



Bezpečnostní politika ČVUT

Příkaz rektora č. 4/2025

VIZE

strana: 5

CÍL

strana: 6

STRATEGICKÉ
CÍLE
A OPATŘENÍ

strana: 15

PILÍŘE
BEZPEČNOSTI
UNIVERZITY

strana: 12

NÁSTROJE
PRO ZAJIŠTĚNÍ
BEZPEČNOSTI

strana: 14



Bezpečnostní politika ČVUT

Zpracoval: Bc. Jaroslav Compel, MPA, bezpečnostní ředitel ČVUT v Praze

© České vysoké učení technické v Praze, květen 2025

www.cvut.cz



Obsah

1.	Vize	5
2.	Cíl	6
3.	Poslání	7
4.	Hodnoty	8
5.	Hrozby	10
6.	Chráněná aktiva	10
7.	Pilíře bezpečnosti univerzity	12
8.	Nástroje pro zajištění bezpečnosti	14
9.	Strategické cíle a opatření	15
	Strategická opatření (pro rok 2025):	16

HROZBY

strana: 10

POSLÁNÍ

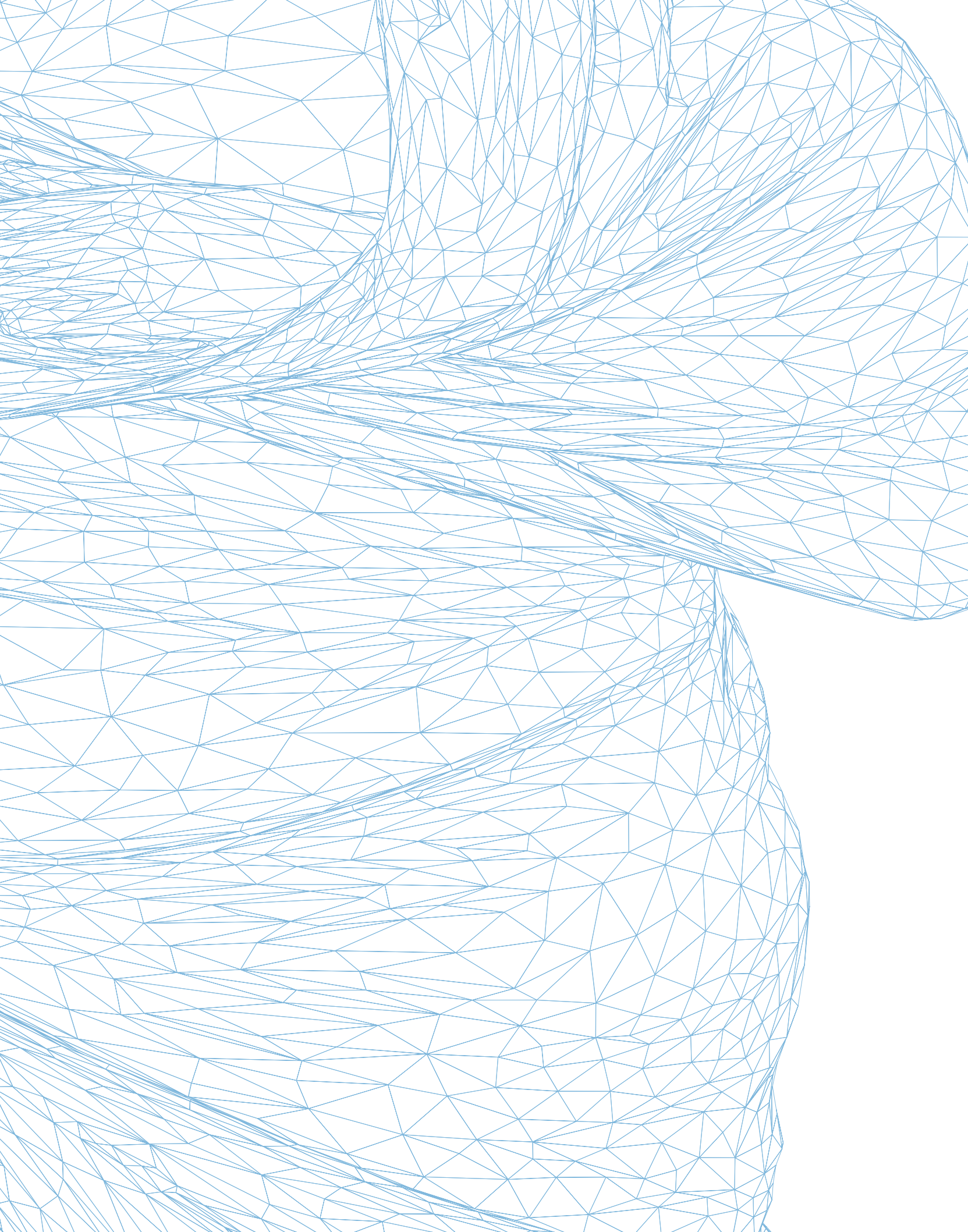
strana: 7

HODNOTY

strana: 8

CHRÁNĚNÁ
AKTIVA

strana: 10





1. Vize

České vysoké učení technické v Praze (ČVUT) vytváří bezpečné akademické prostředí, které podporuje vzdělávání, vědu, výzkum, rozvoj technologií a inovace bez ohrožení integrity, dostupnosti i důvěrnosti osob, informací či infrastruktury univerzity. Hlavní prioritou je ochrana života a zdraví studentů, zaměstnanců a návštěvníků univerzity. Nutností je také zajistit bezpečnost univerzitních objektů a odpovědné nakládání s informacemi ve všech formách.

