Jak bezpečně nakládat s daty

Obsah

1. Účel dokumentu

Cílem tohoto dokumentu je návrh klasifikace dat, s nimiž přicházejí do styku studenti a zaměstnanci UK. Dokument současně poskytuje přehled nejčastějších úložišť dat a předkládá doporučení vhodnosti jejich použití.

Dokument je věnován běžně zpracovávaným datům, se kterými se zaměstnanci a studenti setkávají ve výzkumu, při zajištění provozních a administrativních činnostech univerzity či v rámci výuky.

Dokument se pouze okrajově věnuje práci s vysoce citlivými daty (zdravotnická dokumentace apod.), vysoce cennými daty, kde hrozí finanční škody při jejich zničení či úniku (výzkumná data s vysokou finanční hodnotou, data vysokého strategického významu z hlediska národních a bezpečnostních zájmů státu apod.). Ve všech těchto případech je nutné postupovat individuálně a pro volbu vhodného úložiště dat zpracovat samostatnou analýzu.

Data utajovaná ze zákona jsou zcela mimo rámec tohoto dokumentu a je u nich třeba postupovat podle specifických pravidel.

2. Bezpečnost uložených dat

Při práci s daty řešíme dva základní bezpečnostní problémy:

- ochranu dat před vyzrazením neoprávněné osobě
- ochranu dat před neoprávněnou či nechtěnou modifikací a ztrátou.

2.1 Ochrana dat před vyzrazením neoprávněné osobě

Chráníme se zde před „krádeží dat hackery“, zkopírovaní dat náhodným nálezcem flash disku, zneužitím dat zlodějem notebooku apod.

Ochranou je v první řadě volba odpovídajícího úložiště pro daný typ dat, dále používání přihlašovacích hesel pro přístup k datům, omezení přístupu k souborům pomocí přístupových práv, ochrana dat šifrováním apod.

Šifrování dat

Šifrování dat může být efektní způsob ochrany uložených dat před jejich zpřístupněním neoprávněným osobám. Je však nutné zvážit rizika spojená se ztrátou (de)šifrovacího klíče – nástroje pro šifrování dat mohou od koncového uživatele vyžadovat, aby se vlastními silami postaral o zálohování šifrovacích klíčů / hesel pro případ jejich ztráty, což může být proces vyžadující nadstandardní technické znalosti.

Bez dešifrovacích klíčů / hesel přitom nebude možné data jakkoliv obnovit! Zároveň však zpřístupnění dešifrovacích klíčů / hesel (např. jejich zálohy) neautorizované osobě ohrožuje účinnost šifrování jako prostředku ochrany dat.

Z důvodu komplikovanosti správy hesel / šifrovacích klíčů, doporučujeme pro ukládání dat využívat ta úložiště, která pro danou kategorii dat šifrování nevyžadují.

2.2 Ochrana dat před modifikací či ztrátou

Bráníme se zde ztrátě dat z důvodu nechtěného nebo úmyslného smazání / změně obsahu souboru, selhání úložiště s daty v zařízení, vyděračskému zašifrování/smazání dat počítačovým virem apod.

Opět je důležitá volba vhodného úložiště, respektive úložišť, která sama o sobě mohou obsahovat mechanismy chránící před ztrátou dat.

Obecnými metodami ochrany jsou zálohování dat (uložení více kopií stejných souborů na různá, na sobě nezávislá, úložiště) a dlouhodobé držení jejich historických kopií, mazání „do koše“, používání pokročilých úložišť s integrovanou ochranou dat (např. uložení v cloudu, uložení na profesionálních datových serverech používajících redundantní uložení) apod.

Zálohování dat

Vždy ověřte, zda a jak Vámi zvolené datové úložiště řeší zálohování dat. Bez definovaného procesu pravidelné zálohy vždy existuje riziko ztráty dat nehledě na zvolený typ úložiště. To se týká i profesionálních datových úložišť a cloudů, pokud si zálohování dat nesjednáte explicitně v rámci rozšířených SLA služeb.

