

**singlecase**

**BEZPEČNOSTNÍ KODEX**  
**společnosti Single Case, s.r.o.**

Verze 1.0 (1. 8. 2020)

# 1. Úvodní prohlášení

Účelem tohoto bezpečnostního kodexu (dále jen „**Kodex**“) je zachytit základní pravidla, kterými se společnost Single Case, s.r.o., IČO: 02894815, sídlem Zubatého 295/5, Smíchov, 150 00 Praha 5 (dále jen „**Single Case**“) při výkonu své každodenní činnosti řídí, a stanovit jim odpovídající povinnosti jejích pracovníků. Pracovníkem se pro účely tohoto Kodexu myslí každá fyzická osoba, zaměstnaná nebo jednající jménem, v rámci činnosti nebo v zájmu společnosti Single Case, a to včetně členů statutárních orgánů, vedoucích pracovníků, externích poradců či jiných smluvních dodavatelů.

Společnost Single Case vyvinula a dále vyvíjí aplikaci SingleCase, která je nástrojem pro řízení zejm. advokátních kanceláří. Aplikace SingleCase je IT produkt, jehož hodnota spočívá zejména v jeho kódu, technické specifikaci, architektuře, funkcích a klientských datech. Klienty společnosti Single Case jsou zejména advokáti, na jejichž činnost se vztahuje přísná regulace upravená zejména zákonem

č. 85/1996 Sb., o advokacii, a dalšími stavovskými předpisy vydanými Českou advokátní komorou. Důraz je kladen především na zachování zákonem stanovené povinnosti mlčenlivosti o všech skutečnostech, o nichž se advokát dozvěděl v souvislosti s poskytováním právních služeb a s tím související ochrana klientských dat a spisů.

Ochrana dat klientů, jejich spisů, dokumentů, jakož i ochrana kódu aplikace SingleCase a dalších aktiv společnosti Single Case jsou absolutní prioritou. Pravidla a zásady uvedené v tomto dokumentu jsou závazná pro veškeré pracovníky s přístupem k jakýmkoliv takovým datům v rámci jejich činnosti pro společnost Single Case.

Společnost Single Case lpí na tom, aby při všech jejích činnostech a za všech okolností byla pravidla tohoto Kodexu dodržována. Kodexem se řídí a jsou povinni řídit všichni její pracovníci bez výjimky. Tento Kodex obsahuje základní bezpečnostní pravidla, jimiž se společnost Single Case řídí, a které představují pro její pracovníky závazné vodítko a rámec. Společnost Single Case netoleruje porušování tohoto Kodexu ze strany pracovníků. Porušení tohoto Kodexu ze strany pracovníků může být v rámci civilního práva posouzeno jako odpovědnost za škodu, porušení prevenční povinnosti, porušení smluvní povinnosti apod., a takové nároky budou ze strany společnosti Single Case uplatňovány.

## 2. Bezpečnost a ochrana dat

Společnost Single Case striktně dbá, aby v rámci její činnosti byly dodržovány právní předpisy, základní morální a etické principy, jakož i základní zásady poctivého obchodního styku. Jednání, které je v rozporu s těmito zásadami, společnost Single Case odmítá.

Pracovníci společnosti Single Case jsou v rámci každého svého jednání, kde vystupují jménem společnosti Single Case, v rámci její činnosti nebo v jejím zájmu povinni relevantní právní předpisy a

normy dodržovat, respektovat a svým chováním reprezentovat společnost Single Case tak, aby bylo zachováno její dobré jméno i pověst.

Společnost Single Case dbá nejen na ochranu vlastních citlivých a důvěrných informací, ale zejména o ochranu jakýchkoliv dat svých klientů, a to zejména těch, které má k dispozici v rámci své obchodní činnosti při poskytování aplikace SingleCase, tj. zejména data, dokumenty, spisy, databáze klientů a jejich údaje, finanční ukazatele, personální informace, účetní data apod. Společnost Single Case dbá na ochranu těchto údajů a dat svých klientů tak, aby byly dodrženy požadavky příslušných právních předpisů vztahujících se k výkonu činnosti klientů.

