Produktový list služeb

Popis služby

SingleCase je aplikace pro správu právních spisů, která obsahuje 2 základní moduly. Prvním je **dokumentové úložiště** specificky určené pro ukládání právních dokumentů, spisů a související agendy. Stará se automaticky o verzování dokumentů, jejich sdílení, umožňuje v dokumentech fulltextově vyhledávat a otevírat pro úpravy v programu Microsoft Word. Ke spisům lze přiložit poštu, termíny, úkoly a poznámky. Druhým je **fakturační modul**, který zajišťuje vykazování času, úpravu výkazů a fakturaci práce. Vykázaná práce a vystavené faktury poskytují podklad pro manažerský reporting výnosů a nákladů.

Fyzicky jsou dokumenty uloženy v zašifrované podobě na serverech našeho partnera společnosti Amazon, špičce v oblasti cloudových řešení, a střeženy na bankovní úrovni zabezpečení. Alternativně umožňujeme také zprovoznit aplikaci SingleCase nad dokumentovým úložištěm ve vaší kanceláři (viz níže technické varianty provozu SingleCase).

Komu je služba určena

- Malým advokátním kancelářím a samostatným advokátům, kteří pro ukládání dokumentů dosud používají disk počítače, sdílený disk nebo online úložiště.
- Advokátním kancelářím střední velikosti, které dosud ukládaly dokumenty s pomocí sdíleného disku, DMS nástroje nebo systému pro řízení advokátní kanceláře.
- Velkým advokátním kancelářím, které používají informační systém pro řízení advokátní kanceláře, avšak nevyhovují jim možnosti pro správu dokumentů, případně složitost systému.
- Firemním právním oddělením, kterým nabízíme dokumentové úložiště na míru. Pro detaily nás prosím kontaktujte na adrese info@singlecase.cz.

Jak začít

Své vlastní úložiště si můžete během 3 minut založit přímo na webu. Na otestování ho od nás vždy dostanete zdarma a bez závazku. Po vyplnění údajů kanceláře vám bude rovnou založeno nové úložiště, do něhož můžete ihned přizvat své kolegy a založit svůj první spis. Chcete-li pro založení spisu raději využít svého IT specialistu, můžete, systém rolí počítá i s touto variantou.

Do spisu si můžete své první dokumenty přetáhnout z počítače (chytnout myší a přetáhnout do aplikace můžete také e-maily nebo více dokumentů najednou), přiložit z e-mailového programu (každý spis má svou vlastní adresu pro příjem elektronické pošty), nahrát ZFO dokument po stažení z datové schránky nebo naskenované fyzické dokumenty. Od této chvíle se o sdílení, udržování aktuálních verzí a prohledávání obsahu staráme za vás.

S migrací spisů nebo dokumentů z vašeho sdíleného disku nebo jiného úložiště vám rádi pomůžeme, neváhejte nás prosím kontaktovat na stránce technické podpory nebo na adrese info@singlecase.cz.