3. Kategorizace dat

Kategorie dat	***Popis***	***Příklady***
Veřejná data	Data zpřístupnitelná komukoliv bez jakýchkoliv omezení, např. veřejně vystavena na internetu. Jejich zveřejnění nepředstavuje žádné ohrožení pro UK nebo jiné instituce či osoby.	• veřejně přístupné výzkumné zprávy a výzkumná data • open-source software • propagace • veřejné informace o službách
Interní data	Data určená jen pro vnitřní potřebu obecně definované skupiny osob (např. spolupracovníci projektu, pracovníci instituce apod.). Nevyžadují však zvláštní regulaci nebo ochranu (ze zákona, dle smlouvy apod.). Zpřístupnění mimo danou skupinu nezpůsobí přímou škodu (finanční, morální, právní apod.).	• interní korespondence • zápisy z jednání • vnitřní směrnice a předpisy • nepublikované výzkumné zprávy
Diskrétní data	Data určená výhradně pro vnitřní potřebu přesně definované skupiny osob (např. zaměstnanec a jeho přímý nadřízený, pracovník HR oddělení a uchazeč o zaměstnání, skupina správců IT systému s administrátorskými právy k němu). Vyžadují ze své povahy regulaci nebo ochranu, typicky jsou data chráněná ze zákona nebo na základě nějaké smlouvy/licence (jedná se např. o osobní údaje osob, data spadající pod obchodní tajemství apod.). Zpřístupnění mimo danou skupinu osob velmi pravděpodobně způsobí škodu (finanční, morální, právní apod.).	• ekonomické a personální údaje osobní povahy • osobní údaje studentů, zaměstnanců, spolupracovníků • čísla identifikačních průkazů, rodná čísla apod. • čísla kreditních karet • cenná výzkumná data (poskytující např. konkurenční výhodu) • rozsáhlé kolekce interních dat • přístupové údaje (např. hesla či šifrovací klíče) k málo významným systémům a interním datům

Citlivá data	Data určená striktně jen pro vnitřní potřebu přesně definované skupiny osob (např. zdravotník a jeho pacient, řešitelé projektu pracující s daty podléhajícími komerčnímu či podobnému tajemství apod.). Vyžadují ze své povahy zvláštní regulaci nebo obzvláštní ochranu, typicky jsou data přísně chráněná ze zákona nebo na základě smlouvy/licence (jedná se např. o velmi cenná data spadající pod obchodní tajemství, citlivé osobní údaje apod.). Zpřístupnění mimo danou skupinu oprávněných osob velmi pravděpodobně způsobí škodu (finanční, morální, právní apod.) velkého rozsahu se závažnými a nevratnými následky. V univerzitní praxi do této kategorie spadají jen některá data.	• zdravotní data, citlivé osobní údaje • velmi cenná výzkumná data (poskytující např. unikátní a těžko opakovatelnou konkurenční výhodu) nebo výzkumná data obsahující vysoce důvěrné údaje • rozsáhlé kolekce diskrétních dat • přístupové údaje (např. hesla či šifrovací klíče) k důležitým systémům a datům kategorie diskrétní nebo citlivá

4. Kategorizace úložišť

4.1 Přenosná média

Flash disky, paměťové karty, externí HDD/SSD, CD, DVD, … tj. externí paměťová média, která nejsou pevnou součástí žádného zařízení a uživatelé je používají k přenášení informací mezi různými zařízeními nebo pro dočasné uložení dat.

Na co si dát pozor

Přenosná média jsou typicky přenášena z místa na místo. Snadno mohou být ponechána bez dozoru či ztracena na veřejných místech, kde hrozí jejich krádež a následné zneužití/zveřejnění uložených dat.

U těchto médií je také velmi obtížné zjistit, zda nedošlo k neautorizovanému přístupu k datům (např. kolega si z flash disku zkopíruje nejen prezentaci z konference, kvůli které jsme mu flash disk půjčili, ale také ostatní soubory, které jsou na disku uložené).

Tato úložiště neobsahují prakticky žádné ochranné mechanismy proti ztrátě dat (vícenásobné uložení, automatické kontroly uložených dat apod.), takže z důvodu selhání média mohou být data na nich uložená snadno a bez varování ztracena. Proto nejsou vhodná jako jediné primární úložiště dat, ale jen pro uložení druhé nebo další kopie.

