Security policy at CTU

Code:	ČVUT_PR_2025_04_V01
Type:	Rector's Order
Ref. No.:	CVUT00008112/2025
Regulated area:	ISMS information security
Organizational application:	CTU
Guarantor of standard:	51982 Director of Security Department of CTU Bc. Jaroslav Compel, MPA
Issuer:	doc. RNDr. Vojtěch Petráček, CSc. Rector
No. of pages:	8
No. of annexes:	0
Distribution list:	Security Department of CTU
Affected persons:	employees (B-00000-SUMA-ZAMESTNANEC) students (B-00000-SUMA-STUDENT)
Form of publication:	Inforek
Replaces:	
Issued on:	1st May 2025
Force:	1st May 2025
Effect:	1st May 2025
Other information:	
Signature of issuer:	

m. p.

doc. RNDr. Vojtěch Petráček, CSc.

Rector

Overview of changes

Provision	Detailed specification of changes and justification of changes compared to previous version

List of annexes

List of related documents

Čl. 1 Vision

The Czech Technical University in Prague (CTU) **creates a safe academic environment** that supports education, science, research, development of technologies and innovation without putting at risk the integrity, accessibility and confidentiality of persons, information and infrastructure of the university. The main priority is the protection of life and health of students, employees and visitors at the university. It is also necessary to ensure security of university facilities and responsible handling of information in all forms.

CTU follows the principle that **security is a key precondition for free education and scientific advancement**; this is achieved through **effective and responsible management of security risks and establishing modern preventive measures.**

Key directions of visions:

- **Proactive handling of security threats** through modern technologies and risk analysis.
- Building a **comprehensive culture of security** where students, academics and employees understand their roles within the university's security ecosystem.
- Putting **emphasis** on attainment of knowledge and skills, the so-called **security competences of students, academics and employees** that can be used in case of an emergency situation.
- **Implementing advanced security technologies** including artificial intelligence and cyber defence mechanisms.
- Strengthening **institutional and international collaboration** in the field of academic security including protection of intellectual property rights and prevention of espionage.
- **Protection of sensitive and strategic research** that have a connection and impact on national security and economy and the information environment of the Czech Republic.

Čl. 2 Goal

The **goal is to build and maintain a culture of security** that will ensure resilience and protection of students, academics, employees and partners of the university against physical, cyber, organizational and other threats.

CTU understands security as a state in which all risks are effectively managed and minimized.

Čl. 3 Mission

The mission of the Security Department of the CTU Rector's Office and security management is to **protect the academic environment at CTU through effective management of security risks**, implement modern security measures and educate in the field of security as part of collaboration within the academic sector, collaboration with the public administration and private and non-profit sectors. For this purpose, the Security Department of the CTU Rector's Office ensures **secure sharing of skills, knowledge, innovation and technologies** with an emphasis on openness and collaboration and compliance with legal and ethical standards.

Key areas of mission:

- Protection of **academic freedom, education and integrity of research**.
- Prevention of and readiness for **emergency situations and security incidents**.
- Ensuring **physical, cyber and information security** of the university and its students, academics and other employees.
- Collaboration with **national and international partners** in security.
- **Transparent and responsible** management of security risks.

Čl. 4 Values

CTU bases its security policy on the following values:

1. **Responsibility** – each member of the university community has their role in the protection of security and integrity of the university.
2. **Transparency** – open communication and clear rules regarding security measures.
3. **Collaboration** – active partnership with state institutions, security forces and the academic community, potentially also with the private and non-profit sector.
4. **Resilience** – emphasis on the prevention of and fast adaptation to new threats, risks and emergencies.
5. **Innovation** – using the latest technologies for the prevention, monitoring and response to security challenges.
6. **Ethics** – a balance between security measures and the freedom of research and education.
7. **Foresight** – setting up efficient mechanisms for regular risk analysis, assessment of potential threats and their prevention, including preparation of scenarios with the possibility to respond instead of implementing reactive measures.
8. **Response** – the ability of flexible and comprehensive response to an emerging situation with an emphasis on minimization of negative impacts.
9. **Respect** – regard for the diversity of thought, cultures and opinions and respect for the individual security needs of each member of the academic community.
10. **Vision** – strategic thinking and long-term planning that allows the university to maintain security stability and competitiveness in the academic and scientific research and education.
11. **Perspective** – following the latest trends, openness to change, implementation of innovative approaches in security, the ability to analyze emerging situations calmly and find effective solutions in emergency situations, including the subsequent evaluation and adoption of necessary measures or improvements.

“P R E V I N T O S O”

Security is not an obstacle – it is a way to success.

Čl. 5 Threats

CTU has identified the following **key security threats**:

- **Physical threats** (active armed attack, terrorism, assault of individuals, theft, vandalism, aggressive behaviour, unauthorized entry to a secured area).
- **Cyber threats** (ransomware, phishing, unauthorized access, DDoS attacks, abuse of personal identity).
- **Targeted influencing** (disinformation, psychological manipulation, intentional misinformation/fake news).
- **Human factors** (negligence, ignorance, insider threats, drug abuse).
- **Natural and technical threats** (fires, floods, blackouts, accidents, infectious diseases).
- **Legal and reputational risks** (non-compliance with legal regulations, damage to goodwill of CTU).