ČVUT se řídí zásadou, že bezpečnost je klíčovou podmínkou pro svobodné vzdělávání a vědecký pokrok, a dosahuje jí prostřednictvím efektivního a odpovědného řízení bezpečnostních rizik a nastavením moderních preventivních opatření.

Klíčové směry vize:

- Proaktivní přístup k bezpečnostním hrozbám prostřednictvím moderních technologií a analýzy rizik.
- Budování komplexní kultury bezpečnosti, kde studenti, akademici a zaměstnanci rozumějí své roli v ekosystému bezpečnosti univerzity.
- Důraz na osvojování si znalostí a dovedností, tzv. bezpečnostní kompetence studentů, akademiků a zaměstnanců, které budou využitelné v případě krizové situace.
- Zavádění pokročilých bezpečnostních technologií, včetně umělé inteligence a kybernetických obranných mechanismů.
- Posílení institucionální a mezinárodní spolupráce v oblasti akademické bezpečnosti, včetně ochrany duševního vlastnictví a prevence špionáže.
- Ochrana citlivých a strategických výzkumů, které mají vazbu a dopad na národní bezpečnost a ekonomiku a informační prostředí České republiky.



2. Cíl

Cílem je vybudovat a udržovat bezpečnostní kulturu, která zajistí odolnost a ochranu studentů, akademiků, zaměstnanců a partnerů univerzity před fyzickými, kybernetickými i organizačními nebo dalšími hrozbami.

ČVUT chápe bezpečnost jako stav, ve kterém budou bezpečnostní rizika efektivně řízena a minimalizována.