4.2 Lokální disky

a) V počítačích a noteboocích

Disky pevně zabudované ve stolních počítačích/noteboocích v majetku univerzity (typicky interní HDD/SSD apod.). Jedná se o zařízení přístupná v prostorách univerzity, v kancelářích zaměstnanců, ve studovnách apod. Každé zařízení musí mít definovaného správce (administrátorský účet), a je řádně zabezpečeno (aktualizace,

antivir,…). Typicky je spravováno odborníky IT oddělení fakult a součástí, kteří zajišťují a monitorují jejich bezpečný provoz.

Tato úložiště jsou vhodná pro data, ke kterým je nutný rychlý lokální přístup přímo na daném počítači a není nutné je sdílet s jinými osobami nebo je zpracovávat na více různých zařízeních. Lze je využívat také v případě omezeného nebo žádného připojení k internetu (tzv. práce off-line).

Na co si dát pozor

Aby se zabránilo neautorizovanému přístupu k datům, je třeba důsledně dbát na omezení přístupu k uživatelskému/administrátorskému účtu (přihlašovací hesla apod.), na správné nastavení přístupových práv a dodržovat zásady fyzické bezpečnosti, zejména nenechávat bez dozoru běžící počítač bez „uzamčení obrazovky" (kde je to možné, zamykat kancelář v nepřítomnosti uživatele počítače) apod.

Uložení dat na běžných PC/NB neposkytuje prakticky žádné ochranné mechanismy proti jejich ztrátě (vícenásobné uložení, automatické kontroly uložených dat apod.), takže z důvodu selhání zařízení mohou být data na nich uložená snadno a bez varování ztracena. Lokálně uložená data, která potřebujeme dlouhodobě zachovat, je proto nutné chránit před ztrátou zálohováním (např. na přenosné médium, na síťové nebo cloudové úložiště apod.).

Speciální upozornění pro NB

Zvláštní pozornost je třeba věnovat přenosným počítačům – notebookům. Snadno mohou být ponechány bez dozoru nebo zapomenuty na veřejných místech, čímž hrozí zvýšené riziko jejich krádeže a následné ztráty/zneužití uložených dat.

Z hlediska ztráty dat je u přenosných počítačů riziko o to vyšší, že jsou při transportu a používání na cestách vystaveny vyšší zátěži (vibrace, prach, nárazy, velké změny teplot, …), což zvyšuje pravděpodobnost selhání lokálního úložiště dat.

b) V jiných mobilních zařízeních

Datová úložiště pevně zabudovaná v mobilních zařízeních, tj. mobilních telefonech, tabletech apod. (typicky interní nevyjímatelná paměť, v zařízení instalovaná paměťová karta apod.) v použití zaměstnanců/studentů.

Protože tato zařízení jsou často využívána současně pro pracovní i osobní účely a zpravidla nejsou spravována příslušnými IT odděleními fakulty/součásti, nelze je k ukládání pracovních ani vědeckých dat z bezpečnostních důvodů doporučit.

Na co si dát pozor

Mobilní zařízení jsou uživateli často využívána jako společné zařízení pro pracovní i osobní účely. Je třeba proto dbát zvýšené opatrnosti, aby pracovní data nebyla omylem uložena na osobní cloudové úložiště.

Dle charakteru uložených dat je nutno používat na zařízení zámek obrazovky, tj. ochranu přístupu k funkcím zařízení „vzorem", PINem, heslem či otiskem prstu, který zabrání tomu, aby mohl se zařízením a daty v něm volně pracovat každý, kdo se k zařízení náhodně dostane.

Zvýšenou pozornost je třeba věnovat také instalaci podvodných nebo „zavirovaných" aplikací. I zdánlivě neškodná aplikace, např. počítačová hra instalovaná pro osobní zábavu, může získat přístup k pracovním datům. Na potenciálně škodlivou aplikaci mohou ukazovat například nesmyslně rozsáhlé požadavky na přístupová práva aplikace. Proto je doporučeno využívat výhradně aplikace z oficiálních zdrojů (Google Play, Apple App Store apod.).