Má-li pracovník podezření, že došlo k úniku či zneužití dat, či takový únik nebo zneužití byť potenciálně hrozí, je povinen oznámit tyto skutečnosti neprodleně jednateli společnosti Single Case.

Pracovníci jsou zavázáni zachovávat mlčenlivost o citlivých, soukromých a jinak sdělených údajích, a to zejména v rozsahu, který je stanoven v dohodě o mlčenlivosti, kterou má každý pracovník se společností Single Case uzavřenu.

Nad rámec výše uvedeného jsou pracovníci povinni dodržovat při veškerých relevantních činnostech následující bezpečnostní pravidla:

## 2.1. Bezpečnostní checklist

1. V rámci veškeré elektronické komunikace využívat výhradně firemní e-mailovou schránku na doméně singlecase.cz nebo aplikaci Slack. Jedinou výjimkou z tohoto pravidla je testování aplikace SingleCase ve vývojářském prostředí, kdy lze využít propojení s dalšími e-mailovými schránkami.
2. Registrovat se do veškerých aplikací třetích stran (vč. aplikací pro vývoj (např. Bitbucket, JIRA, Slack, Amazon AWS a další) výhradně e-mailem na doméně singlecase.cz. Jedinou výjimkou z tohoto pravidla je testování aplikace SingleCase ve vývojářském prostředí.
3. Veškeré firemní informace a dokumenty ukládat výhradně do firemních systémů a aplikací. Nesmí se používat soukromé zálohovací cloudové služby (jako např. Dropbox, OneDrive, iCloud apod.) pro ukládání firemních dokumentů.
4. Hesla na počítačích používaných k práci (vč. hesla k přihlášení systému) musí mít více než 12 znaků a obsahovat kombinace různých skupin znaků (minimálně malá a velká písmena a čísla). Nesmí se používat snadno uhádnutelná hesla citlivá pro tzv. slovníkové útoky. Doporučuje se hesla vytvářet přímo správcem hesel.
5. Veškerá hesla ukládat pomocí tzv. aplikací správce hesel (*password manager*) jako např. *1Password*.
6. Osobní účty ve firemních a/nebo zákaznických systémech mohou být používány pouze oprávněným vlastníkem. Nesmí se předávat přístupové údaje dalším zaměstnancům s výjimkou technických účtů a/nebo účtů, které jsou ke sdílení výslovně určeny.
7. Na počítačích používaných k práci musí být zapnuto šifrování harddisku (např. Windows BitLocker, OS X FileVault). Heslo nebo šifrovací fráze musí splňovat požadavky bodu 3.
8. Musí být zapnuté aktualizace zabezpečení operačního systému. Vždy je nutné používat aktuální software.
9. Na všech počítačích používaných k práci musí být zapnutý firewall a nainstalovaný firmou

schválený antivirový software. Antivirus musí mít povolené skenování za běhu a automatické stahování aktualizací na denní bázi.