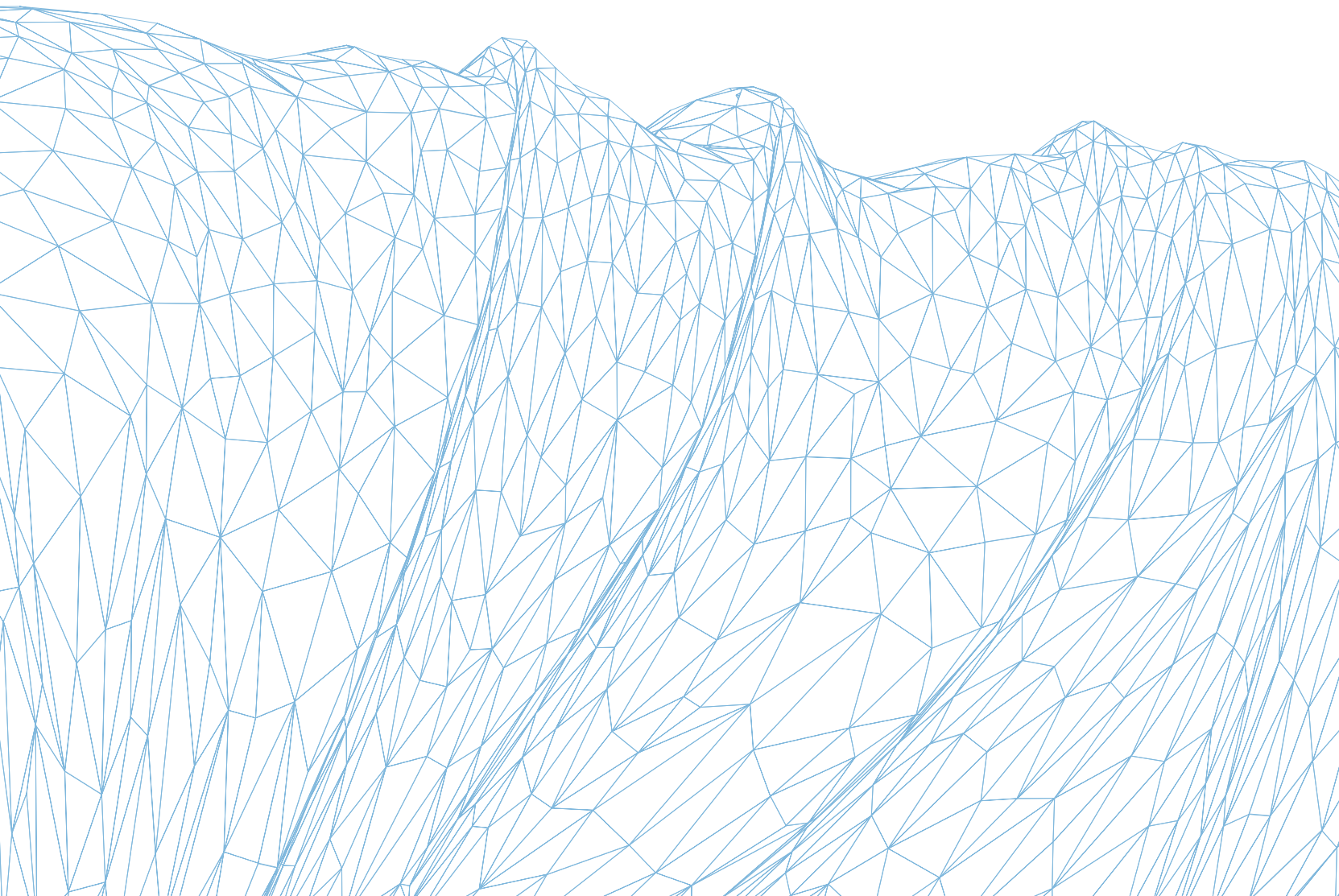


3. Poslání

Posláním odboru bezpečnosti Rektorátu ČVUT a bezpečnostního managementu je chránit akademické prostředí ČVUT pomocí efektivního řízení bezpečnostních rizik, implementovat moderní bezpečnostní opatření a vzdělávat v oblasti bezpečnosti, a to jak při spolupráci v rámci akademického sektoru, tak ve spolupráci se státní správou a soukromým či neziskovým sektorem. Za tím účelem odbor bezpečnosti Rektorátu ČVUT zajišťuje bezpečné sdílení dovedností, znalostí, inovací a technologií s důrazem na otevřenost a spolupráci při dodržování zákonných a etických standardů.