Velkým problémem bezpečnosti mobilních zařízení je péče o jejich zabezpečení ze strany výrobců. Pokud výrobce neposkytuje včasné softwarové opravy bezpečnostních problémů operačního systému apod., nemusí být koncový uživatel přes veškerou svou snahu schopen dané zařízení dostatečně zabezpečit.

Aby se předešlo ztrátě dat při ztrátě/krádeži/poruše zařízení, je vhodné maximum dat ze zařízení synchronizovat do cloudu nebo na síťová úložiště, což bývá typická situace u soudobých mobilních zařízení.

4.3 Síťová a cloudová úložiště provozovaná na infrastruktuře UK

Datová úložiště v majetku univerzity zpřístupněná koncovým uživatelům přes počítačovou síť. Tato úložiště jsou vhodná pro data, která je nutné sdílet s jinými osobami nebo je zpracovávat na více různých zařízeních.

Poznámka

Zabezpečení a dostupnost dat uložených na síťových a cloudových úložištích není dána jen zvoleným technickým řešením, ale především odbornou správou a nastavením procesů ukládaní a zálohování dat.

a) Úložiště typu „NAS“ (Network Attached Storage)

Uložení dat na datových úložištích připojených do LAN může v případě řádné správy splnit požadavky na zabezpečení a dostupnost vědeckých dat, je však doporučeníhodné využít mechanismy chránící před fyzickým selháním jednoho nebo více disků (RAID apod.). Třebaže NAS lze v případě kvalitní správy doporučit jako primární úložiště dat, je i zde nezbytné řešit zálohování.

Na co si dát pozor

*Tento typ méně nákladných a intuitivně spravovatelných úložišť často svádí k poloprofesionální správě přímo uživateli/vlastníky dat. Při nevhodné konfigurace bez absence zálohovacích mechanismů však může být tato varianta uložení dat poměrně riziková (např. při poruše více disků bez jejich průběžné výměny jsou data ohrožena srovnatelně jako na lokálních discích)**. Dejte přednost profesionálním řešením ve správě IT odborníků.***

b) Profesionální datová úložiště fakult a součástí (disková pole, SAN,…)

Uložení dat v serverovnách fakult a součástí prostřednictvím profesionálních úložných řešení (často redundantní disková pole, SAN) poskytuje zvýšenou ochranu dat proti jejich poškození nebo ztrátě, zálohování dat probíhá automaticky péčí správce úložiště, přesná politika zálohování bývá k dispozici v popisu parametrů úložiště. Centrální serverové uložení dat umožňuje lepší sledování přístupu k datům a zlepšuje tak možnosti zjištění neautorizovaného přístupu.

Na co si dát pozor

Aby se zabránilo neautorizovanému přístupu k datům, je třeba důsledně dbát na správné nastavení přístupových práv k datům. Často je problémem kapacita těchto úložných prostor, neboť při nákupu nebývají dimenzována jako úložiště poskytující kapacitu pro rozsáhlá vědecká data, ale pouze na běžný provoz fakulty/součásti.

4.4 Síťová a cloudová úložiště provozovaná externími subjekty mimo UK infrastrukturu

Technicky se jedná o pokročilá datová centra s několikanásobným uložením dat a speciálními funkcemi úložišť poskytující vysokou ochranu dat proti jejich poškození nebo ztrátě. Cloudové uložení dat také umožňuje lepší sledování přístupu k datům a zlepšuje tak možnosti zjištění neautorizovaného přístupu. S ohledem na to, že tato úložiště bývají navrhována za účelem často komerčního poskytování služeb široké skupině uživatelů, nebývá problém dohodnout pro jednotlivé vědecké projekty i nadstandardní kapacity.

