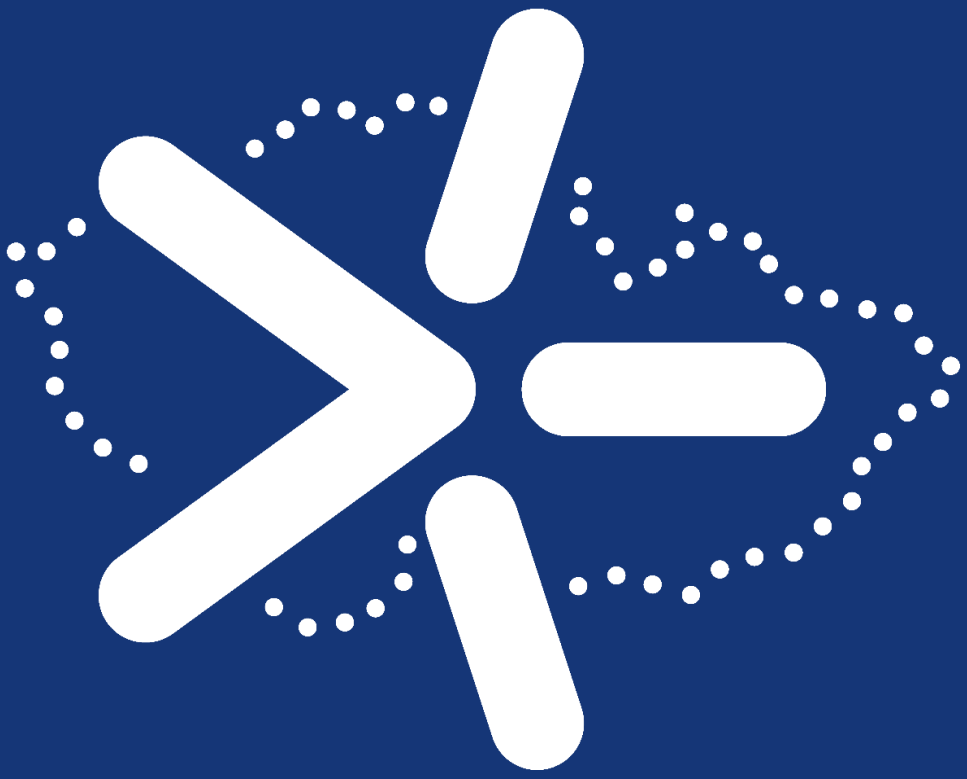

# VÝSTUP Č. 8 ČZU

## Soubor požadavků na ověření původu předávaných či uchovávaných dokumentů.

Cíl: Stanovení požadavků na ověření původu předávaných či uchovávaných studijních dokumentů.

Pracovní skupina 3 – NPO C2
Ing. Petr Vlachynský

https://www.planobnovycr.cz/

Financováno Evropskou unií
NextGenerationEU

# Obsah

1. Úvod ..... 2
2. Studijní dokumenty ..... 2
3. Původ studijních dokumentů ..... 3
4. Elektronické dokumenty v SIS a prokazatelnost jejich původu ..... 4
5. Elektronický podpis/razítko/pečeť ..... 6
6. Klasifikace dokumentů ..... 7
7. Technická specifikace úložiště ..... 10
8. DLP v rámci SIS a kolaborativní platformy ..... 12
9. Konverze dokumentů ..... 13
10. Ověření pravosti diplomů ..... 14
11. Zahraniční spolupráce ..... 15



Financováno Evropskou unií
NextGenerationEU

# 1. Úvod

Výstup č. 15 slouží jako soubor procesních a technických požadavků na ověření původu předávaných či uchovávaných studijních dokumentů. Zaměřeno je na základní parametry zabezpečení dokumentů, se kterými se univerzity mohou setkat ve své každodenní práci ve studijním informačním systému.

Výstup je mapován na cíl č. 17 projektu Národního plánu obnovy, specifického cíle 2 a byl vypracován pracovní skupinou 3.

Součástí výstupu je také evidence dokumentů, související se zahraniční spoluprací, která je vydána jako samostatná excelová tabulka.

# 2. Studijní dokumenty

Pro určení studijních dokumentů využijeme definici z Výstupu č. 13 pracovní skupiny 3 projektu NPO-C2, která zní takto:

*Studijní dokumenty lze pro účely tohoto výstupu chápat jako záznamy událostí souvisejících s jednotlivými studenty a jejich studiem na VVŠ. Tyto dokumenty byly v tradičním pojetí uchovávány v listinné podobě v tzv. „složce studenta".*

Pojem studijní dokumenty může být v současnosti poněkud matoucí, neboť mimo tradiční písemnosti zahrnuje také data, která jednotlivé události zaznamenávají ve studijních informačních systémech (SIS), obvykle ve formě databázových záznamů. Typickým příkladem jsou záznamy o absolvovaných zkouškách. Z těchto dat vznikají dokumenty (listiny) převážně v reakci na konkrétní žádosti studentů (např. potvrzení o studiu, výpis studijních výsledků apod.) nebo v případě, kdy univerzita vystupuje vůči studentovi jako orgán veřejné moci, a forma dokumentu je určena stylem oficiální komunikace (např. rozhodnutí o ukončení studia).