Klíčové oblasti poslání:

- Ochrana akademické svobody, vzdělávání a integrity výzkumu.
- Prevence a připravenost na krizové situace a bezpečnostní incidenty.
- Zajištění fyzické, kybernetické a informační bezpečnosti univerzity a jejích studentů, akademických a dalších zaměstnanců.
- Spolupráce s národními i mezinárodními partnery v oblasti bezpečnosti.
- Transparentní a odpovědné řízení bezpečnostních rizik.



4. Hodnoty

ČVUT staví svou bezpečnostní politiku na následujících hodnotách:



2.

Transparentnost – otevřená komunikace a jasná pravidla v oblasti bezpečnostních opatření.

T

1.

Odpovědnost – každý člen univerzitní komunity hraje svou roli v ochraně bezpečnosti a integrity univerzity.

O

11.

Nadhled – sledování nejnovějších trendů, otevřenost vůči změnám, uplatňování inovativních přístupů v oblasti bezpečnosti, schopnost analyzovat nastalé situace s klidem a hledat efektivní řešení i v krizových situacích, včetně následného vyhodnocení a přijetí potřebných opatření či vylepšení.

N

10.

Vize – strategické myšlení a dlouhodobé plánování, které umožňuje univerzitě udržet si bezpečnostní stabilitu a konkurenceschopnost v oblasti akademického a vědeckého výzkumu a vzdělávání.

V

„PREVINTOSO“

Bezpečnost není překážka –
je to cesta k úspěchu.



3.

Spolupráce – aktivní partnerství se státními institucemi, bezpečnostními složkami a akademickou komunitou, případně soukromým a neziskovým sektorem.

S

4.

Odolnost – důraz na prevenci a rychlou adaptaci na nové hrozby, rizika a krizové situace.

O

5.

Inovace – využití nejmodernějších technologií pro prevenci, monitorování a reakci na bezpečnostní výzvy.

I

6.

Etika – rovnováha mezi bezpečnostními opatřeními a svobodou výzkumu i vzdělávání.

E

7.

Předvídavost – nastavení efektivních mechanismů pro pravidelnou analýzu rizik, vyhodnocování potenciálních hrozeb a jejich prevence, včetně vypracování scénářů s možnostmi reakce namísto reaktivních opatření.

P

8.

Reakce – schopnost pružné a komplexní reakce na nastalou situaci s důrazem na minimalizaci negativních dopadů.

R

9.

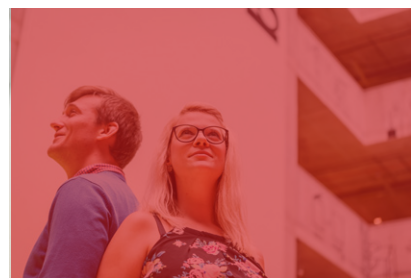
Respekt – úcta k diverzitě myšlenek, kultur a názorů a zároveň respekt k individuálním bezpečnostním potřebám každého člena akademické obce.

R

5. Hrozby

ČVUT identifikuje následující klíčové bezpečnostní hrozby:

- Fyzické hrozby (aktivní ozbrojený útok, terorismus, napadení osob, krádeže, vandalismus, agresivní chování, neoprávněný vstup do zabezpečených prostor).
- Kybernetické hrozby (ransomware, phishing, neoprávněný přístup, DDoS útoky, zneužití osobní identity).
- Cílené ovlivňování (dezinformace, psychická manipulace, záměrné zkreslování/fakenews).
- Lidské faktory (nedbalost, neznalost, insider threats, drogová závislost).
- Přírodní a technické hrozby (požáry, povodně, výpadky energie, havárie, infekční onemocnění).
- Právní a reputační rizika (nedodržení legislativních předpisů, poškození dobrého jména ČVUT).