10. Při opuštění počítače používaného k práci vždy uzamknout obrazovku. Nastavit automatický zámek obrazovky na 10 minut nebo kratší dobu (doporučené jsou 2 minuty).
11. Všechny produkční kód aplikace vždy ukládat do verzovacího nástroje (GitLab, Bitbucket aj.).
12. Na produkční prostředí nahrávat kód výhradně prostřednictvím standardního procesu pomocí verzovacího nástroje. Žádné ruční úpravy kódu na produkčním prostředí.
13. Veškeré změny v produkci provádět dle platných procesů, na základě odůvodnění a schválení.
14. Všechna připojení musí využívat pouze chráněné kanály (HTTPS, SSH, zabezpečené pracovní wi-fi a/nebo kabel).
15. Zapnout vícefaktorové ověřování (MFA) na Google aplikacích a všech dalších firemních systémech, které vícefaktorovou autentizaci podporují. Jedinou výjimkou z tohoto pravidla je testování propojení aplikace SingleCase a aplikací Gmail; pro takovéto testování nesmí být použit osobní emailový účet zaměstnance.
16. **Nikdy nesdílet a neposílat obsah, který obsahuje klientská data. V printscreeenech musí být veškerá klientská data začerněna.**
17. **Nestahovat klientská data na počítač používaný k práci. Jedinou výjimkou je, pokud je to nezbytné pro import nebo kontrolu dat, v takovém případě je nutné pravidelně data promazávat, aby nikdy na počítači klientská data nezůstala déle než je nezbytně nutné.**
18. **Data klienta sloužící pro import musí být po zpracování importu smazána z e-mailu a disku počítače. Záloha importních tabulek se vloží do soukromého účtu úložiště (účet společnosti SingleCase v aplikaci SingleCase - nerudovka.app.singlecase.cz) do privátního spisu s odpovědným uživatelem - jednatelem společnosti Single Case.**
19. **Pokud má být použit administrátorský účet ke klientskému účtu v aplikaci, je předem nutný písemný souhlas klienta.**
20. Veškeré tištěné dokumenty s potenciálně důvěrnými informacemi musí být uloženy v uzamykatelné skříni v kanceláři společnosti Single Case.
21. Mobilní telefon musí být zabezpečen zámek obrazovky a PIN kódem.
22. Pravidelně odstraňovat dokumenty z pracovního stolu (skartovač papírů je dostupný na pracovišti) a mazat tabule, ledaže jsou výslovně označené "nemazat" a neobsahují vysoce citlivé informace.
23. Hlásit jednatelem společnosti Single Case (e-mailem [pavel.krkoska@singlecase.cz](mailto:pavel.krkoska@singlecase.cz) nebo telefonicky 739 475 360) veškerá potenciální bezpečnostní rizika (včetně ztráty nebo krádeže firemního laptopu či mobilního telefonu), a to neprodleně.
24. Hlásit jednatelem společnosti Single Case veškeré podezřelé aktivity a potenciální bezpečnostní incidenty, a to neprodleně.
25. Při používání firemních prostředků pro soukromé účely zajistit zachování všech bezpečnostních pravidel a striktně oddělovat osobní informace a dokumenty od dokumentů a informací společnosti a zákazníků.

Pracovníci jsou dále povinni respektovat následující zakázaná jednání a těchto se zcela vyvarovat.

## 2.2. Zakázaná jednání

1. Nikdy nepoužívat shodné heslo pro více aplikací a/nebo uživatelských účtů.

2. Neukládat hesla v prohlížečích (s výjimkou testovacích přístupů).
3. Při nutnosti předat kolegům heslo k produkční aplikaci poslat vždy jiným kanálem, než jakým probíhá komunikace (např. sms zprávou). Ve zprávě s heslem nesmí být zmíněn systém, do kterého je heslo určeno, ani přihlašovací jméno.
4. Nikdy nezasílat žádná hesla skrz nezabezpečené kanály, zejména ne e-mailem.
5. Žádné účty hosta (bez hesla) na počítačích používaných k práci.
6. Nikdy neponechávat počítač používaný k práci bez dozoru.
7. Žádné pirátské nebo nelegální aplikace na počítačích používaných k práci.
8. Nikdy neinstalovat aplikace z neznámého zdroje.
9. Nepoužívat firemní počítače a zdroje (jako např. připojení k Internetu) k nelegálním, neetickým či jinak nevhodným účelům.
- 10. Nepřístupovat k zákaznickým datům (a to ani zašifrovaným) bezdůvodně. Každý přístup k datům zákazníka musí být odůvodněný např. požadavkem na technickou podporu, chybovou hláškou aplikace apod.**

Pracovníci berou na vědomí, že společnost si vyhrazuje právo používání výpočetní techniky, systémů a infrastruktury společnosti přiměřeným způsobem a v souladu s platnou legislativou monitorovat.

### 3. Závěr

Pracovníci berou na vědomí, že výčet pravidel v tomto Kodexu není a nemůže být úplný a může být pravidelně doplňován a aktualizován. Pracovníci se i v otázkách, situacích a vztazích, které tento Kodex výslovně neupravuje, chovají a jednají v souladu s principy a cíli Kodexu, právními předpisy, dobrými mravy, pravidly etiky, morálky a poctivého obchodního styku, tak aby dostáli dobrého jména a pověsti společnost Single Case a chránili veškerá data klientů společnosti Single Case. V případě jakýchkoliv nejasností se pracovníci obracejí na jednatele společnosti Single Case.