Studijní dokumenty mohou obecně zahrnovat tyto typy dokumentů:

- Záznamy o výsledcích studia
- Sylaby
- Diplomy



Financováno Evropskou unií
NextGenerationEU

- Životopisy a motivační dopisy
- Přijímací dokumenty
- Učební plány a programy
- Potvrzení o studiu
- Dokumenty o stipendiích a finanční podpoře studia

Kompletní výčet studijních dokumentů je ve zpracované tabulce z výstupu č. 13 vypracovaného pracovní skupinou 3 projektu NPO-C2 a také v náhledu níže. Významným zdrojem pro uchovávání studijních dokumentů je Studijní informační systém (SIS).

| ID | Název dokumentu | Vystavuje | Rozhodovací pravomoc | Pro koho určen | Využití | Proces vystavení | Evidence souvisejících dat | Ochrana | Skartační znak | Typ dokumentu |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Přehled o výsledku studia** | Studijní oddělení - referentka studia; SIS - self service | - | Student, Zahraniční student, Státnicová komise | Výpis o výsledku studia určený zejména pro studenty - uznání studia. Interní kontrola/přehled. | Na vyžádání - studijní oddělení. Self service - student v SIS, také v případě ukončení studia jako záloha | SIS | Fyzický/elektronický podpis referenta, čas.razítko. Self service - bez validace. | S1 | Výpis |
| 2 | **Výpis studijních výsledků - Transcript of Records** | Zahraniční oddělení, Studijní oddělení - referentka. | - | Stážisti (pro vyjíždějící studenty/zahraniční stážisty) | Dokument o složení předmětů. | Na vyžádání - referentka. | SIS | Fyzický/eklektronický podpis referenta | S1 | Výpis |
| 3 | **Potvrzení o průběhu studia** | Studijní oddělení, SIS - self service student | - | Student - Státní orgány (úřad práce, cizinecká policie, zdravotní pojišťovna) | Potvrzení o průběhu studia - program, forma, jazyk výuky, období aktivního a neaktivního studia apod. | Na vyžádání - studijní oddělení. Self service - student v SIS | SIS | Fyzický/elektornický podpis referenta. Self service - elektornická pečeť. | S1 | Potvrzení |
| 4 | **Potvrzení o studiu - k důchodovému pojištění** | Studijní oddělení | - | Student - pro ČSSZ | Potvrzení o odstudované době studia | Na vyžádání - studijní oddělení, self service - student v SIS | SIS | Pečeť, časové razítko | S1 | Potvrzení |
| 5 | **Potvrzení o ukončení studia** | Studijní oddělení | - | Student - Státní orgány (úřad práce, cizinecká policie, zdravotní pojišťovna) | Potvrzení o ukončení studia. | Vydání při zanechání studia na základě prohlášení studenta (Rozhodnutí z vlastní vůle - prohlášení DZ případně v listinné podobě) | SIS | Fyzický/elektornický podpis | S1 | Potvrzení |
| 6 | **Rozhodnutí o ukončení studia / Potvrzení o** | Studijní oddělení, SIS - self service student | - | Student | Potvrzení o ukončení studia. | Vydání na základě úspěšného ukončení studia. Uloženo ve složce studenta | SIS | Elektronická pečeť, časové razítko | S45 | Rozhodnutí |

Obrázek 1 Studijní dokumenty Výstup č. 13 NPO-C2

## 3. Původ studijních dokumentů

Původ studijních dokumentů je určen tím kdo dokument vytvořil a kdy byl vytvořen. Ověření původu dokumentu je proces, kterým se zjišťuje, zda dokument byl vytvořen osobou, která tvrdí, že ho vytvořila, a zda byl vytvořen v době, kterou tvrdí, a zda byla tato osoba oprávněna dokument vytvořit.

Pro ověření původu studijních dokumentů se používají různé metody, jako například ověření podpisu, ověření pečeti, ověření autenticity dokumentu, ověření jeho obsahu a další.

Je důležité, aby ověření původu dokumentu bylo provedeno spolehlivým způsobem, aby bylo zajištěno, že dokument je skutečný a že nebyl pozměněn. Zde narážíme na základní pilíř informační bezpečnosti, a to důraz na integritu.