6. Chráněná aktiva

Klíčová aktiva ČVUT:

- Lidé (studenti, akademičtí pracovníci, zaměstnanci, externí spolupracovníci).
- Informační aktiva (vědecké znalosti, osobní údaje, akademické a administrativní systémy).
- Fyzická infrastruktura (budovy, laboratoře, servery, výpočetní technika).
- Značka a reputace (prestiž ČVUT, etické zásady, legislativní compliance).



7. Pilíře bezpečnosti univerzity

Pro zajištění efektivní ochrany akademické komunity a infrastruktury ČVUT staví svou bezpečnostní strategii na následujících pilířích:

1.

Fyzická bezpečnost

- Přístupový systém a monitoring kampusu
- Ochrana výzkumných laboratoří a strategických objektů
- Bezpečnostní opatření pro veřejné akce

2.

Krizové řízení

- Nouzové plány pro fyzické i digitální hrozby
- Evakuační a krizové plány pro studenty a zaměstnance
- Spolupráce s bezpečnostními složkami a krizovými týmy

3.

Kybernetická bezpečnost

- Ochrana IT systémů a výzkumných dat
- Pravidelné bezpečnostní audity a školení zaměstnanců
- Monitoring a prevence kybernetických útoků

4.

Bezpečnost práce

- Dodržování bezpečnostních norem v prostorách ČVUT, laboratořích a učebnách
- Prevence pracovních úrazů a zdravotních rizik
- Systém školení v oblasti bezpečnosti práce pro zaměstnance i studenty



5.

Požární bezpečnost

- Prevence požárů v budovách univerzity
- Požární evakuační plány, školení cvičení personálu
- Spolupráce s hasičským sborem a pravidelné inspekce

6.

Utajované informace

- Identifikace a kategorizace utajovaných informací
- Přístupová politika pro osoby s bezpečnostní prověrkou
- Ochrana před únikem citlivých informací, zejména v rámci strategických a obranných výzkumů

8.

Ochrana výzkumu

- Kategorizace výzkumných projektů podle bezpečnostní citlivosti
- Opatření proti průmyslové a akademické špionáži
- Soulad s národními a mezinárodními předpisy o ochraně informací

7.

Personální bezpečnost

- Prověřování zaměstnanců a externích pracovníků
- Řízení přístupových oprávnění
- Opatření proti vnitřním hrozbám (insider threats)

9.

Spolupráce a regulace

- Zásady spolupráce se zahraničními institucemi a partnery
- Exportní regulace a ochrana technologického transferu
- Zapojení do mezinárodních bezpečnostních iniciativ

10.

Bezpečnostní opatření

- Programy prevence kriminality a osvěty na univerzitní půdě
- Nouzová kontaktní linka pro studenty a zaměstnance
- Mechanismy pro hlášení bezpečnostních incidentů

11.

Vzdělávání a osvěta

- Povinná školení v oblasti fyzické a kybernetické bezpečnosti
- Programy pro zvýšení povědomí o bezpečnosti a vlivového působení cizí moci
- Osvěta a mediální kampaně pro posílení bezpečného akademického prostředí



8. Nástroje pro zajištění bezpečnosti

ČVUT využívá následující nástroje pro zajištění bezpečnosti:

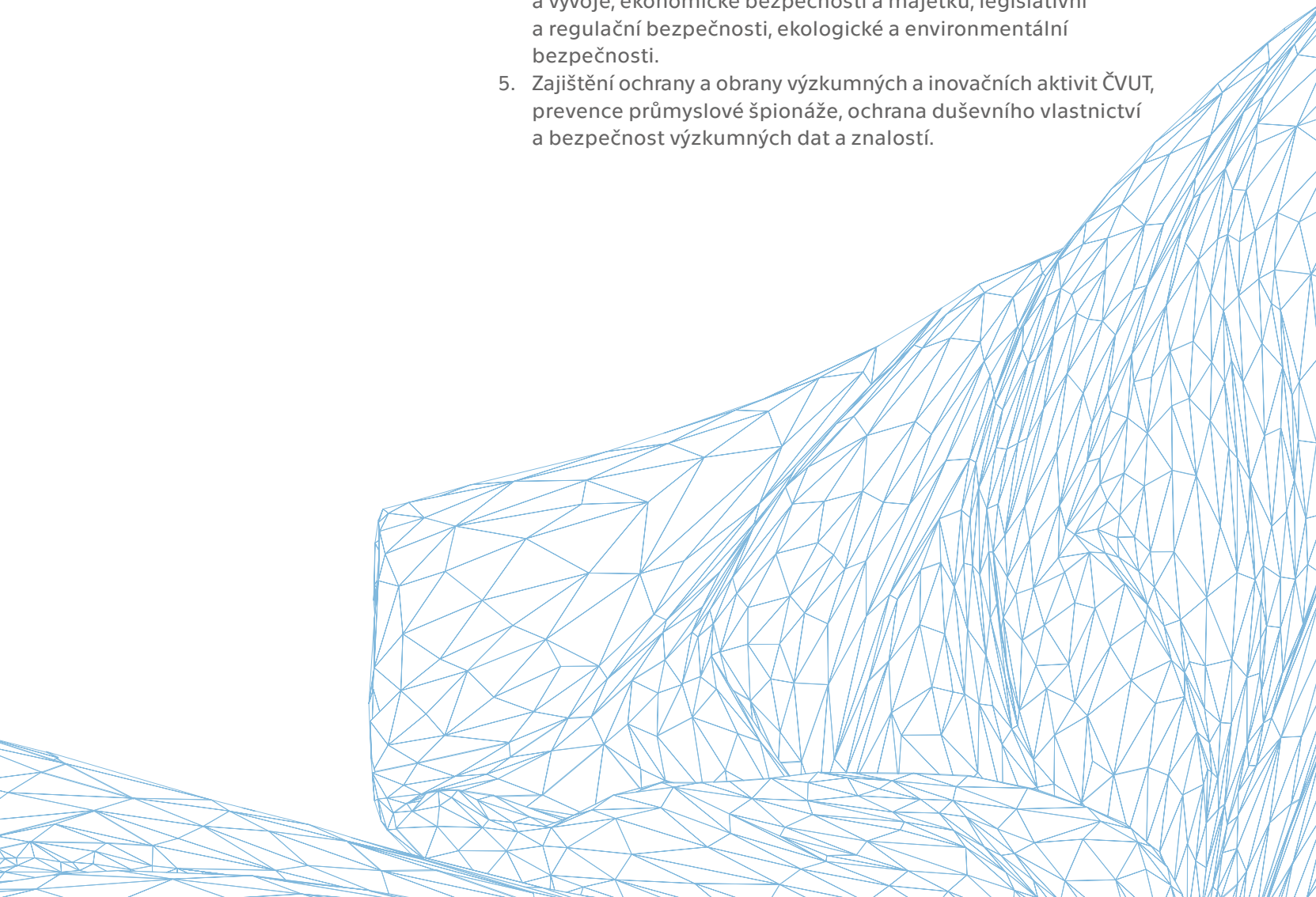
- Opatření k zvládnutí mimořádných situací (krizové řízení) a systémy reakce na krize (systém krizového vyrozumění ČVUT – MicroGuard, incident response team, plány kontinuity provozu).
- Organizační opatření (bezpečnostní směrnice, pravidelné audity, řízení přístupů).
- Technická opatření (firewally, antivirové systémy, šifrování, monitoring sítě).
- Vzdělávání a osvěta (školení zaměstnanců a studentů, bezpečnostní workshopy).
- Právní rámec (dodržování GDPR, zákonů o kybernetické bezpečnosti, interních předpisů).



