lifecycle, ensuring that security requirements are integrated into every stage of development. The Annex to the Rules for Information Technology Development Work, titled 'Requirements for IT Development Work,' outlines the default requirements applicable to all projects. However, based on a risk assessment, reduced requirements may be applied to specific systems and applications. Even in exceptional cases, adherence to the principles of Secure Software Development Lifecycle must be ensured, along with the protection of systems and data in accordance with international best practices.

4.2 [repealed – entry into force 29.04.2025]

4.3 The Secure Software Development Lifecycle involves conducting security analysis from the planning stage, performing risk assessments during system design, applying secure coding practices throughout development, carrying out risk-based security testing before deployment, and continuous monitoring for vulnerabilities and applying updates during the maintenance period.

4.4 Initiation

4.4.1 Members of the university can make IT development proposals on the intranet (through the Help Centre);
4.4.2 An IT development proposal is reviewed by the IT development manager, who forwards it to the business project or process manager for processing;
4.4.3 The business project manager and the process manager review the IT development proposal. If necessary, the person who made the IT development proposal, the IT development manager or the IT architect will be involved in the development of a possible solution;
4.4.4 The business project manager organises communication and feedback related to the IT development proposal. The final status of an IT development proposal can be either rejected or accepted for development;
4.4.5 If a development proposal is accepted for development, the business project manager, in cooperation with the IT project manager, decides whether it is a small-scale development, an IT development order or an IT project. Implementation of the IT development will proceed accordingly;
4.4.6 The business project manager, in cooperation with the process manager, prepares an IT development order and terms of reference based on the IT development proposal or identified development need.
4.4.7 The IT development manager approves the development order (approved or returned to be supplemented);
4.4.8 Small-scale IT developments are implemented directly through the IT project manager, not by following the procedure for processing IT development orders, however, the technical, architectural, documentation and testing requirements must be fulfilled also in the case of small-scale IT developments.

4.5 Prioritising and planning IT development orders

4.5.1 The prioritisation of IT developments involves IT development orders and IT development projects, for which proper terms of reference have been prepared and which have been approved by the IT development manager.
4.5.2 The IT development manager holds meetings on IT development orders with all the heads of the units of the administrative and support structure and business project managers once a quarter to jointly review the current status, priorities, feasibility, time frame and estimated cost of IT development orders. If necessary, adjustments are made in the IT development orders and the corresponding agreements and changes shall be indicated in the work. A budget for small-scale developments is planned for information systems or applications for the next calendar year. The scope and costs of IT management are discussed, and service level agreements are specified.
4.5.3 The IT development manager collects the IT development orders, incl. the budget of small-scale IT developments for the IT development steering group and prepares the initial budget proposal for IT developments. The proposal shall be prepared based on the priority, feasibility and time frame of the IT development orders.

4.5.4 The IT development budget proposal is processed by the IT development steering group, who proposes amendments if necessary. The head of the IT development steering group submits the IT development budget proposal to the Rector for approval.
4.5.5 The IT development budget is approved based on IT development orders and is broken down according to the approved budget by IT development orders, IT projects and small-scale IT development work. The IT project manager is responsible for the use of the budget.
4.5.6 After approval of the budget for IT development work, the IT development orders are scheduled in the order in which the work is to be carried out. Business project managers schedule IT development work in cooperation with the IT project managers and the IT development manager, taking into account the IT developments already underway and the capacity of the IT development partners to perform the work.
4.5.7 The priority, schedule and budget of an IT development order can be changed, if necessary, with the approval of the IT development manager and head of the IT Services.

4.6 Analysing and planning IT development orders

4.6.1 A business analysis is prepared for IT development orders, a new solution is planned, and a system analysis is prepared. For each IT development order, the business project manager and the IT project manager decide which outputs need to be produced in these stages taking into account the requirements.
4.6.2 Security risks must be identified and corresponding requirements defined during the business analysis and planning stage to ensure the confidentiality, integrity, and availability of information systems. Security risk mitigation measures must also be integrated into the system architecture during these stages.
4.6.3 The IT architect reviews the final solution design and, if necessary, consults the Information Security Division to validate security aspects and assess compliance with information security requirements.