Financováno Evropskou unií
NextGenerationEU

# 4. Elektronické dokumenty v SIS a prokazatelnost jejich původu

Verzování dokumentů slouží k zachování historie změn provedených v určitém časovém úseku na dokumentu. Verzování může být považováno za pokročilejší způsob zálohování, záloha pravidelně (např. 1x denně) zkopíruje stav dokumentu i v případě, že nedojde ke změnám. Naproti tomu verzování vyvolá uložení dokumentu ve chvíli, kdy dojde k jeho změně. Zálohování tedy nemusí obsahovat všechny změny dokumentu v čase, kdežto verzování by mělo změny v daném časovém úseku zachovat[1]. V praxi se obvykle kombinují oba přístupy, kdy zálohování slouží k prevenci před havárií, a verzování pro editační účely. To znamená, že k obnově ze zálohy mají přístup administrátoři systému, naproti tomu verzování je obvykle dostupné všem uživatelům oprávněným dokument upravovat. Oprávnění uživatelé obvykle mají možnost procházet historii verzí dokumentů. Vrátit se k starší verzi dokumentu má primárně vlastník dokumentu.

Nejdůležitější vlastnosti verzování jsou:

• Automatická správa a identifikace verzí – správné číslování verzí (revizí).

• Identifikace kdo, kdy a jakým způsobem konkrétní část dokumentu změnil.

• Podpora spolupráce editorů – tzn. např. zobrazení v reálném čase, který editor a na které části dokumentu právě provádí změny.

• Verzování má další nároky na úložiště – je třeba vytvořit tzv. repositář změn. Jeho kapacita limituje počet verzí, které se zpětně uchovávají.

• Různé systémy mají různou politiku uchovávání historie verzí, např. cloudová úložiště uchovávají typicky 30 dnů zpět nebo 100 verzí zpět.

• Většinou verzování neuchovává kopie celého dokumentu ale pouze rozdíly dokumentu oproti předchozí verzi.

• Používají se dva způsoby přístupu k verzování:

o Zamykání souborů – jeden editor zamkne dokument a může provádět změny, ostatní smí jen číst, dokud editor dokument neuvolní.

[1] https://www.rug.nl/digital-competence-centre/it-solutions/it-security/backup-versioning



Financováno Evropskou unií NextGenerationEU

- Slučování verzí – souběžné editování bez zamykání, vhodné pouze pro dokumenty s jednoduchou strukturou. Hrozí kolize při současné změně ve stejné části.

V současné době se lze s verzováním dokumentů setkat v mnoha systémech uložení dat. Nejčastěji se používá:

- Síťová úložiště serverů (např. ShadowCopy u Microsoft Windows Serveru)
- Cloudové služby – MS Office 365 OneDrive, SharePoint, GoogleDrive, DropBox, aj.
- Privátní cloudové systémy – OwnCloud
- Document Management Systémy (DMS)

Verzování je vhodný doplněk systému periodického zálohování. Periodická záloha dat může sloužit jako základ ochrany dat, a systém verzování tuto zálohu vhodně doplňuje o možnost vrátit se k jakékoli verzi určitého dokumentu v nedávné historii (např. Microsoft Volume Shadow Copy Service [2]).

Auditování a logování jsou veškeré operace související s činnostmi všech účtů (tj. nejenom běžných, ale i privilegovanějších, např. přidání/odebírání rolí nebo členství ve skupinách) musí být auditovány a tyto auditní události musí být časově synchronizovány a uloženy v nezměnitelné podobě nejméně po nezbytně dlouhou dobu z důvodu provedení auditního šetření v případě možného vzniknuvšího bezpečnostního incidentu[3]. Podle § 22 Vyhlášky o kybernetické bezpečnosti 82/2018 Sb., je veřejná vysoká škola jako orgán veřejné moci ve smyslu provozování významného informačního systému povinna uchovávat záznamky událostí nejméně po dobu 12 měsíců.

[2] https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service

[3] https://nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf



Financováno Evropskou unií
NextGenerationEU

## 5. Elektronický podpis/razítko/pečeť

K zajištění integrity dokumentu, deklarace času vytvoření či autentizace proklamované identity autora dokumentu se v případě elektronických dokumentů používají následující nástroje.

Elektronický podpis

V případě podepisování elektronických dokumentů je doporučeno používat Kvalifikovaný elektronický podpis, který je ekvivalentem úředně ověřeného podpisu. Používá se k zaručení identity autora či odpovědné osoby za obsah dokumentu. Digitální podpis také poskytne informaci, zda jsou data v té podobě, ve které byla podepsána. K vytvoření Kvalifikovaného elektronického podpisu je zapotřebí vystavení kvalifikovaného certifikátu uznávanou certifikační autoritou, při jehož vydání dochází k ověření totožnosti žadatele.