a) Úložiště CESNET

Datová úložiště provozována Oddělením datových úložišť sdružení CESNET mohou využívat akademičtí pracovníci, studenti a pracovníci výzkumných organizací v ČR pro vzdělávací a výzkumné účely, a to jak v režimu bez sdílení dat (tzv. VO Storage) tak v režimu tzv. virtuální organizace umožňující sdílení dat mezi uživateli v rámci federace identit eduID.cz. Do této kategorie spadají i služby typu CESNET OwnCloud a CESNET FileSender. Použití těchto úložišť se řídí Pravidly využití služeb datových úložišť CESNET. Úložiště jsou provozována českou organizací, která je spoluvlastněná akademickými institucemi v ČR a UK je členem jejího statutárního orgánu. Datová úložiště jsou **certifikována podle normy pro systém managementu bezpečnosti informací ČSN EN ISO/IEC 27001:2014**., provozovatel úložiště vynakládá veškeré možné úsilí, aby data ochránil před ztrátou nebo zpřístupnění nepovolaným osobám. **Služby je možné doporučit i k ukládání diskrétních dat** (např. v případě nutnosti zajištění vysokých záruk za zabezpečení a dostupnost dat, např. **u citlivých dat**), je možné doporučit sjednání individuálního Service Level Agreement kontraktu.

b) Úložiště poskytovaná na základě centrálně uzavřených smluv s UK

Aktuálně mají studenti a zaměstnanci univerzity možnost využívat cloudových služeb **Microsoft 365**. Jedná se zejména o službu osobního úložiště OneDrive a službu dokumentové knihovny SharePoint. Součástí nabízeného balíku Microsoft 365 je též např. elektronická pošta Outlook a řada dalších služeb. Nakládání s daty v rámci této cloudové služby je zajištěno smlouvou uzavřenou mezi UK a společností Microsoft. Součástí smlouvy jsou i „standardní smluvní doložky“ vydané Evropskou komisí a **zaručující, že zpracování dat je v souladu s právem EU**. Data uživatelů z EU jsou uložena v datacentrech na území EU (konkrétně v Holandsku a Irsku). Bezpečnostní politika Microsoftu je v souladu s ISO 27001, 27002 a 27018. Tyto cloudové služby společnosti Microsoft splňují i požadavky GDPR. Z pohledu bezpečnosti i s ohledem na relativně vysokou poskytovanou kapacitu služeb (např. služba OneDrive pro firmy poskytovaná v rámci licenčního balíku A1 je omezena 1TB na uživatele, v případě licence A3 až 5TB dat na uživatele) i snadné možnosti sdílení dat lze tento způsob ukládání doporučit, a to i pro data a dokumenty vytvářené v rámci řešení vědeckých projektů.

Poznámka

*Osobní úložiště slouží primárně pro ukládání osobních dat. Do osobního úložiště **OneDrive** máte přístup pouze vy a sami si řídíte, zda a komu zpřístupníte v případě potřeby dokument nebo složku. Zde máte tedy uložené dokumenty, které nemáte obvykle potřebu sdílet s kolegy. V případě potřeby jednorázového doplnění, konzultace je možné dokument nasdílet, po ukončení aktivity je však vhodné sdílení ukončit.*

***SharePoint** je naopak sdílené úložiště týmu, (oddělení, projektu, procesu…). Není potřeba nastavovat přístupy k dokumentům pro jednotlivé uživatele, přístupy jsou řízeny členstvím v týmu. Sdílená data jsou přístupná pro všechny členy týmu po celou dobu spolupráce.*

c) Úložiště poskytovaná na základě individuálních smluv s UK

Doporučeníhodnou variantou je využití standardních komerčně nabízených služeb, vždy je však nutno dbát řádného smluvního zajištění kvality služeb (definice SLA parametrů) i zajištění, aby zpracovávání dat bylo plně v souladu s právem EU (plně odpovídalo požadavkům GDPR).

Na co si dát pozor

Využití profesionálních komerčních služeb je často spojené s relativně vysokou cenou těchto služeb; při sjednávání smluv se zamyslete i nad udržitelností zvoleného řešení v dlouhodobém horizontu (např. po ukončení financování projektu). Skutečně jste ověřili možnost využití služeb CESNET z.s.p.o.?