4.7 Executing IT development orders

4.7.1 The IT project manager requests a quote for the IT development order and obtains approval of the IT development manager and the head of the IT Services. In the course of it, the exact financial value of the IT development order is confirmed.
4.7.2 The IT project manager forwards the IT development order to the IT development partner for execution.
4.7.3 The IT development partner delivers the completed work to the IT project manager.
4.7.4 An IT development order is deemed to be fulfilled when the system manager has installed the work carried out under the IT development order on the production platform of the information system or application and the IT project manager has signed a record of acceptance. A record of acceptance need not be signed for IT developments carried out within the university. The record is the basis for invoicing.
4.7.5 Payments for IT development work are made according to the IT development budget. Any potential changes to the budget shall be approved by the IT development manager and the head of the IT Services.
4.7.6 Invoices for IT development work shall be approved by the IT development manager, the IT project manager and the head of the IT Services. IT project managers shall include the agreed project and activity codes on purchase invoices.

4.8 Implementing IT projects

4.8.1 The process manager makes a proposal to initiate an IT project, and the process owner formulates the goal. The area director verifies that the outputs comply with the organisation’s goals and users’ needs.
4.8.2 The process manager coordinates the objectives and measurable outputs with the beneficiaries.
4.8.3 Before launching an IT project, the following roles set out in the Rules for Information Technology Development Works hall be defined and manned: the process manager, business project manager, IT project manager.
4.8.4 The business project manager, in cooperation with the project team, prepares an IT project plan, which shall be approved by the IT development steering group.
4.8.5 After its launch, the IT development project is broken down into smaller IT development orders, fixing the scope of the IT project based on the initiation proposal.

4.8.6 An IT project shall be implemented by applying an agile approach, i.e. the development process is divided into a number of iteration cycles, by delivering intermediate results at the end of each cycle, on the basis of which it can be validated whether the steps have been taken in the right direction and the scope can be completed. The business project manager, IT project manager and IT development partner review the progress of the work at agreed intervals and, if necessary, specify the requirements.
4.8.7 When the agreed scope is completed, the IT project is terminated.

Table 1. Table of an IT development process

Stage	Input	Action	Output	Executor	Where
Initiation	Idea/problem	Making an IT development proposal;	An IT development proposal	Members of the university	Help Centre (IT development proposal form)
	IT development proposal	Processing, deciding and providing feedback on the IT development proposal;	The IT development proposal has been processed and a decision on the proposal has been made	Business project manager	JIRA (workflow of the IT development proposal)
	An IT development proposal or order submitted by the process manager	Preparing an IT development order and terms of reference;	A JIRA request has been compiled for an IT development order	Business project manager	JIRA project TTD
	A JIRA story has been compiled for an IT development order	Approving the IT development order	The IT development order and terms of reference have been approved	IT development manager	JIRA project TTD
Planning and budgeting	The IT development order and terms of reference have been approved	Prioritizing and planning of the IT development order in cooperation with business project managers, process managers and area directors;	A prioritised IT development order	IT development manager	JIRA project TTD
	Prioritised IT development order	Preparing a budget proposal for IT developments/proposing amendments	A budget proposal for IT developments	IT development manager	JIRA project TTD/ Excel
	A budget proposal for IT developments	Processing the budget proposal for IT developments	The budget for IT developments has been processed	IT development steering group	Excel & PowerBI
	The budget for IT developments has been processed	Approving the budget for IT developments	An approved IT budget	Rector	JIRA project TTD / NAV project module / PowerBI
	An approved IT budget	Planning and sequencing of IT developments	The IT development plan	Business project manager and IT project manager	JIRA project TTD
Analysis	An IT development order	Preparing a business analysis (collecting functional and non-functional requirements)	A business analysis	Business project manager (organises the analysis)	Confluence
	Business analysis	Planning	The solution has been designed	Business project manager (organises the analysis)	Confluence

Stage	Input	Action	Output	Executor	Where
	The solution has been designed	Preparing a system analysis	A system analysis	IT project manager (organises the analysis)	Confluence
	A system analysis	Approving the results of the analysis	The analysis has been approved	IT architect	JIRA project TTD/ Confluence
Implementation	An IT development order	Requesting a quote for the IT development order and agreeing on the scope	The development order with the volume of the tender has been approved	Business project manager	JIRA TTD
	An IT development order	Forwarding the IT development order to an IT development partner	The IT development work has been forwarded to the IT development partner in JIRA	IT project manager	JIRA
	The IT development work has been forwarded to the IT development partner in JIRA	Executing the IT development orders	The work has been completed	IT development partner	The platforms agreed with the IT development partner
	The work has been completed	Testing the completed work	The work has been tested	IT development partner, business project manager, IT project manager	Confluence
	The work has been tested	Installing the solution	The IT solution has been installed	System manager	Confluence
	The IT solution has been installed	Signing a record of acceptance of work	A record of acceptance of work has been signed	IT project manager	Confluence
	A record of acceptance of work has been signed	Invoicing for work completed	An e-invoice	Business project manager	
Deployment	The IT solution has been installed	Providing user training and preparing guidelines	Guidelines have been prepared, and user training has been provided	Business project manager	Confluence
	The IT solution has been installed	Updating the process documentation and informing the stakeholders		Process manager	