Časové razítko

Tento nástroj zaručuje, že uvedená data v elektronické podobě existovala v určitý časový okamžik v dané podobě. Časové razítko tedy slouží k zaručení integrity, kdy k elektronickému podpisu přidává časovou deklaraci toho, zda uvedená data vypadala při aplikování razítka. Používá se také k archivaci dokumentu, jelikož prodlužuje platnost dokumentu s elektronickým podpisem o 5 let. Časové razítko lze takto na dokument aplikovat opakovaně a je proto možné daný dokument archivovat téměř nekonečně dlouho.

Elektronická pečeť

Elektronická pečeť představuje ekvivalent razítka organizace. Pečetí zajistíme informaci o tom, že se jedná o oficiální dokument dané organizace. Certifikát pro elektronickou pečeť je možné vydat pouze zástupci právnické osoby. Ve spojení s elektronickým podpisem a časovým razítkem vytváří ideální kombinaci, která zaručí, že daný dokument opravdu pochází z konkrétní organizace, byl vytvořen konkrétním, ověřeným, uživatelem a jaká byla jeho přesná podoba v daný čas aplikace časového razítka. Tato kombinace ochranných prvků nám zajistí původ i integritu elektronického dokumentu.



Financováno Evropskou unií
NextGenerationEU

## 6. Klasifikace dokumentů

Klasifikace informací, potažmo dokumentů tyto informace obsahujících, je základním předpokladem pro úspěšné vynucování pravidel bezpečnosti informací. Klasifikace informací je obvykle prováděna pomocí 3 a více klasifikačních stupňů, které odrážejí důvěrnost informací v dokumentech obsažených, přičemž jako základní lze považovat stupně:

- **Veřejné** (informace volně přístupné mimo organizace)
- **Interní** (informace přístupné zaměstnancům organizace)
- **Důvěrné** (informace určené konkrétním (skupinám) příjemcům)
- **Kritické** (informace, jejichž únik by mohl závažně poškodit organizaci)

Některé organizace stupeň kritický, zejména ve vztahu ke studijním dokumentů nedefinují, Detailnější vysvětlení klasifikačním stupňům vycházející z materiálů NÚKIB[4] a jejich spojení s konkrétními studijními dokumenty lze nalézt v následující tabulce:

| **Úroveň důvěrnosti** | **Klasifikační stupeň** | **Obecný popis** | **Relevantní pro studijní dokumenty** |
|---|---|---|---|
| Nízká | Veřejné informace | Informace jsou buď veřejně dostupné, nebo byly určeny k zveřejnění. Tyto informace mohou být dále poskytovány a šířeny bez omezení. Porušení důvěrnosti informací neohrožuje zájmy organizace nebo osoby. | Např. sylaby, studijní plány |
| Střední | Interní | Informace, které tvoří know-how organizace. Nejsou veřejně dostupné a jejich ochrana není vyžadována žádným právním předpisem nebo smluvním ujednáním. Tyto informace | Záznamy o výsledcích studia, diplomy, |

[4] https://nukib.gov.cz/download/publikace/podpurne_materialy/Ploha%205%20-%20Vzorov%20pravidla%20ochrany%20jednitlivch%20rovn%20aktiv.pdf

| | | | |
|---|---|---|---|
| | | mohou být sdíleny v rámci organizace a s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejné kanály. Při předání informací musí být zajištěna důvěrnost komunikace. Pro ochranu důvěrnosti informací musí být využívány prostředky pro řízení přístupu. | |
| Vysoká | Důvěrné | Informace, které nejsou veřejně dostupné, jsou chráněny právními předpisy, nebo smluvními ujednáními, například se jedná o osobní údaje. Tyto informace mohou být sdíleny pouze s osobami, kterým byly poskytnuty, a s partnery, kteří splňují need-to-know. Informace nesmí být poskytnuta jiným osobám. Pro ochranu důvěrnosti informací jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí musí být chráněny pomocí kryptografických prostředků. Zálohy by měly být zabezpečeny fyzicky nebo alespoň zaheslovány. | OÚ studenta, žádosti o stipendia, žádosti s přiloženými zdravotními dokumenty, potvrzení o speciálních potřebách studenta, žádost o individuální studijní plán apod. |
| Kritická | Kritické | Informace, které nejsou veřejně dostupné, vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie. Tyto informace nesmí být poskytnuty jiné osobě než té, které | - |



Financováno Evropskou unií
NextGenerationEU

| | | | |
|---|---|---|---|
| | | byla informace určena, pokud nebyly výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. Pokud příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace. Pro ochranu důvěrnosti informací musí být využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále musí být použity metody ochrany, které zabraňují zneužití informací ze strany administrátorů. Přenosy informací musí být chráněny pomocí kryptografických prostředků. | |

Je důležité si uvědomit, že klasifikační stupně jsou definovány ve vztahu k důvěrnosti. Vzhledem k významu jednotlivých dokumentů je třeba zachovat individuální požadavky na dostupnost; požadavky na integritu, které přímo souvisí s původem studijních dokumentů (viz. kapitola 3) nejsou klasifikačním stupněm ovlivněny.