9. Strategické cíle a opatření

Strategické cíle (pro období 2025–2027):

1. Posílení bezpečnostní kultury ČVUT – zvýšení bezpečnostního povědomí a odpovědného chování široké akademické obce.
2. Modernizace bezpečnostních technologií v oblasti zajišťování bezpečnosti ČVUT – implementace nejnovějších technologických standardů pro ochranu IT infrastruktury a dat.
3. Minimalizace bezpečnostních rizik v rámci ČVUT prostřednictvím aktivního monitoringu a řízení bezpečnostních procesů.
4. Udržování souladu s aktuální bezpečnostní legislativou a regulacemi – dodržování všech relevantních zákonů a nařízení týkajících se nejenom fyzické, personální, kybernetické, informační bezpečnosti, ale i zajištění bezpečnosti výzkumu a vývoje, ekonomické bezpečnosti a majetku, legislativní a regulační bezpečnosti, ekologické a environmentální bezpečnosti.
5. Zajištění ochrany a obrany výzkumných a inovačních aktivit ČVUT, prevence průmyslové špionáže, ochrana duševního vlastnictví a bezpečnost výzkumných dat a znalostí.



Strategická opatření (pro rok 2025):

1. Audit bezpečnostního systému ČVUT a otestování jednotlivých bezpečnostních opatření (penetrační testy, bezpečnostní audity).
2. Zahrnutí aktivního zajišťování bezpečnosti ČVUT do systému výkonu managementu ČVUT.
3. Optimalizace krizových plánů pro případy fyzických a kybernetických hrozeb.
4. Zavedení pravidelného bezpečnostního školení a nácviku reakce pro všechny zaměstnance a studenty ČVUT.
5. Vytvoření systému včasného varování a reakce na kybernetické incidenty v rámci ČVUT (vznik Security Operations Center (SOC)¹ a Computer Security Incident Response Team (CSIRT)² ČVUT).
6. Zavedení opatření k posílení odolnosti ČVUT vůči nelegitimnímu ovlivňování.
7. Příprava a implementace NIS2³.

Tento dokument poskytuje základní rámec pro další vytváření bezpečnostní strategie ČVUT. Definuje klíčové hodnoty a pilíře bezpečnosti. Nastavuje dlouhodobé i krátkodobé cíle pro zajištění bezpečného akademického prostředí v rámci ČVUT. Ve vztahu k bezpečnosti ČVUT a krizovému řízení, pověřuje rektor ČVUT ředitele odboru bezpečnosti Rektorátu ČVUT vydáváním interních norem v rozsahu strategických opatření k posílení a ukotvení bezpečnostní politiky ČVUT.