Výhody pro právníky

- **Jednoduché vykazování s předvyplňováním času**: počítejte čas strávený na jednotlivých případech. Umíme napovídat a předvyplňovat výkazy za vás – a zpříjemnit tak tuto málo oblíbenou činnost.
- **Fakturace**: pracuje s různými typy účtování, umí pracovat i se speciálními variantami (dvě hodinové sazby po dosažení paušálu/capu apod.), umožňuje úpravu výkazů (seškrtání), zahrnutí do paušálu, generuje podklady k fakturaci. Umí počítat budoucí cashflow (přehled rozpracované práce).
- **Manažerský reporting výnosů a nákladů**: poskytuje přehledy podle klientů a spisů (všech spisů, všech klientů, spisů daného klienta, spisů daného odpovědného advokáta). Počítáme vykázanou práci oproti vyfakturované, recovery rate reálnou hodinovou sazbu. U právníků měříme efektivitu práce (reálný hodinový výnos, poměr vyfakturovaných hodin).
- **Dostupnost systému odkudkoli**: Díky cloudovému řešení jsou vám dokumenty, spisy a veškerá metadata v systému SingleCase dostupné 24 hodin denně. Běžná dostupnost systému je 99,98% času.
- **Jednoduché nahrávání**: Dokumenty přidejte do spisu prostým přetažením myší do aplikace nebo přeposláním e-mailu. Okamžitě se postaráme o sdílení se všemi právníky s přístupem do spisu.
- **Přímá integrace s Wordem**: Jedním kliknutím myši dokument otevřete pro prohlížení a úpravy ve Wordu. Po uložení se dokument automaticky nahraje zpět do aplikace.
- **Automatické verzování**: Kdykoli uložíte upravovaný dokument nebo nahrajete dokument v aktuální podobě, vytvoří se v aplikaci nová verze dokumentu – staré jsou kdykoli zpětně dostupné. Postaráme se také o automatickou kontrolu proti simultánním úpravám a o rychlé porovnávání obsahu dokumentů.
- **Fulltextové vyhledávání v obsahu dokumentů**: Samozřejmostí je fulltextové prohledávání veškerého obsahu dokumentů, pošty, úkolů a všech jejich metadat.
- **Časová osa pro přehled vývoje spisu**: Veškeré důležité revize, e-maily od klienta, budoucí lhůty nebo třeba poznámky k vývoji případu uvidíte přehledně na časové ose spisu.
- **Správa pošty ke spisu**: Do spisů SingleCase lze vkládat nejen dokumenty, ale také připojovat poštu přijatou datovými schránkami, e-mailem i fyzicky. Důležitou komunikaci ke spisu tak máte stále při ruce (i pokud přišla kolegům) a můžete na ni přímo ze systému odpovídat.
- **Hlídání termínů a úkolů**: Ke spisu můžete vytvářet termíny a také úkoly konkrétním advokátům – tak abyste nezmeškali žádné jednání nebo lhůtu. Termíny i úkoly hlídá

SingleCase za vás a automaticky na ně upozorňuje e-mailem. Můžete si je také synchronizovat do kalendáře v Outlooku.

- **Poznámky ke spisu a dokumentům**: Jste zvyklí přidávat si poznámky k dokumentům, úkolům nebo celému případu, na kterém pracujete? Mysleli jsme si to. Se SingleCase je to hračka.
- **Funguje na tabletu i na mobilu**: Poskytujeme aplikaci pro mobilní telefony, která hlídá termíny, zobrazuje změny ve spisu a náhled dokumentů. Obsažena je také verze pro tablety se stejnými funkcemi jako aplikace na PC. Podporujeme iOS a Android.
- **Robustní zálohování**: Vaše dokumenty jsou automaticky zálohovány na více fyzicky oddělených místech současně, tak abyste o ně nikdy nepřišli.

Tarify a varianty provozu

Služby SingleCase si můžete objednat v rámci čtyř placených tarifů dle platného ceníku. Služby si můžete nezávazně vyzkoušet po dobu 30 dní – poté vás budeme kontaktovat s požadavkem na úhradu faktury pro další pokračování služeb.

SingleCase dodáváme ve dvou technických variantách, které se liší místem, na kterém jsou uložena veškerá data, a ze kterého systém běží. Doporučenou variantou je řešení cloudové úložiště, kdy si můžete službu založit online z webu www.singlecase.cz. Výhodami jsou vysoká dostupnost, profesionální zálohování, bezpečnost dokumentů a veškerá údržba v ceně a v naší režii.

Alternativní variantou je řešení s vlastním serverem, které běží přímo z vaší kanceláře. Doporučujeme pouze pro případy, kdy jste již investovali do technického vybavení a máte k dispozici IT administrátory schopné provádět technickou podporu.