Základním předpokladem pro to, aby byly informace úspěšně chráněny je označení dokumentů klasifikačním stupněm. Klasifikace může být jak manuální, provedená autorem dokumentu, tak automatická (poloautomatická) na základě charakteristik a informací, které jsou v dokumentu obsaženy (např. osobní údaje, rodné číslo, nadpis dokumentu atp.). Organizace obvykle vynucují výchozí úroveň klasifikace pro dokumenty, které nebyly klasifikačním stupněm opatřeny na stupni interní. Ve všech případech je pak klasifikace zodpovědností vlastníka dokumentu. Pro zajištění dostatečné úrovně důvěrnosti je zásadní stanovení parametrů ukládání, předávání a následné lividace dokumentů.



Financováno Evropskou unií
NextGenerationEU

## 7. Technická specifikace úložiště

Datová úložiště pro centrální služby z pohledu typu zařízení a výkonu technologie spadající do serverových a síťových úložišť s určitou úrovní fyzického a výkonového zabezpečení. Významnou kapitolou je také zabezpečení dat na jejich ztrátu, retence dat nebo doba obnovy do běžného provozu od chvíle, kdy jsou data nenávratně ztracena z běžného provozního prostředí. Dále lze data rozdělovat podle toho jaké jsou důležitosti nebo jak rychle mají být dostupná a mimo jiné také pro jaké množství lidí tato data prezentujeme ve stejný moment. Tedy jak je s daty aktivně a dynamicky nakládáno na aplikační úrovni.

Fyzické a geografické zabezpečení dat je jedním ze základních kamenů bezpečnosti dat. Datové zdroje instituce patří mezi nejvíce ceněné informační zdroje, které organizace má. Důležitost je zdůvodnitelná především pro jejich nenahraditelnost v případě ztráty nebo zcizení. Data jsou v centrálních úložištích ukládány dle pravidel „3,2,1“. Nejjednodušší interpretace pro tento způsob nakládání s daty je uložení informace na tři samostatné kopie, ve dvou místech, která jsou oddělena určitou racionální vzdáleností a jednou kopií, která by měla být mimo běžné provozní prostředí tedy „mimo systém“.

Z pohledu fyzické bezpečnosti jsou data centrálně uchovávána v místech k tomu určených. Takováto místa jsou serverovny nebo datacentra s fyzickou bezpečností na takové úrovni, aby bylo zamezeno přístupu k fyzickému médiu nebo zařízení. Tato místa jsou monitorována, zabezpečena elektronickým zabezpečovacím systémem, hlídána kamerovým systémem, platí pro ně také s omezením kartového přístupu a musí být mechanicky odolná vůči pokusům o vniknutí, krádež a vandalismu.

Na úrovni geografického rozmístění jsou data vždy minimálně na dvou geograficky rozdílných místech s tím, že obě místa jsou v zásadě vybavena tak, aby pracovala jako autonomní celek. V oblasti centrálních úložišť je nejčastějším způsobem výstavba datových úložišť ve formě clusteru čítající minimálně dvě zcela autonomní zařízení. Na tato zařízení se aplikuje tzv. režim synchronní replikace dat, aby ve stejný moment byla na obou zařízeních uložena stejná data. Tím je zajištěna vysoká dostupnost a schopnost ukládat data v reálném čase. V posledních letech je také běžné aplikovat pokročilé funkce pro optimalizaci dat za účelem jejich redukce ve smyslu velikosti nebo objemu. Pro účely redukce velikosti jsou



Financováno Evropskou unií
NextGenerationEU

zavedena komprimovaná data pomocí algoritmů pro redukci dat. Druhý způsob je možnost data deduplikovat, což reálně způsobuje snížení objemu dat, na pokud možno minimální počet identických kopii stejného datového souboru.

Z pohledu nároků na výkon, jak lze data prezentovat pro odpovídající počty uživatelů jsou centrální úložiště odstupňována co do výkonu a typu diskového prostoru. Nejrychleji pracující jsou disková úložiště bez mechanických částí (SSD a NVME). Plně vybavené all-flash úložiště jsou bohužel ještě pořád relativně drahá, a proto se disková úložiště nadále kombinují s pomalejšími, ale levnějšími mechanickými disky. Tento typ zařízení aplikuje tzv. TIER storage zásady a dovoluje data dle toho, jak jsou často jsou vyžadována umístit do rychlého úložiště, a naopak data v méně častém až pasivním režimu lze odkládat na pomalejší diskové kapacity.

