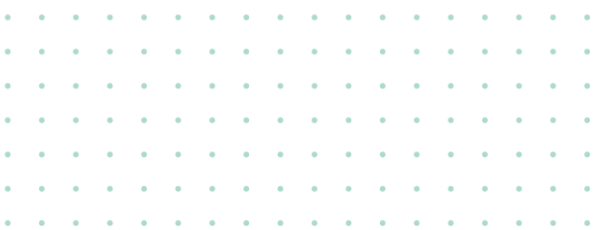


Guidelines for IT development 2025



VISION		Interdisciplinary university, competitive at the international level, developing and transferring new knowledge and innovations		GOAL		Ensuring the effective implementation of the University's activities and strengthening the competencies of its human resources	
VALUES		SOCIAL RESPONSIBILITY		COOPERATION		CONTINUOUS IMPROVEMENT	
STRATEGIC OBJECTIVES		<ul style="list-style-type: none">• Develop a reliable and interoperable IT infrastructure of the University, integrating with national and international IT platforms• Digitise the University's management processes• Develop IT services according to the principles of interoperability, availability and security		<ul style="list-style-type: none">• Develop the interoperability of the University's IT infrastructure and employee participation in international IT activities (GEANT, EuroHPC, EOSC, CERN CMS, etc.)• Develop IT service solutions in the education and research segment• Strengthen cooperation with the ŠMSM and NKSC in the management of IT security and cyber incidents		<ul style="list-style-type: none">• Organise the data managed by the University as information resources• Develop general IT competencies and IT security maturity in employees and students	
SUCCESS CRITERIA		<div>↓</div> <ul style="list-style-type: none">• Interoperability with the VIISP, eIDAS, FABIS, NŠA registers at the national level and with the ECIU DXP, GEANT, EOSC at the international level• Digitise the processes necessary for the performance of key administrative functions - 100%• IT infrastructure resilient to cyber threats -100%		<div>↓</div> <ul style="list-style-type: none">• The University IT infrastructure integrated into the EuroHPC - 100%• Research data integrated into the EOSC platform - 100%• The Security Operations Centre (SOC) is established and accredited at the University for the IT segment in education and research - 1		<div>↓</div> <ul style="list-style-type: none">• The data analytics platform for the University's digitised processes is enabled – 1• The share of the University employees capable of identifying information attacks and misleading information - 70%	