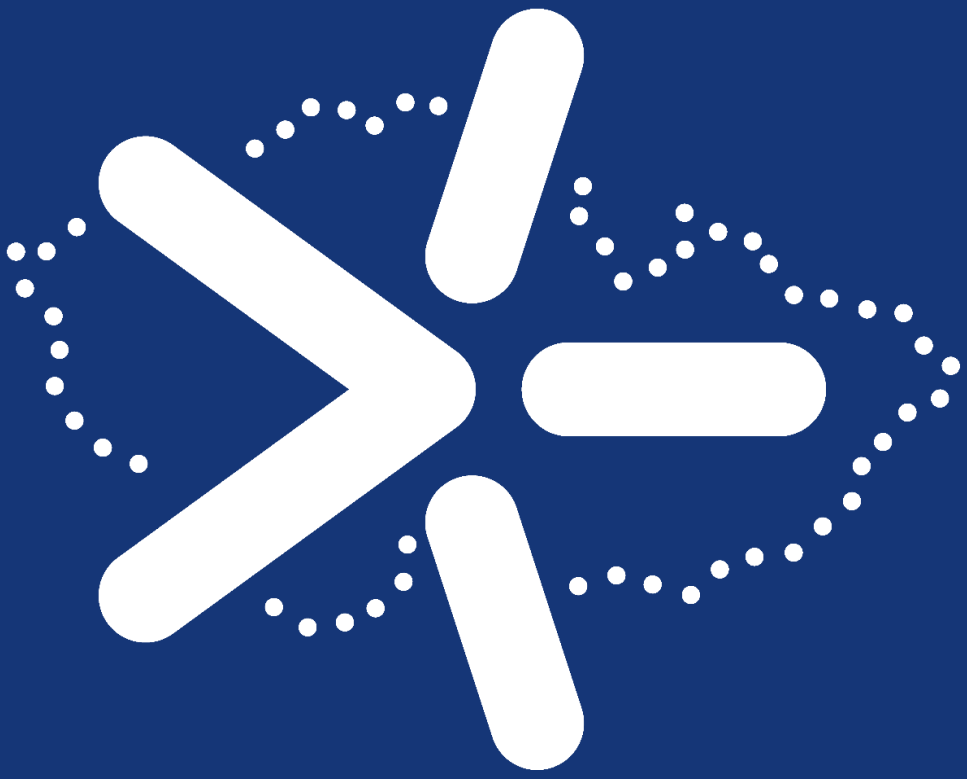

Soubor doporučení pro ověřování identity a monitoring průběhu ověřování znalostí vysokoškolských studentů v online prostředí, včetně SZZ.

VUT v Brně
Centrum výpočetních a informačních systémů

Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Projekt NPO C2 se zaměřuje na bezpečnost distančních forem výuky. Jeho cílem je systematicky zajistit komplexní bezpečnost distančního vzdělávání, a to jak z technického, tak i procesního hlediska. Projekt vychází z existujících doporučení, standardů a metodik. Náleží do specifického cíle C2 v rámci Národního plánu obnovy 2022-2024, jeho účastníky jsou všechny veřejné vysoké školy v ČR, koordinátorem je ČVUT. Hlavními úkoly jsou analýza a výběr vhodných komponent "kolaborativní platformy", pod kterou se rozumí všechny komponenty zajišťující nástroje pro online a hybridní výuku (studijní informační systém, např. IS MU, IS STAG, e-learningový systém (Moodle), komunikační platforma(Microsoft 365)), zabezpečení procesního a technického provázání distanční formy výuky, a nastavení bezpečného předávání a uchovávání studijních dokumentů.

VUT v Brně se zapojilo do projektu NPO, cíle C2 zaměřeného na bezpečnost distančních forem výuky, s dílčím cílem definovat ve spolupráci s dalšími vysokými školami vznikne soubor doporučení pro ověřování identity a monitoringu průběhu ověřování znalostí vysokoškolských studentů v online prostředí. V rámci tohoto dílčího cíle proběhla analýza výchozího stavu ověřování identity a monitoringu průběhu ověřování znalostí vysokoškolských studentů v online prostředí, a následně k posouzení využití souboru doporučení pro ověřování identity a monitoringu průběhu ověřování znalostí vysokoškolských studentů v online prostředí.

V průběhu realizace byly vyhodnocovány výstupy pracovních skupin projektu, které byly sdíleny napříč řešiteli zapojených vysokých škol.