Poslední instance záchrany a bezpečnosti dat je záloha na médium mimo provozní systémy organizace za pomocí software pro tvorbu záloh a jejich spuštění při obnově. Jako dosud nejčastější médium pro ukládání dat jsou již mnoho let využívány magnetické pásky. Jejich výhodou je cena a ověřená bezpečnost uložených dat. Zásadní nevýhodou je jejich nemožnost z pásky v reálném čase efektivně číst a zálohy je obvykle nutné ukládat na diskové úložiště pak s časovou stopou jednorázově zabalit a uložit v jenom kuse na pásku. Z důvodů různých nároků na obnovu dat jsou data také zálohována podle různých politik. Příklad možného zálohování:

- denní záloha na deduplikační storage MediaAgent2
- denní synchronize na pásku LTO7, retence 30 dnů
- selektivní kopie 13ti týdenních full backupů na pásku LTO7, retence 92 dnů
- selektivní kopie 12ti měsíčních backupů na pásku LTO8, retence 1 rok
- selektivní kopie 10ti ročních backupů na pásku LTO8, retence 10 let
- 1x týdně syntetická full záloha (Neděle v 8:00)
- 1x denně inkrementální záloha (denně v 21:45)

Ukázka obnovy systému (RTO = Recovery Time Objective) – odhad v čase

1. Obnova z diskové kopie

Objem obnovených dat: 129.68 GB

Čas potřebný k obnově: 35 minut

2. Obnova z LTO kopie



Financováno Evropskou unií
NextGenerationEU

Objem obnovených dat: 129.68 GB

Čas potřebný k obnově: 5 hodin a 41 minut

Zálohovací politiky pro ukázku:

1. 14DaysToWSSSDS-CVMAXXX-30DaysToLTO8

Po 14 dní od začátku zálohovací úlohy jsou data uložena na diskovém úložišti "DiskStorageWSSSDS-CVMAXXX". Po 30 dní od začátku zálohovací úlohy na diskové úložiště jsou data v kopii uložena na LTO médiu.

2. 5YearsTo(WSSSDS-CVMAXXX)LTO7

Po 0 dní od začátku zálohovací úlohy jsou data uložena na diskovém úložišti "DiskStorageWSSSDS-CVMAXXX". Po 1825 (=5 let) dní od začátku zálohovací úlohy na diskové úložiště jsou data v kopii uložena na LTO médiu.

## 8. DLP v rámci SIS a kolaborativní platformy

DLP systémy jsou specifická řešení, která pomocí bezpečnostních pravidel-politik chrání data na základě obsahu souborů (content) nebo jejich původu (context). Zpravidla dochází k označení-klasifikaci dat, nad nimiž jsou uplatněny zmíněné politiky, nebo jsou data označena na principu dynamického prohledávání citlivých informací uvnitř souborů a v obsahu komunikace.

Microsoft365 nabízí řadu nástrojů pro ochranu dat, včetně Data Loss Prevention (dále také jen „DLP"). DLP je služba, která pomáhá organizacím, včetně vysokých škol, detekovat potenciální úniky dat a zabránit jim při neoprávněném nebo chybném zaslání mimo skupinu uživatelů, kteří by měli mít přístup k těmto datům, a to monitorováním a ochranou citlivých informací. Microsoft služba DLP poskytuje inteligentní detekci a kontrolu citlivých informací napříč aplikacemi Office 365, OneDrive, SharePoint, Microsoft Teams a také na koncových zařízeních.

Microsoft Purview Data Loss Prevention je cloudové řešení, které nabízí snadné nasazení, použití a škálovatelnost. Pomáhá předcházet rizikovému nebo neoprávněnému použití citlivých dat na aplikacích, službách a zařízeních. Pomáhá předcházet neoprávněnému sdílení, přenosu nebo použití citlivých informací napříč aplikacemi, službami a zařízeními.



Financováno Evropskou unií
NextGenerationEU

Pokud chcete chránit svá data, můžete zvážit následující doporučení:

- Identifikujte citlivá data a určete, kdo má k nim přístup.
- Vytvořte politiku pro ochranu dat, která určuje, jaká data jsou citlivá a jak se k nim má přistupovat.
- Použijte nástroje pro detekci a prevenci ztráty dat
- Vytvořte plán pro řešení incidentů, pokud dojde k úniku dat.

## 9. Konverze dokumentů

Konverze (často také autorizovaná konverze) je proces převodu dokumentů z fyzické (tištěné) podoby do digitální a naopak. Konverzí se rozumí úplné převedení dokumentu způsobem zajišťující shodu předloženého dokumentu a jeho konvertované, což je potvrzeno připojením doložky o provedení konverze. Doložka o provedení konverze se připojuje ke každému nově vzniklému dokumentu. Současně se také ukládá do centrálního úložiště ověřovacích doložek. Dokument, který provedením konverze vznikl tak má stejné právní účinky jako původní dokument, jehož převedením výstup vznikl.