Bezpečnostní upozornění

Do této kategorie patří např. i cloudová datová úložiště poskytovaná v rámci služby ***Google G Suite for Education*** *na základě individuálních smluv s vybranými fakultami/součástmi UK. Zejména se jedná o datové kapacity Google Drive, patří sem ale i další data uložená v G Suite for Education cloudu, např. elektronická pošta v Google Mail, poznámky v Google Keep, kalendářová data v Google Calendar apod. Přes veškeré snahy dosud stále nedošlo ve smluvních vztazích k ujednání, jež by zaručila, že ukládání dat a jejich zpracování je v souladu s právem EU. Z tohoto důvodu služby* ***není možné bez dalších opatření doporučit k ukládání diskrétních a citlivých dat****.*

d) Úložiště bez smlouvy s UK – síťová a cloudová úložiště pro veřejnost

Do této kategorie spadají zejména veřejné cloudové služby (zřízené typicky zdarma koncovým uživatelem jen proti elektronické registraci přes web) jako Microsoft OneDrive, Google Drive, Dropbox, Úschovna, Uložto, Amazon úložiště, repozitáře na GitHub apod.

Zásadním rozdílem a „poznávacím znamením“ této kategorie cloudových úložišť oproti cloudovým službám uvedeným výše je skutečnost, že UK nemá žádný (právní) vztah s provozovateli těchto externích služeb, a proto není schopna garantovat jakékoliv záruky ohledně bezpečnosti/důvěrnosti uložených dat nebo politiky nakládání s nimi.

Na co si dát pozor

Je třeba si uvědomit, že žádná z těchto služeb není skutečně bezplatná – ve skutečnosti „platíte“ svěřenými daty, která dáváte provozovateli služby plně k dispozici, často k neomezenému využití. Proto je nutné mít na vědomí potenciálně vysoké riziko zneužití takto uložených dat.

5. Doporučení pro výběr datového úložiště

	veřejná data	interní data	diskrétní data	citlivá data
přenosná média	🟢	🟡	🔴	🔴
lokální disky (počítač/notebook)	🟢	🟡	🟡	🔴
lokální úložiště (telefon/tablet)	🟢	🟡	🔴	🔴
síťová a cloudová úložiště typu „NAS“ (Network Attached Storage) provozovaná na infrastruktuře UK	🟢	🟡	🟡	🔴
profesionální datová úložiště fakult a součástí (disková pole, SAN,…) řádně provozovaná vlastními IT zaměstnanci na infrastruktuře UK	🟢	🟢	🟢	🟡
datová úložiště a služby CESNET	🟢	🟢	🟢	🟡
síťová a cloudová úložiště provozovaná mimo infrastrukturu UK na základě centrálně nebo individuálně uzavřených smluv (při řádném smluvním zajištění GDPR a SLA)	🟢	🟢	🟢	🟡
síťová a cloudová úložiště pro veřejnost	🟢	🔴	🔴	🔴

🟢 vhodné

🟡 možné po provedení bezpečnostních opatření (šifrování, přístupové heslo, přístupová práva)

🔴 nevhodné

V případě specifických požadavků nebo ve speciálních odůvodněných případech, kdy nelze využít doporučené úložiště dat, je nutné provést individuální analýzu konkrétního případu a zavést taková opatření, která zaručí bezpečnost uložených dat.

6. Způsoby přenosu dat

Denně řešíme při spolupráci s kolegy sdílení a přenos dat a souborů. Možnosti přenosu dat jsou závislé na rozsahu přenášených dat.

6.1 Posílání dat jako příloha emailu

Data malého rozsahu (typicky soubory kancelářských aplikací apod.) v řádech MB jsou často přenášena emailem (podle typu emailového klienta lze přenášet v jedné zprávě soubory do velikosti zpravidla 10 MB).

Na co si dát pozor

*V případě přenosu diskrétních dat je vždy nezbytné soubory **šifrovat**. Posílat emailem citlivá data nelze doporučit ani při použití šifrování. Uvědomme si, že emaily jsou dnes běžně doručovány do různých mobilních zařízení (telefony, tablety, hodinky apod.) s různou úrovní zabezpečení, riziko vyzrazení je při přenosu nešifrovaných souborů vysoké.*

6.2 Využití flashdisků a USB disků

Dnes již velmi levné flash či USB disky velmi dobře poslouží k přenosu často i poměrně rozsáhlých dat, při použití šifrování nelze proti tomuto způsobu nic namítat, pokud správa koncových PC jejich zapojení umožňuje (řada firem využití USB portů k těmto účelům právě z důvodů ochrany dat před jejich zcizením zakazuje). Je však vždy potřeba dbát na bezpečné předání šifrovacího klíče a uvědomit si, že tento způsob přenosu neumožňuje ověřit, komu byla data poskytnuta.