Srovnání výhod a nevýhod obou variant nabízí následující tabulka:

Privátní cloud (výchozí, doporučujeme)	Vlastní server
Dokumenty šifrovány při uložení i při přenosu. Šifrovací klíče v držení kanceláře (nejsou na serveru).	Běžně lze šifrovat pouze celý disk, ne jednotlivé dokumenty. Šifrovací klíče v držení kanceláře (uloženy na serveru).
Fyzicky střežený přístup k serverům	Většinou těžko řešitelné v případě umístění v kanceláři
Neomezené dokumentové úložiště *	Kapacita omezena IT vybavením v kanceláři, snadno řešitelné
Garantovaná dostupnost 99,5 % **	Dostupnost služby typicky horší (závislá na HW kanceláře)

Pro zajištění běhu je nutný omezený přístup Poskytovatele k datům dle podmínek Služby	Data zcela ve správě IT kanceláře, lze zcela zamezit přístupu Poskytovatele
Zálohování 24/7 na více fyzicky oddělených místech	K dispozici jsou zálohovací skripty pro IT kanceláře
Pravidelné aktualizace v ceně (max 1x měsíčně)	Aktualizace poskytovány a hrazeny zvlášť (max 3x ročně)
Pravidelné bezpečnostní audity aplikace i prostředí	Pravidelné bezpečnostní audity aplikace
Údržba HW i SW v ceně	V ceně pouze aplikace

* Podléhá principu rozumného užívání
** Nezapočítávají se plánované nedostupnosti služeb. V případě menší dostupnosti vracíme poplatek za daný měsíc

Bezpečnost dokumentů a povinnost mlčenlivosti advokáta

SingleCase provozujeme na cloudových serverech EC2 společnosti Amazon, jejíž datová centra jsou chráněna fyzickými zabezpečovacími mechanismy včetně vojenského perimetru. Přístup k zařízením je povolen pouze autorizovaným osobám. Fyzicky jsou dokumenty uloženy v zašifrované podobě na serverech společnosti Amazon v Německu a Irsku a data vaše i vašich klientů nikdy neopustí země Evropského hospodářského prostoru (EEA).

Citlivá data před uložením šifrujeme 256-bitovou šifrou AES, která je vysokým standardem šifrování. Přenos dat je z zabezpečen 256-bitovým SSL šifrováním a certifikáty důvěryhodných certifikačních autorit. Elektronické verze dokumentů jsou neustále zálohovány na záložním serveru.

Víme, že v SingleCase budete mít uloženy také dokumenty, na něž se vztahuje povinnost mlčenlivosti advokáta dle § 21 zákona o advokacii. Jsme si také vědomi možnosti orgánů činných v trestním řízení provádět prohlídky prostor, v nichž advokát vykonává advokacii postupem podle § 85b trestního řádu, tj. za nezbytné součinnosti České advokátní komory. V této souvislosti trestní kolegium Nejvyššího soudu vydalo dne 25. 6. 2015 stanovisko (Tpjn 306/2014), v němž mj. konstatovalo, že místem výkonu advokacie jsou také úložiště, v nichž lze ukládat, zpracovávat a využívat informace o klientech, která jsou provozovaná od advokáta odlišnou osobou, umožňující dálkový přístup pomocí internetové sítě, a že na takové místo se též užije postup podle § 85b trestního řádu. Takovým místem je samozřejmě i SingleCase. Proto Vám zaručujeme, že pokud, se na nás orgány činné v trestním řízení obrátí jako na zprostředkovatele cloudového úložiště ohledně výkonu takové prohlídky, jsme samozřejmě připraveni o tom ihned informovat jak Vás, tak Českou advokátní komoru.

Technické požadavky

K běhu SingleCase Vám stačí běžné PC s internetovým prohlížečem. Pro bezproblémovou funkci doporučujeme:

- Windows 7, 8, 10 nebo Mac OS X
- Prohlížeče Chrome, Firefox, Safari, Internet Explorer 10 a vyšší
- Pro mobilní přístup jsou k dispozici aplikace pro iOS a Android

Systém zabezpečení dat
(aktualizace 1. 3. 2018)

Tímto dokumentem se my, společnost SingleCase, s.r.o., se sídlem Zubatého 295/5, 150 00 Praha 5, IČO: 02894815, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 225059, co do bezpečnosti ukládaných dat řídíme při poskytování služeb v rámci aplikace SingleCase.