Ověřovací doložka je výstupem procesu konverze elektronických dokumentů a podle § 69a Zákona č. 499/2004 Sb., o archivnictví a spisové službě musí obsahovat:

- Označení osoby, která konverzi provedla společně s elektronickým podpisem
- Identifikační číslo ověřovací doložky
- Počet listů, který obsahuje převedený dokument
- Informaci o viditelném prvku, který není možné plně převést na dokument v digitální podobě
- Datum vyhotovení ověřovací doložky

Ověřením autenticity vydané autorizované konverze lze pomocí identifikačního čísla vystavené ověřovací doložky. Přesné specifika tohoto ověření se mohou lišit u dodavatele služby například u doby uchování těchto doložek. Služby jako CzechPoint nebo spisové služby třetích stran disponují vlastními produkty pro provedení elektronické konverze dokumentů a doložky o provedení konverze se ukládají v úložištích poskytovatele/dodavatele.



Financováno Evropskou unií
NextGenerationEU

Dokument, který vznikl převodem z fyzické podoby, musí být opatřen platným kvalifikovaným elektronických podpisem nebo kvalifikovanou elektronickou pečetí, které je možné vystavit u certifikačních autorit (v ČR jde o CzechPoint, 1. Certifikační autorita a EIdentity).Je však třeba konstatovat, že služba elektronické konverze negarantuje, že fyzický dokument, který byl vstupem pro konverzi nebyl pozměněn.

Jak již bylo několikrát zmíněno, konverze elektronických dokumentů je spjata se spisovou službou napojenou na studijní informační systém.

IS/STAG vyvíjen ZČU podporuje aktuálně 6 systémů spisové služby, ke kterým je externě napojen. Konverzi si pak spisová služba řeší samostatně.

IS MUNI naopak podporuje vlastní systém spisové služby, tudíž konverzi podporuje v balíčku společně se studijním informačním systémem. Tento systém podporuje konverzi dokumentů z moci úřední v souladu se Zákonem č. 300/2008 Sb., o elektonických úkonech a autorizované konverzi dokumentů, včetně konverzí, které jsou prováděny automatizovaně. Systém je řešen vlastní službou, která je napojena na rozhraní systému CzechPoint.

UIS má momentálně podle dostupných informací možnost napojení na systémy spisové služby ICZ group a AthenA u vysokých škol ČZU, respektive VŠE.

## 10. Ověření pravosti diplomů

V rámci naplnění požadavku §47b zákona č. 111/1998 Sb., o vysokých školách, musí vysoká škola nevýdělečně zveřejňovat bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba. Způsob zveřejnění pak stanoví vnitřní předpis každé vysoké školy. Jedním z možnosti naplnění požadavku je například služba PravyDiplom.cz, vyvíjený a provozovaný Masarykovou univerzitou. Ostatní veřejné vysoké školy se mohou zapojit a připojit k tomuto projektu, který garantuje snadné a rychlé ověření diplomu online.

Uživatelé i školy importují údaje ve formátu XML o svých vydaných diplomech ze systému školy a následně se poloautomatizovaně nahrají do systému PravyDiplom přes zabezpečený šifrovaný přenos dat, je tedy obtížné je modifikovat či odposlechnout během transferu. Základní principy integrity a důvěrnosti jsou dodrženy.



Financováno Evropskou unií
NextGenerationEU

Služba je alternativou k osobnímu ověření diplomu, které bylo doposud možné pouze při návštěvě dané VVŠ a fakulty. Údaje, které si žadatel u ověření zobrazí vychází pouze z rozhodnutí konkrétní VVŠ a nastavení systému. Výchozí hodnotou pro vyhledávání je číslo diplomu, jméno a příjmení. Výstupní hodnoty se pak mohou lišit od pouhého potvrzení, že diplom je pravý až po zobrazení URL na závěrečnou práci studenta.

## 11. Zahraniční spolupráce

Během procesu výjezdu do zahraničí v rámci projektu Erasmus, ale i mimo něj vznikají studijní dokumenty, které jsou často evidované jiným způsobem, než dokumenty vznikající v rámci běžného studia. Tyto dokumenty mohou vznikat ve dvou jazykových variantách, a to v češtině a angličtině. Studijní dokumenty pro potřeby tohoto projektu nezahrnují veškeré materiály, které slouží jako podpora vzdělávání (skripta, prezentace, záznamy přednášek, aj.), slouží pro potřeby akreditace (sylaby předmětů, struktura studijního programu/oboru).

Z pohledu instituce se setkáváme s dvěma procesy týkajících se studijních dokumentů. Jeden z nich je vytváření studijních dokumentů a druhý proces je jejich ověřování. K oběma procesům jsou níže vypsaná doporučení, která vycházejí ze zjištěných skutečností ohledně skutečného stavu na ČZU.