V Praze dne 1. 5. 2025



Bc. Jaroslav Compel, MPA
bezpečnostní ředitel ČVUT v Praze

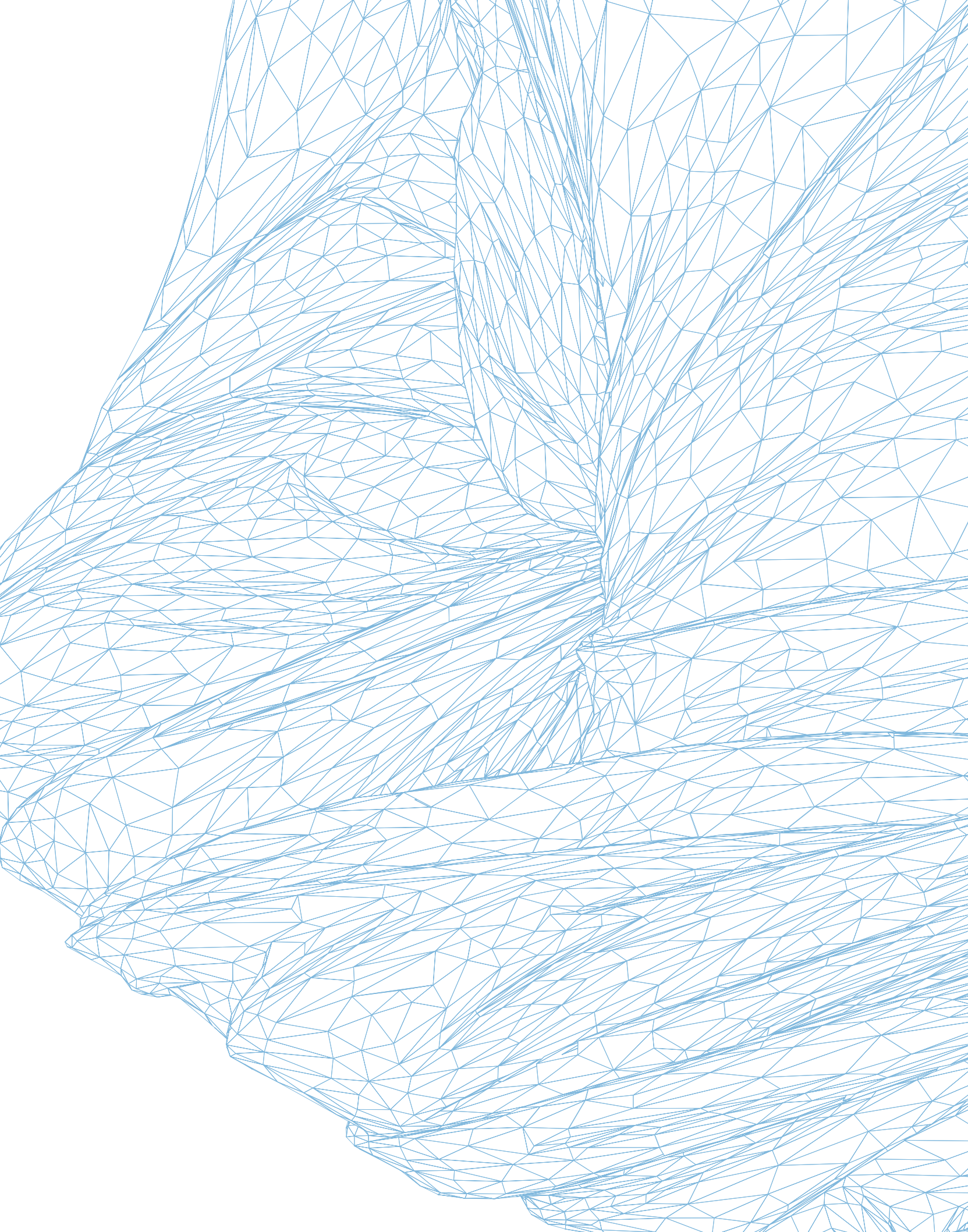


doc. RNDr. Vojtěch Petráček, CSc.
rektor ČVUT v Praze

¹/**SOC** (Security Operations Center) je centralizovaná funkce nebo tým zodpovědný za vylepšování stavu kybernetické bezpečnosti v organizaci a za prevenci, detekci a reakci na hrozby.

²/**CSIRT** (Computer Security Incident Response Team) je obecný termín pro označení týmu, který se v rámci své působnosti zabývá bezpečnostními incidenty, reakcí na ně (RESPONSE), jejich řešením a koordinací jejich řešení.

³/**NIS2** (Network and Information Security 2) je celoevropská směrnice o kybernetické bezpečnosti, tedy bezpečnosti informačních systémů, počítačových sítí, aplikací, software a informací.



01000010

01100101

01111010

01110000

01100101

01100011

01101110

01101111

01110011

01110100

00100000

01101110

01100101

01101110

01101001

00100000

01110000

01110010

01100101

01101011

01100001

01111010

01101011

01100001



**ODBOR
BEZPEČNOSTI
ČVUT V PRAZE**