1) Bezpečnost dat a povinnost mlčenlivosti advokáta

Místo a způsob uložení dat

SingleCase ke svému provozu využívá privátního cloudu umístěného ve Frankfurtu na serverech společnosti Amazon Web Services, Inc. se sídlem 440 Terry Ave N, Seattle, WA, 98109 United States. Systém je tak stále dostupný a díky používaným šifrovacím možnostem také maximálně bezpečný. Dokumenty šifrujeme tak, že klíče k nim má v držení pouze zákazník, nikoli my jako poskytovatel.

V případě zákazníků - advokátů ctíme povinnost mlčenlivosti advokáta dle § 21 zákona o advokacii. SingleCase je místem, kde můžete ukládat data svých klientů (viz také stanovisko trestního kolegia Nejvyššího soudu Tpjn 306/2014). Veškerá data zákazníků spravujeme dle Směrnice 95/46/ES a Zákona o ochraně osobních údajů – Poskytovatel cloudu garantuje, že data nikdy neopustí země Evropského hospodářského prostoru. Pokud se na nás obrátí orgány činné v trestním řízení, informujeme o tom jak zákazníka, tak Českou advokátní komoru.

Zálohování a export

Dokumenty, data vaše i vašich klientů jsou křížově zálohovány na více místech. V nepravděpodobném případě výpadku aplikace nebo dokumentů postupujeme dle transparentních scénářů tzv. *disaster recovery* pro zajistění přístupu v co nejkratším čase.
Dokumenty i veškerá data si můžete kdykoli stáhnout přímo z aplikace SingleCase. Rádi vám také budeme posílat plné zálohy vašich spisů – automaticky a na úložiště dle vašeho výběru.

2) Řízení přístupu k datům a technické opatření jejich zabezpečení

Vymezení pojmů

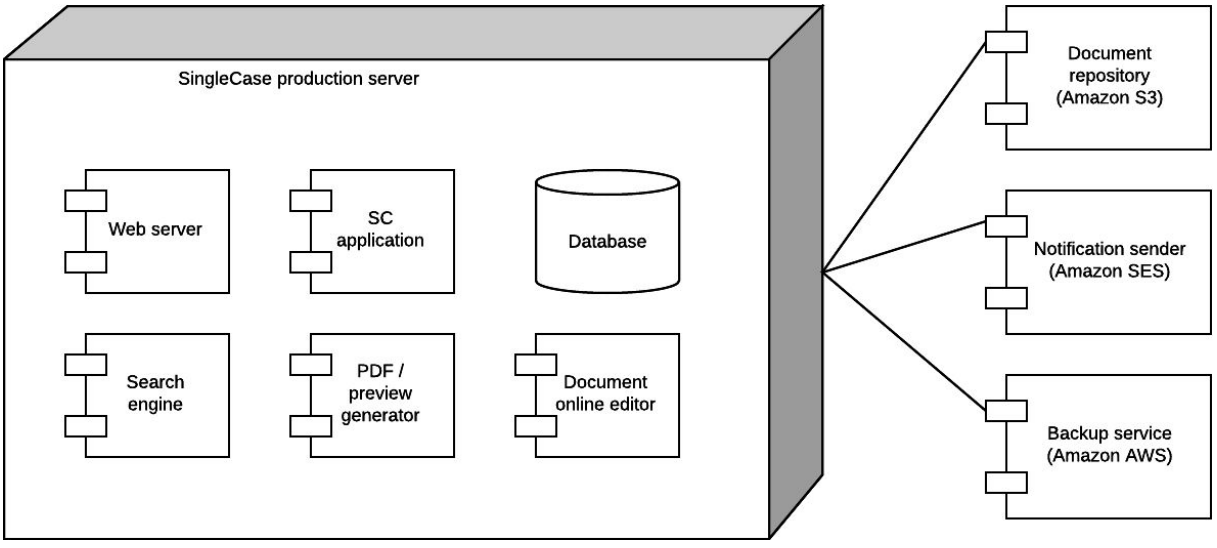
Datové centrum – Místo, kde je fyzicky umístěn server, a které mu poskytuje konektivitu k internetu, fyzické zabezpečení, zálohování a další služby. SingleCase používá datové centrum společnosti Amazon Web Services, Inc. ve Frankfurtu.