Na co si dát pozor

Jak bylo již výše uvedeno, v případě použití těchto přenosných medií je pro zajištění bezpečnosti zásadní zajistit šifrování uložených dat. Je nezbytné mít na paměti vysoké riziko snadné ztráty média, tedy i ztráty uložených dat či jejich případného zneužití.

6.3 Využití úložišť pro jednorázové / časově omezené předání dat

Existuje řada webových portálů, které umožňují pohodlně nahrát i rozsáhlá data za účelem jejich zpřístupnění/stažení dalším osobám (identita osob oprávněných ke stažení je určena zadáním emailové adresy). I na tyto portály je potřeba nahlížet jako na dočasná datová úložiště a mít na paměti výše uvedené aspekty jednotlivých služeb.

a) Služba CESNETu „FileSender“ provozovaná sdružením CESNET z.s.p.o.

   Službu FileSender lze z důvodů uvedených v důvodu v odst. 4.a) kapitoly Kategorizace úložišť považovat za důvěryhodnou a spolehlivou a k jednorázovým přenosům dat ji doporučujeme upřednostnit. Služba aktuálně umožňuje přenos dat až 1,9 TB na jeden přenos (bez HTML5 je omezení 2 GB na jeden soubor) a nově nabízí při nahrání využít možnosti šifrování. Uživatel tak má jistotu, že data na portálu jsou uložena šifrovaně (data nejsou čitelná ani pro správce úložiště), uživatel pak musí zajistit distribuci šifrovacího hesla adresátům (např. mailem, SMS apod).

b) Služby jiných komerčních portálů typu „ulož.to, uschovna.cz, e-disk apod.“

   naopak nelze z důvodů vysokého rizika zneužití dat v žádném případě doporučit.

6.4 Využití funkcionality „sdílení“ datových úložišť

Metoda sdílení v rámci Vámi vhodně zvoleného datového úložiště je určitě vhodným řešením, neboť zajišťuje trvale Vámi pověřeným uživatelům přístup k nasdíleným aktuálním datům. Vždy si buďte jisti, jaká práva při sdílení ostatním uživatelům přidělujete.

Na co si dát pozor

Pro citlivá či důvěrná vědecká data je volba vhodného datového úložiště zásadní především z pohledu garance záruky ohledně bezpečnosti/důvěrnosti uložených dat nebo politiky nakládání s nimi (viz odst. 4.3)

6.5 Sdílení v rámci cloudového prostředí

Cloudová úložiště mají propracovaný způsob sdílení dat pro uživatele cloudu i pro hosty, umožňují zpřístupnit dokumenty s časovým omezením či dokumenty vyžadující ověření uživatele při každém přístupu.

Na co si dát pozor

Doporučujeme sdílení v rámci pracovních skupin (teamsy). S ohledem na skutečnost, že na UK je v rámci M365 služeb provozováno několik prostředí (tzv. tenantů), dejte pozor na to, komu data sdílíte a zda Vámi vybraný uživatel identitu v tenantu skutečně využívá. Omezte sdílení prostřednictvím linků pro hosty mimo tenant, k takovým datům mohou získat přístup i neoprávnění uživatelé.

7. Základy kybernetické bezpečnosti

CO DĚLAT	CO NEDĚLAT
Používejte silné heslo a změňte ho, pokud se domníváte, že mohlo být prolomeno	Nesdělujte nikomu své heslo
Oznamte jakoukoli ztrátu nebo podezření na ztrátu dat	Nepoužívejte své univerzitní heslo pro žádný jiný účet
Dávejte si pozor na falešné e-maily nebo telefonáty se žádostí o důvěrné informace – cokoli podezřelého nahlaste bezpečnostnímu týmu na adrese abuse@cuni.cz	Neotvírejte podezřelé dokumenty či odkazy
Udržujte software aktuální a používejte antivirus na všech zařízeních, kde je to možné	Nenarušujte bezpečnost univerzitních systémů
Mějte na paměti rizika používání veřejných Wi-Fi nebo počítačů	Neposkytujte přístup k univerzitním informacím a systémům
Zajistěte, že univerzitní data jsou uložena v univerzitních systémech	Nekopírujte důvěrné informace univerzity bez povolení
Chraňte svá osobní zařízení heslem a šifrováním	Nenechávejte své počítače a telefony odemčené