V rámci tohoto výstupu byla vytvořena evidence, která obsahuje veškeré zjištěné studijní dokumenty, které jsou relevantní v procesu přijíždějících a vyjíždějících studentů v rámci zahraničních pobytů. Tato evidence obsahuje tyto informace:

- ID dokumentu
- Název dokumentu
- Kdo jej vystavuje
- Program spolupráce
- Postavení univerzity
- Rozhodovací pravomoc u dokumentu
- Pro koho je určen
- Využití
- Proces vystavení
- Evidence souvisejících dat



Financováno Evropskou unií
NextGenerationEU

- Ochrana dokumentu
- Skartační značka
- Typ dokumentu

Evidence je volně dostupná jako součást výstupu a může být upravena pro potřeby jednotlivých vysokých škol. Všechny zjištěné informace jsou vázány na testovanou univerzitu a nemohou být považovány za garanci správnosti pro všechny vysoké školy. Evidence tak slouží jako ukázkový materiál a inspirace pro ostatní veřejné vysoké školy.

Vytváření studijních dokumentů

Ve velké míře vznikají studijní dokumenty na ČZU elektronicky a jsou opatřené kvalifikovaným elektronickým podpisem zodpovědné osoby. Dokument tedy obsahuje informace potvrzující obsah a identifikuje osobu, která dokument vytvořila či je za vznik a obsah dokumentu zodpovědná, což zajišťuje zachování integrity dokumentu. Zároveň jsou dokumenty, u kterých je potřeba, aby vznikaly ve fyzické podobě, např. dokumenty potřebné pro vízový proces vyžaduje ministerstvo vnitra zasílat ve fyzické podobě poštou.

Ověřování studijních dokumentů

Proces ověřování dokumentu lze chápat jako ověření původu a zda se jeho obsah po vytvoření nezměnil. Tyto vlastnosti lze u elektronických dokumentů zajistit elektronickým podpisem. Kdy elektronický podpis zajišťuje identifikaci osoby, která je za obsah dokumentu zodpovědná a zároveň zajišťuje integritu tj., že se obsah dokumentu od podepsání nezměnil. Proto v rámci ověřování původu a zachování integrity elektronických dokumentů dochází k ověření elektronického podpisu. Elektronické dokumenty bez elektronického podpisu nelze z pohledu integrity a původu dokumentu ověřit. Proto by z pohledu bezpečnosti neměly být dokumenty v této formě uznány. Instituce by si měla vyžádat dokumenty s elektronickým podpisem či v jiné formě např. zaslání dokumentů ve fyzické podobě s úředně ověřenými podpisy poštou.

K ověření původu, pravosti a integrity fyzických dokumentů slouží procesy jako Superlegalizace, Apostila a notářské či úřední ověření podpisu. Pro dokumenty v jiném než českém či anglickém jazyce je student/zájemce o studium povinen zřídit úředně ověřený překlad.



Financováno Evropskou unií
NextGenerationEU

V procesu ověřování v rámci studia se setkáme také s ověřováním totožnosti, které probíhá při zápisu do studia. Student/zájemce o studium je povinen předložit platný doklad totožnosti (občanský průkaz v rámci zemí EU, či pas).

Uznání předchozího zahraničního vzdělání

Existují různé dohody mezi státy, které upravují podmínky uznávání vzdělání. Příkladem může být Smlouva mezi Českou republikou a Slovenskou republikou o vzájemném uznávání rovnocennosti dokladů o vzdělání vydávaných v České republice a ve Slovenské republice (Praha, 28.11.2013, publikována pod č. 23/2015 Sb.m.s., platná od 28.3.2015):

- Nová právní situace při principu právní kontinuity zachovává stav, Česká republika stejně jako Slovenská republika považují vysokoškolské vzdělání a vysokoškolské diplomy, vydané po dobu od rozdělení České a Slovenské Federativní Republiky (tj. od 1. ledna 1993), i po vstupu Smlouvy v platnost po 28. březnu 2015 za nedotčené a uznávají je obecně vzájemně za rovnocenné, a to automaticky (bez dalšího řízení).

Podobné smlouvy či dohody platí také mimo jiné pro Polsko, Německo, Maďarsko a Slovinsko. Jedná se ale o uznání vzdělání jako takového, nesmíme zapomínat na nutnost ověření původu a integrity samotných dokumentů.

V rámci programu Erasmus je pod záštitou Evropské unie zřízena platforma Erasmus Without Papers, která zprostředkovává předávání elektronických dokumentů mezi, do programu zapojenými, institucemi. Elektronické dokumenty předávané prostřednictvím této platformy jsou opatřeny elektronickými podpisy, což zajišťuje původ i zachování integrity dokumentů.



Financováno Evropskou unií
NextGenerationEU