Server – Počítač, na kterém běží aplikace SingleCase. Rozlišuje se fyzický server (konkrétní kus hardwaru) a virtuální server (kus pronajaté výpočetní kapacity, HW je typicky velmi výkonný a dělitelný na malé části – případ SingleCase). Kromě samotné aplikace SingleCase (viz níže) běží na serveru také podpůrné aplikace nutné pro její provoz, např. vyhledávací engine, aplikace pro online úpravu dokumentů, databáze, webový server, komponenta pro generování náhledů a jiné.

Aplikace – Počítačový program SingleCase a podpůrné aplikace, které běží na serveru a vykonává operace z pověření uživatele (čtení/zápis do databáze, čtení/zápis do dokumentového úložiště) nebo na pozadí (e-mailové notifikace, příjem pošty, automatická záloha atd.).

Databáze – Struktura, ve které jsou uložena data aplikace.

Dokumentové úložiště – Místo, ve kterém jsou uloženy fyzické dokumenty. Propojeno s aplikací prostřednictvím odkazů na dokumenty z databáze.



Server

Server si pronajímáme prostřednictvím služby *Amazon AWS*, který zabezpečuje jeho fyzickou bezpečnost a dostupnost aplikace. V rámci týmu SingleCase existují dvě osoby s přístupem ke konfiguraci serveru, tím jsou CEO a CTO (vedoucí vývoje). Přístup ke konfiguraci neznamená automaticky možnost přístupu na server, nicméně prostřednictvím konfigurace lze přístup udělit.

Přístup na samotný server je řízen na úrovni uživatelských účtů konkrétních zaměstnanců SingleCase. K produkčnímu serveru s daty zákazníka mají přístup dvě osoby, a to CTO a senior vývojář (pro zajištění možnosti zásahu v případě absence CTO). Přístupem k serveru získává uživatel možnost přístupu k souborům aplikace vč. přístupovým údajů k databázi.

Databáze

Databáze je umístěna přímo na serveru SingleCase. K datům zákazníka mají přístup tři uživatelé s administrátorskými právy – speciální uživatel, pod kterým se hlásí aplikace (více o jejím zabezpečení níže), dále CTO a senior vývojář. **Přístup k datům z naší strany je vždy omezen na konkrétní účty, slouží výhradně k identifikaci a opravě chyby a vždy pouze na dobu nezbytně nutnou**. Podobně jako v případě serveru nepoužíváme z bezpečnostních důvodů účty administrátora, uživatelé se vždy hlásí se svými přístupovými údaji a veškeré jejich operace jsou logovány.

Dokumenty

Dokumenty jsou umístěny na speciálním dokumentovém úložišti *Amazon S3*. Architektura úložiště je postavena na principu malých oddělených úložišť (tzv. *buckets*). Každý *bucket* je šifrován svým vlastním klíčem a znemožňuje vydání dat bez jeho znalosti – tento způsob tedy efektivně zamezuje stažení byť jen zašifrovaných dokumentů bez vědomí vlastníka klíče.
Oproti běžnému uložení dokumentů na disku je v *bucketu* oddělen binární obsah dat od jejich popisovače – bucket tedy neobsahuje čitelný název dokumentu. SingleCase využívá metodu, v rámci které je v každém *bucketu* uložen právě jeden dokument – nabytím klíče k jednomu dokumentu tedy nelze získat přístup k jinému.