7.1 Přihlašovací údaje

Přestože je zabezpečení dat na síťových a cloudových úložištích na vysoké úrovni, nejslabším článkem obvykle bývá koncový uživatel, respektive způsob jeho autentizace: Pokud pro přístup používáte slabé heslo / heslo sdílené s jinými službami apod., a zároveň je heslo jediným prvkem autentizace, pak může vyzrazení hesla nepovolané osobě vést ke kompromitaci zabezpečení všech dat a služeb, ke kterým máte přístup.

Přístupové údaje k pracovním datům byste nikdy neměli zadávat do cizích počítačů (v kavárně, u kamaráda apod.), u kterých nemáte žádné povědomí ani záruky o jejich zabezpečení. Používejte svoje notebooky, telefony apod.

Abyste zvládli používat silná hesla unikátní pro každou službu, může být užitečné používat kvalitní správce hesel.

7.2 Soukromé počítače využívané pro pracovní účely

Je nutné si uvědomit, že na domácí počítače či jiná zařízení používaná pro přístup k pracovním datům by měly být kladeny stejné požadavky na zabezpečení, jako na pracovní počítače. Málo kdo má doma kamerový systém a vrátnici s nepřetržitým dohledem, proto věnujte zvýšenou pozornost fyzickému zabezpečení v době vaší nepřítomnosti (např. když jste na pracovišti).

Nezapomínejte na své ratolesti, které nejen mohou zapomenout zamknout při odchodu z domácnosti, ale často budou domácí počítač využívat spolu s vámi – striktní oddělení uživatelských účtů na počítači pro pracovní a osobní účely a nedostupnost administrátorských oprávnění dětem na sdíleném počítači by mělo být samozřejmostí. Stejně jako instalace kvalitního antivirového a antimalware software a firewallu.

Zabraňte instalaci her a podezřelého software na počítač, který používáte k práci. Instalujte jen důvěryhodný software, u kterého jste ověřili jeho autenticitu, zamyslete se nad konfigurací software (např. antivirové programy často automaticky odesílají soubory, které se jim zdají podezřelé, svému výrobci – takto mohou být z vašeho počítače bez vašeho vědomí odeslána data, která by se do rukou třetí strany dostat neměla).

Pamatujte, že data, která na domácím počítači nemáte, tam nemusíte chránit – ponechávejte pracovní data na síťových a cloudových úložištích a na domácí počítač stahujete jen minimum dat a jen na nezbytně nutnou dobu. Diskrétní a citlivá data pokud možno vždy šifrujte.

7.3 Povinnost hlášení ztráty služebních zařízení

Na základě pokynu pověřence na ochranu osobních údajů máte **povinnost nahlásit pověřenci každou ztrátu či odcizení každého zařízení nebo datového nosiče**, které mohou umožnit přístup k osobním nebo citlivým údajům, za které UK odpovídá. Tento pokyn se týká každého zařízení, ze kterého lze data získat např. prolomením ochrany (hesla) nebo vyndáním disku a získáním údajů samotných nebo hesel pro přístup do systémů univerzity. Typicky jde o notebook, tablet, počítač z kanceláře nebo i mobilní telefon s přístupovými údaji. Ztrátu co nejdříve oznámí pracovník, který ji zjistil, nebo jeho nadřízený, a to na adresu gdpr@cuni.cz.

7.4 Hlášení bezpečnostních incidentů

Koordinaci **řešení bezpečnostních incidentů v univerzitní síti** zajišťuje již od roku 2015 **bezpečnostní tým počítačové sítě Univerzity Karlovy CSIRT-CUNI**. Hlášení bezpečnostních incidentů zasílejte dle návodu emailem na abuse@cuni.cz.