Table 2. Procurement of IT developments, IT development partners, including the IT management service

Stage	Input	Action	Output	Executor	Where

Procurement	A need to order IT development work	Preparing and conducting procurements for IT developments, development partners and IT management	Procurement documents, incl. the technical specification, the draft framework agreement and public contract, the evaluation methodology and eligibility criteria	IT project manager and business project manager	Confluence
	The procurement of IT developments has been approved	Approving the procurements of IT development work	The procurement of IT developments has been approved	IT development manager	
	A framework agreement	Execution of the framework agreement and public contracts	Public contracts	IT project manager	

ANNEX
Requirements for IT development work

1. Requirements for documentation
1.1. General requirements for storing documents related to IT development
1.1.1. Materials related to an information system or application, its development and other necessary documentation shall be stored on platforms managed by the IT Services.
1.1.2. In the course of execution of IT development orders (hereinafter referred to as "development order"), the documentation shall be recorded and/or updated in the case of small-scale developments in compliance with the requirements set out below.
1.1.3. The IT development manager has the right to allow exceptions to the requirements depending on the specificities of an information system or application.
1.2. Requirements for IT development proposals (hereinafter referred to as "development proposal")
1.2.1. Development proposals shall be documented and processed on the JIRA platform.
1.2.2. A development proposal shall be accompanied by the following information:
1.2.2.1. the description of the development proposal (the description of the problem, the description of a possible solution);
1.2.2.2. the benefits resulting from the implementation,
1.2.2.3. the related information system or application;
1.2.2.4. the related processes;
1.2.2.5. the decision on the IT development proposal.
1.3. Requirements for development orders and terms of reference
1.3.1. Development orders are added to the JIRA platform under the TalTechDigital (TTD) project.
1.3.2. A development order shall be accompanied by the following information:
1.3.2.1. the responsible structural unit (contracting entity);
1.3.2.2. the process;
1.3.2.3. the primary information system or application;
1.3.2.4. the related information systems or applications;
1.3.2.5. the business project manager (*assignee* in JIRA project TTD);
1.3.2.6. the process manager (*reporter* in JIRA project TTD);
1.3.2.7. the IT project manager;
1.3.2.8. the estimated budget/cost;
1.3.2.9. the approved budget by year;
1.3.2.10. the description of the development order;
1.3.2.11. the description of the problem to be solved;
1.3.2.12. the proposed solution/market research;
1.3.2.13. the goal:
1.3.2.14. the expected benefits and cost-effectiveness;
1.3.2.15. the measurable result;
1.3.2.16. the priority;
1.3.2.17. the beneficiaries;
1.3.2.18. the key personnel/related parties;
1.3.2.19. the restrictions and risks;
1.3.2.20. the preliminary data protection impact assessment;
1.3.2.21. the information security risk analysis.
1.4. Requirements for JIRA and Confluence platforms of an information system or application
1.4.1. Depending on the development order, tasks are created for the development work on the JIRA platform of each information system or application.
1.4.2. An IT development partner (hereinafter referred to as "development partner") shall be added to the JIRA platform of the information system or application. Development tasks are communicated to the partner through the platform to obtain a quote and subsequently fulfil the order.
1.4.3. Communication related to development work between the contracting entity, development partner or members of the team shall be documented in JIRA under the corresponding task (commenting functionality).
1.4.4. Any of the following information related to an information system or application shall be entered on the Confluence platform in the form of text, a file, or a reference:

1.4.4.1. the parties involved in the development (the team, the development partner and other relevant persons);
1.4.4.2. the materials created upon the preparation and conducting of procurements;
1.4.4.3. the framework agreements and public contracts;
1.4.4.4. other legal documents or relevant materials;
1.4.4.5. if necessary, restriction on access to the materials shall be established in Confluence.
1.5. Requirements for analysis:
1.5.1. **Business analysis** involves defining, analysing and structuring of requirements:
1.5.1.1. expectations and feedback from users and stakeholders (what the future solution should be and what needs to be done);
1.5.1.2. a description of the current *(as is)* state of a process and the list of roles;
1.5.1.3. a description of the future *(to be)* state of a process and the list of roles;
1.5.1.4. descriptions of the functional requirements (what the system must do, what the user can do, what services the system should provide);
1.5.1.5. descriptions of non-functional requirements;
1.5.1.6. descriptions of integration solution requirements;
1.5.1.7. descriptions of business rules, restrictions and regulations;
1.5.1.8. descriptions of the data used or required in the business process;
1.5.1.9. data protection impact assessments;
1.5.1.10. a feasibility assessment and plan.
1.5.2. **Planning** involves the following:
1.5.2.1. market research carried out to find a more suitable solution and/or best practice;
1.5.2.2. a feasibility assessment and plan;
1.5.2.3. (a) draft design(s) (of an information system or application);
1.5.2.4. comparison of alternative proposed solutions and technologies;
1.5.2.5. an initial IT architecture model;
1.5.2.6. IT security risk assessment;
1.5.2.7. a sample model *(mockup)*.
1.5.3. **System analysis** involves the following:
1.5.3.1. descriptions of data integrations and data sources;
1.5.3.2. a database model;
1.5.3.3. the final system architecture design (component diagram);
1.5.4. the results of the analysis shall be documented on the Confluence platform of the information system or application.
1.6. Requirements for acceptance of work:
1.6.1. The existence of appropriate deployment documentation (including deployment files, maintainability, availability and reliability requirements together with the associated access rights) is a prerequisite for deployment.
1.6.2. The documentation created or updated in accordance with the requirements is a prerequisite for accepting work.
1.6.3. A record of acceptance of work shall be signed.
1.7. Requirements for the use of the IT development fund and invoicing
1.7.1. Development work is covered from the corresponding financial source of the IT Services.
1.7.2. The IT development fund does not cover staff costs, secondments or economic costs.
1.7.3. Any maintenance and consultation costs shall be covered by the budget of small-scale developments.
1.7.4. Invoices shall be settled based on a record of acceptance signed by both parties.
1.8. Requirements for IT project plans
1.8.1. An IT project plan shall include the following:
1.8.1.1. the description of the problem;
1.8.1.2. the possible damage caused if the problem persists;
1.8.1.3. the project objectives;
1.8.1.4. relevance of the project to the strategic goals of the university;
1.8.1.5. the expected results;
1.8.1.6. the project beneficiaries;
1.8.1.7. the project benefits;
1.8.1.8. the stakeholders;

1.8.1.9. the project risks (incl. data protection and information security risks);
1.8.1.10. the description of required resources;
1.8.1.11. the initial project budget;
1.8.1.12. the initial main phases of the project;
1.8.1.13. the description of the initial architecture of the technical solution;
1.8.1.14. the IT system or application management model and the estimated IT management costs.

2. Requirements for IT solutions

2.1. Requirements for user interfaces

2.1.1. The user interface of a web application must comply with at least WCAG 2.0 level AA.
2.1.2. All the decisions regarding the design of user interfaces must be approved by the contracting entity before they are implemented.
2.1.3. A web-based user interface shall be compatible with the most common web browsers, including on smart devices (Android, IOS).
2.1.4. The colour scheme and logo used in the application design must correspond to the corporate visual identity (CVI) and the design system for digital environments of the contracting entity.
2.1.5. An application must function properly with different screen sizes and resolutions, including those of the most common devices, ensuring a clear layout, readability, and optimal usability.
2.1.6. Exceptions are allowed to standard software or with the approval of the IT development manager.