K přístupu k dokumentu je nutné rozšifrovat soustavu šifrovacích klíčů, přičemž každý z nich odemyká další v řadě. Hierarchie klíčů je následující:

1. **Heslo uživatele** – uloženo v databázi chráněno tzv. pomalou hašovací funkcí bcrypt (cost=10) používající technologii solení, vyžadována je kvalita hesla (délka i rozsah znaků)
2. **Klíč uživatele** – uložen zašifrovaný v databázi 256-bitovou symetrickou šifrou (AES), generuje se při při vytvoření nového uživatele spolu s jeho heslem, každý uživatel má unikátní klíč
3. **Hlavní klíč firmy**, tzv. *master* klíč, uložen zašifrovaný v databázi 256-bitovou symetrickou šifrou (AES)
4. **Klíč dokumentu** – uložen zašifrovaný v databázi 256-bitovou symetrickou šifrou (AES), je součástí metadat dokumentu spolu s odkazem na *bucket*, každý dokument je umístěn v jiném *bucketu* a tedy má unikátní klíč

Aplikace

Aplikace má při svém běhu přístup k datům, krátkodobě i těm, které jsou při uložení šifrovány (například při synchronizaci pošty se po přihlášení uživatele rozšifrují přístupové údaje ke schránkám, aplikace k nim má přístup do dokončení úlohy). Aplikaci proto podrobujeme pravidelným (2x ročně) bezpečnostním auditům externího partnera – specialisty na bezpečnost aplikací.

Audit je prováděn v těchto fázích:

1. **Audit architektury** – posuzována kvalita návrhu komponent aplikace, systém ukládání šifrovacích klíčů, umístění a ochrana aplikace, databáze i dokumentů
2. **Kontrola zdrojového kódu** – odhaluje potenciální problémy nebo chyby v nakládání s daty při běhu aplikace
3. **Penetrační testy** – testování aplikace v živém provozu s cílem odhalit běžné problémy webových aplikací (např. definovány projektem *OWASP*), které by mohly vést k porušení důvěrnosti informací externím (pokus o prolomení aplikace) nebo interním (pokud o zvýšení práv uživatelem s omezenými právy) útočníkem.

3) Kategorie dat v SingleCase a jejich zabezpečení šifrovacími klíči v držení kanceláře

SingleCase obsahuje systém šifrování s využitím šifrovacích klíčů, které jsou v držení zákazníka. Aktuálně (11/16) se těmito klíči šifrují fyzické dokumenty v úložišti Amazon S3 a přístupové údaje k poštovní schránce uživatelů. V průběhu je přechod na plné šifrování u vybraných kategorií dat, tak aby k nim byl vyloučen jakýkoli přístup Poskytovatele.

Kategorie dat	**Plán šifrování**	**Náročnost / dopady šifrování**
Klient – název	Nelze šifrovat	• E-mailové notifikace (nelze posílat s názvem klienta) • Synchronizace s kalendářem (dtto) • Rychlost filtrování spisů v seznamu • Obecně práce s výkazy, fakturami (pomalý výběr filtru)
Klient – metadata (adresy, fakt. údaje)	V plánu šifrování vlastními klíči	• Nemožnost sledování solventnosti (IČO, datum narození / rodné číslo)
Spis – název	Nelze šifrovat	• E-mailové notifikace (nelze posílat s názvem spisu) • Synchronizace s kalendářem (dtto) • Rychlost filtrování spisů v seznamu • Obecně práce napříč aplikací (zpomalení v řádu desítek procent)
Spisy - metadata	V plánu šifrování vlastními klíči	• Rychlost filtrování spisů v seznamu
Kontakty (klient, spis)	V plánu šifrování vlastními klíči	-
Protistrany	V plánu šifrování vlastními klíči	• Rychlost filtrování spisů v seznamu • Nemožnost sledování solventnosti
Sazby (klient, spis)	V plánu šifrování vlastními klíči	-
Dokumenty – fyzické	Šifrováno vlastními klíči	-
Dokumenty - název	Nelze šifrovat	• Nemožnost hledání v dokumentech stávajícím mechanismem (teoreticky lze s velmi velkým dopadem na rychlost)