Čl. 6 Protected assets

Key assets of CTU:

- **People** (students, academic workers, outside collaborators).
- **Information assets** (scientific knowledge, personal data, academic and administrative systems).
- **Physical infrastructure** (buildings, laboratories, servers, computer technology).
- **Brand and reputation** (prestige of CTU, ethical standards, legislative compliance).

Čl. 7 Security pillars of the university

To ensure effective protection of the academic community and infrastructure, CTU bases its security strategy on the following pillars:

1. **Physical security**

- Access system and monitoring of campus
- Protection of research laboratories and strategic facilities
- Security measures at public events

2. **Crisis management**

- Emergency plans for physical and digital threats
- Evacuation and crisis plans for students and employees
- Collaboration with security forces and crisis teams

3. **Cybersecurity**

- Protection of IT systems and research data
- Regular security audits and employee training
- Monitoring and prevention of cyber attacks

4. Occupational safety

- Compliance with safety standards at CTU premises, laboratories and classrooms
- Prevention of occupational accidents and health risks
- System of training of occupational safety for employees and students

5. Fire safety

- Fire prevention in university buildings
- Fire evacuation plans, staff training and drill
- Collaboration with the fire department and regular inspections

6. Classified information

- Identification and categorization of classified information
- Access policy for persons with security clearance
- Protection against leakage of sensitive information, in particular within the framework of strategic and defence research

7. Personnel security

- Screening of employee and outside collaborators
- Management of access authorizations
- Measures against insider threats

8. Protection of research

- Categorization of research projects according to security sensitivity
- Measures against industrial and academic espionage
- Compliance with national and international regulations on information protection

9. Collaborations and regulations

- Principles of collaboration with foreign institutions and partners
- Export regulations and protection of technology transfer
- Involvement in international security initiatives

10. Security measures

- Crime prevention and awareness programmes on campus
- Emergency contact line for students and employees
- Mechanisms for reporting security incidents

11. Education and awareness

- Mandatory training in physical and cybersecurity
- Programmes to increase awareness of security and foreign influence operations
- Education and media campaigns to strengthen a safe academic environment

Čl. 8 Tools to ensure security

CTU uses the following **tools to ensure security**:

- **Measures to handle emergencies** (crisis management) and crisis response systems (crisis information systems of CTU – MicroGuard, incident response team, continuity of operation plans).
- **Organizational measures** (security directive, regular audits, access management).
- **Technical measures** (firewalls, antivirus systems, encryption, network monitoring).
- **Education and awareness** (training of employees and students, security workshops).
- **Legal framework** (compliance with GDPR, laws on cybersecurity, internal regulations).

Čl. 9 Strategic goals and measures

Strategic goals (for 2025–2027):

1. Strengthening of the culture of security at CTU – increasing security awareness and responsible conduct of the academic community.

2. Modernization of security technologies used in ensuring security at CTU – implementation of the latest technology standards for the protection of the IT infrastructure and data.

3. Minimization of security risks at CTU through active monitoring and management of security processes.

4. Maintaining compliance with the updated security legislation and regulations – compliance with all relevant laws and regulations on physical, cyber, information security as well as ensuring security of research and development, economic security and property, legislation and regulation security, environmental security.

5. Ensuring protection and defence of research and innovation activities of CTU – prevention of industrial espionage, protection of intellectual property rights and security of research data and knowledge.

Strategic measures (for 2025):

1. Audit of the security system at CTU and testing of individual security measures (penetration tests, security audits).

2. Incorporation of active insurance of security at CTU in the system of management performance at CTU.

3. Optimization of crisis plans for physical and cyber threats.

4. Introduction of regular security training and drills for all employees and students at CTU.

5. Creation of a system of early warning and response to cyber incidents at CTU (establishment of the Security Operations Center (SOC)[1] and Computer Security Incident Response Team (CSIRT)[2] at CTU).

[1] SOC (Security Operations Center) is a centralized role or team responsible for enhancing cybersecurity in an organization and for the prevention of, detection of and response to threats.
[2] CSIRT (Computer Security Incident Response Team) is a general term used for a team that deals with security incidents and response to them, their solution and coordination of solutions.

6. Introduction of measures to strengthen the resilience of CTU to illicit influencing.

7. Preparation and implementation of NIS2[3].

This document provides a basic framework for further development of security strategy at CTU. It defines the key values and pillars of security. It sets out long-term and short-term goals to insure a secure academic environment at CTU. In relation of security at CTU and crisis management, the rector of CTU authorizes the director of the Security Department of the CTU Rector's Office to issue internal standards in the form of strategic measures to strengthen and embed security policy at CTU.

[3] NIS2 (Network and Information Security 2) is a European directive on cybersecurity, i.e. security of information systems, computer networks, applications, software and information.