Cíl 8: Analýza řešení a postupů integrace vhodných metod ověřování identity a monitoring průběhu online zkoušek, včetně SZZ (např. proctoring):

- v prostředí Moodle (používá VUT). Proběhlo vlastní ověřování a analytické práce předložených možností – konfigurace proctoringu v testu, PDC proctoring z pohledu studenta, PDC proctoring z pohledu učitele, další možnosti PDC proctoringu, administrace a technická stránka PDC proctoringu. Aktivní vs. neaktivní proctoring.
- v rámci provedených analýz jsme si zajistili cenovou nabídky na implementaci proctoringu, kterou v rámci studie proveditelnosti nerealizovali vůči vysokým nákladům s pořízením tohoto rozšíření,
- plně distanční podoba zkoušení, a to včetně státních závěrečných zkoušek aktuálně na VUT ve velkém poštu neprobíhá, což byl jeden ze zásadních rozhodujících aspektů pro nepořízení proctoringu,

- formu proctoringu jsme ale i přesto implementovali v kombinaci intagrace dolpňku Safe exam browser a Teams online videa, kdy doplněk dočasně zamkne zařízení proti jinému použití než je vyplnění testu a online video zajistí zkoušejícímu přehled, jestli není test vyplňovaný proti pravidlům,
- implementace této kombinace je jedním z našich doporučení, jak k zabezpečení online zkoušení přistoupit,
- VUT má novou pracovní silou na Odboru podpory a testování zajištěnou systémovou podporu evidence účastníků distanční formy a nejen pro ně,
- dále má VUT kompletní databázi těchto účastníků, se kterými aktivně pracuje i v rámci informačního systému, se kterým je Moodle propojen,
- integrace řeší i evidenci o absolvování kurzů jednotlivými účastníky,
- v rámci bezpečnosti zajištění přístupů k jednotlivým materiálům jsme vyvinuli jednotnou autentizační infrastrukturu, na kterou je Moodle napojen, aby se daná osoba přihlašovala do všech systémů pod jednotnou identitou a my ji tak mohli mapovat napříč celým informačním systémem, včetně Moodle,
- jednotná autentizační infrastruktura nám zároveň rozšířila zabezpečení o druhý faktor,
- v prostředí MS365 probíhaly schůzky pracovní skupiny, vyhodnocování získaných podnětů v rámci univerzitního prostředí a systémů VUT

Doporučení:

1. **Autentizace uživatelů**
- Používání silného hesla a multifaktorovou autentizaci (MFA) pro přihlašování.
- Pravidelně měňte hesla a vyžadujte od studentů, aby své hesla měnili také.

2. **Nastavení zkoušek:**
- Využívání časového omezení pro dokončení zkoušky.
- Náhodné generování pořadí otázek a odpovědí pro každého studenta.
- Používání velké databáze otázek a generování unikátní sady otázek pro každého studenta.
- Zvažení použití otevřených a uzavřených otázek, aby bylo těžší otázky sdílet.

3. **Proctoring (dohled nad zkouškou):**
- Implementování nástroje pro online proctoring, který může monitorovat studenty prostřednictvím webkamer, mikrofonů a sdílení obrazovky. V našem případě doporučení na Teams.
- Upozornění studentů na to, že budou monitorováni, a vysvětlit jim, jak proctoring funguje.

4. **Technická opatření:**
- Nastavení omezení prohlížení webu během zkoušky, pokud to systém dovoluje. V našem případě doporučení na Safe exam browser.
- Pravidelně aktualizovat Moodle nebo jiné LMS na nejnovější verzi kvůli aplikování bezpečnostních záplat.

5. **Ověření identity:**
- Při přihlašování ke zkoušce vyžadovat ověření totožnosti (například prostřednictvím studijního průkazu nebo jiné formy identifikace). Je totiž možné, že test nevyplňuje student, který je do systému přihlášen.

6. **Logování a sledování aktivit:**
- Aktivování logování aktivit v Moodle, aby bylo možné sledovat, kdy se studenti přihlásili, které otázky odpovídali a jak dlouho trvalo dokončení zkoušky.
- Analyzovat logy na podezřelé chování nebo neobvyklé vzorce.

7. **Školení a informovanost:**
- Poskytování školení pro studenty a učitele ohledně bezpečných praktik při online zkouškách.
- Informování studentů o důsledcích podvádění a o opatřeních, která jsou zavedena k ochraně integrity zkoušek.
- Implementování těchto opatření může výrazně přispět k bezpečnosti a férovosti online zkoušek v Moodle.