Složky - název	V plánu šifrování vlastními klíči	• Rychlost výpisu dokumentů
Úkoly a termíny – název	Nelze šifrovat	• Nelze posílat e-mailové notifikace • Nelze synchronizovat úkoly a termíny do kalendáře
Úkoly a termíny – popis	V plánu šifrování vlastními klíči	• Nelze zaslat popis úkolu / termínu v notifikaci
Korespondence – předmět	Šifrování vlastními klíči v realizaci	• Rychlost výpisu pošty • Rychlost vyhledávání v poště
Korespondence – obsah	Šifrování vlastními klíči v realizaci	-
Poznámky ve spisu	Šifrování vlastními klíči v realizaci	-
Výkazy – popis	V plánu šifrování vlastními klíči	• Rychlost načtení / úpravy faktur • Rychlost přehledu výkazů (zpomalení v řádu desítek procent)
Náklady – popis	V plánu šifrování vlastními klíči	• Dtto jako výkazy, pouze s nižším dopadem (menší množství výkazů)
Faktury – celková částka	Nelze šifrovat	• Rychlost načítání přehledu faktur • Kritický vliv na výpočet reportů (nyní se generují při načtení - neukládají se, nutná změna)
Přístupové údaje ke schránce uživatele	Šifrováno vlastními klíči	-

Způsob nakládání s šifrovacím klíčem v držení kanceláře

1) Při registraci nového účtu se vytvoří tzv. *master klíč*, kterým šifrujeme dokumenty. Uživateli se také vytvoří jednorázově zobrazí *obnovovací klíč kanceláře*, systém následně vyzve k jeho vytištění a bezpečnému uložení. Klíčem lze obnovit přístup k šifrovacím dokumenty v případě zapomenutí přihlašovacích údajů všemi uživateli aplikace.

2) Po registraci se *master klíč* také použije pro vytvoření hesla prvního uživatele. Následně je zašifrován a již nikdy se v aplikaci neobjeví v nezašifrované podobě.

3) Po přihlášení uživatele se jeho heslo použije ke krátkodobému dešifrování *klíče uživatele* odvozeného z *master klíče*, díky němuž může po dobu svého přihlášení přistupovat k dokumentům, případně zakládat nové uživatele. Bez přihlášení neexistuje žádná možnost, jak se k dokumentům v aplikaci dostat.

4) Změna hesla uživatelů je možná pouze po přihlášení administrátora do aplikace – není tedy kupříkladu možné obnovit heslo uživateli přes e-mailovou adresu. V případě, že heslo zapomene administrátor, můžeme krátkodobě zvýšit práva jinému uživateli – ten následně vytvoří nové heslo kolegům.

5) V případě ztráty hesel všech uživatelů přepneme na žádost zákazníka aplikaci do režimu obnovy, kdy je možné zadat *obnovovací klíč*. Po obnovení je možné znovu vytvořit heslo administrátora.

   Upozornění: Použité šifrování neumožňuje, aby se k dokumentům v případě ztráty hesel všech uživatelů dostal kdokoli jiný. Proto je pro případnou obnovu klíčové ponechat si bezpečně uložený klíč vygenerovaný při prvním použití.

4) Řízení bezpečnosti uvnitř firmy

Access policy

Konkrétní způsob řízení přístupů (uživatelů i aplikace) je popsán do většího detailu v dokumentu v dokumentu *SingleCase access policy*, jehož vlastníkem je CTO, který zajišťuje jeho dodržování. Dokument popisuje zejména scénáře přidělení, obnovy a odvolání přístupů a konkrétní způsob realizace.

Security policy

Bezpečnostní standardy nakládání s citlivými informacemi je popsán v dokumentu *SingleCase security policy*, jehož vlastníkem je CEO, který zajišťuje jeho dodržování. Dokument popisuje způsob nakládání s hesly, jejich kvalitu, scénáře jednání vč. těch zakázaných.

Oba dokumenty rádi poskytneme k nahlédnutí.