2.2. Requirements for IT architecture and technical solutions

2.2.1. Modular architecture must be used for information systems and applications. Information systems must have completely decoupled front end (the presentation layer) and back end (business logic layer) architecture and must be independently deployable.
2.2.2. It must be possible for information systems or applications to communicate via service interfaces and the functionality of an information system or application must be supported by an API. The preferred standards are REST and JSON. All API interfaces must be secured with strong authentication and authorization mechanisms, and API calls must be validated to prevent misuse and safeguard the system against malicious activities.
2.2.3. Application logic and data management functions shall be separated and independent.
2.2.4. When using third-party software, the developers must ensure it is sourced exclusively from trusted and official providers, and that its licensing complies with the university's policies and requirements. Security checks and risk assessments must be conducted before integrating software into an information system or application.
2.2.5. Information systems and applications shall be designed and implemented based on the once-only data entry principle.
2.2.6. Information systems and applications must be designed in accordance with the Principle of Least Privilege, ensuring that users are granted access only to the resources and functions necessary for their roles. Access levels must be managed based on user roles.
2.2.7. Authentication shall be carried out using the university’s ID (Azure AD). In exceptional cases where the use of Entra ID is not possible due to specific restrictions, alternative secure authentication methods must be implemented. In such cases, the use of multi-factor authentication (MFA) is mandatory to ensure the highest level of system and data security.
2.2.8. Based on risk assessments carried out as part of information security risk management, data requiring a high level of protection within information systems must be encrypted both at rest and in transit, using modern encryption standards and best practices.
2.2.9. The names of the tables and attributes in a database must be in English.
2.2.10. Applications and information systems must meet the OWASP ASVS requirements. The implementation of OWASP ASVS requirements is guided by general principles; however, for specific projects, the scope must be determined based on the results of a risk assessment.
2.2.11. It must be possible to move an application from one domain or site to another without reprogramming.
2.2.12. UTF-8 encoding must be used for all data, databases, SQL scripts and applications.
2.2.13. All table entries must include the dates of entry, modification, and deletion.
2.2.14. The health check reports of an application shall be provided in the machine-readable JSON format.
2.2.15. Data creation, modification, and deletion activities must be recorded in database logs.

2.2.16. Exceptions to IT architecture and technical requirements are allowed with the approval of the IT development manager and IT architect. The IT development manager, in collaboration with the IT architect, also has the authority to establish additional requirements for IT development orders and projects to ensure compliance with specific technical and security standards. Additional requirements may be more detailed, outlining specific solutions and best practices.

2.3. Requirements for source codes

2.3.1. The codebase of an information system or application must be managed in the code version control system managed by the IT Services.

2.3.2. The generated code must comply with best practices and security standards, including the OWASP Secure Coding Practices. The implementation of OWASP Secure Coding Practices is guided by general principles. However, for specific projects, the scope must be determined based on the results of a risk assessment. When writing code, you must:

2.3.2.1. prevent common security vulnerabilities, including but not limited to SQL injection, cross-site scripting)(XSS), and buffer overflow;

2.3.2.2. perform input validation and proper data handling at all critical points;

2.3.2.3. ensure security measures are integrated throughout the system, in compliance with risk assessments and security standards;

2.3.2.4. avoid storing sensitive data, such as application or information system access credentials (username and password), mandates and configuration elements in the source code;

2.3.2.5. implement secure error-handling mechanisms that do not reveal sensitive information.

2.3.3. The program code to be developed must adhere to the Clean Code standard. Critical functionality of the code must be covered by unit tests.

2.3.4. All new software, whether created or purchased, shall be deployable through continuous integration and continuous delivery/deployment (CI/CD) process. The CI/CD development process must be secure and incorporate built-in security controls, such as automated security scans, code quality analysis, and vulnerability detection, prior to software deployment.

2.3.5. The names of variables, types and functions must be substantive and give an indication of their purpose.

2.3.6. It must be possible to configure the installation settings (e.g. a system that runs only on servers of a specific service provider or manufacturer cannot be accepted);

2.3.7. The IT development manager has the right to allow exceptions in the case of some information systems or applications. Additionally, the IT development manager has the authority to set further requirements to ensure projects meet specific technical and security standards. These additional requirements may provide more detailed guidance, including specific instructions and recommended best practices for development tasks.

2.4. Requirements for installation

2.4.1. Software must be installed in a controlled environment, where access control, traceability of changes, and protection against unauthorized actions are ensured. To ensure this:

2.4.1.1. separate development, testing, and production environments must be used, with strict access restrictions;

2.4.1.2. all software version transitions between environments must be documented and limited to authorized users through a secure, traceable CI/CD (continuous Integration and delivery/deployment) process.

2.4.1.3. The IT development manager has the authority to establish additional requirements for software installation and deployment to ensure the system meets specific technical, security, and performance standards. Additional requirements may include, for instance, specific configuration settings, installation environment specifications, or the implementation of additional security measures during deployment.

2.5. Requirements for testing

2.5.1. The tested stories and tests performed shall be described based on functional and non-functional requirements.

2.5.2. Following the developments, load and security tests must be conducted based on the results of the risk assessment. The test results must be documented and stored in the information system or on the Confluence platform.