SingleCase řešení výpadků služby

Dokument popisuje možné scénáře výpadku služby SingleCase, postup a časy postupného obnovení.

SCÉNÁŘ 1. Výpadek databáze na serveru

Webová stránka je dostupná, ale hlásí chybu připojení k databázi. Přihlášení je nedostupné, stejně jako export dat.

Řešení: obnovení databáze ze zálohy (maximálně 24 hodin staré)
Čas reakce: pracovní den během 10 minut, mimo něj 60 minut
Čas spuštění: 30 minut
Čas úplné obnovy dat: v závislosti na množství dat a rozsahu poškození

Postup:
1. Pokus o opravu v databázi bez nutnosti obnovy ze zálohy
2. V případě úplné nedostupnosti databázového připojení vypnutí webového serveru
3. Obnovení poškozené databáze z poslední zálohy (max 24 hodin staré)
4. Nahození webového serveru, pokud došlo k vypnutí
5. Oprava chyby v databázi a nahrání aktuální verze databáze
6. V případě chyby většího rozsahu postupné obnovení dat místo jednorázového

SCÉNÁŘ 2. Výpadek serveru (webový nebo celý stroj)

Webová stránka není vůbec dostupná, hlásí chybu serveru.

Řešení: obnovení serveru ze snapshotu (obrazu stroje), obnova databáze ze zálohy
Čas reakce: pracovní den během 10 minut, mimo něj 60 minut
Čas spuštění: 60-90 minut
Čas úplné obnovy dat: v závislosti na stavu serveru a dostupnosti databáze

Postup:
1. Pokus o připojení ke stroji a spuštění webového serveru
2. Nahrání snapshotu serveru na nový server a přesměrování DNS
3. Nahrání databáze z původního serveru nebo poslední zálohy (max 24 hodin staré)
4. Nahození webového serveru
5. V případě obnovy databáze ze zálohy postupné obnovení dat dle dostupnosti databáze na původním serveru

SCÉNÁŘ 3. Nechtěné smazání dat zákazníkem nebo chybou aplikace

SingleCase běží, chybí pouze konkrétní data (např. spis, klient, dokument)

Řešení: obnovení dat ze zálohy
Čas reakce: pracovní den během 60 minut
Čas úplné obnovy dat: 1-24 hodin v závislosti na rozsahu dat, pouze v případě dostupnosti zálohy.

Zálohy jsou k dispozici:

1. Pro metadata 1, 2, 3, 4, 5 dní zpětně, dále 1, 2, 3, 4 dny zpětně, dále 1, 2, 3, 4, 5 měsíců zpětně
2. Pro dokumenty 1x týdně po dobu dvou měsíců zpětně

Postup:
1. Zjištění, jestli se inkriminovaná data nachází v poslední záloze (příp. předchozích zálohách) databáze, příp. dokumentů
2. Postupná obnova dat dle jejich dostupnosti
3. Alternativně je možné poskytnout kritické dokumenty přednostně přímým zasláním klientovi

SCÉNÁŘ 4. Nedostupnost poskytovatele / datového centra Amazon / páteřního připojení k internetu

Webová stránka není vůbec dostupná, nelze načíst stránku.

Řešení: spustit webový server na alternativním umístění, obnova databáze ze zálohy, dokumentů ze záloh zákazníka (případně bez dokumentů)
Čas reakce: pracovní den během 10 minut, mimo něj 60 minut
Čas spuštění: 24 hodin
Čas úplné obnovy dat: v závislosti na dostupnosti záloh a dokumentů

Postup:
1. Spuštění webového serveru na provizorním umístění (náš webhosting), přesměrování DNS záznamů
2. Obnovení databáze z poslední zálohy umístěné mimo servery Amazon
3. Postupná obnova dat dle jejich dostupnosti (v této fázi se nepředpokládá plné obnovení dokumentů, pouze z případných záloh zákazníka, a spuštění pouze v read-only módu)
4. Po znovuobnovení dostupnosti datového centra přesměrování zpět na server Amazon