|  |  |
| --- | --- |
| Název dokumentu: | **SMĚRNICE Bezpečnost počítačové sítě a ochrana osobních údajů**  |
| Garant dokumentu: | Vedoucí technického oddělení |
| Seznam příloh: | Příloha č. 1 – Servisní zásahy – jak na to |
| Změny v dokumentu: | Aktualizace odstavce 4.1. Politika ochrany osobních údajů |

OBSAH:

[1 Účel 2](#_Toc182574300)

[2 Platnost 2](#_Toc182574301)

[3 Použité zkratky a pojmy 2](#_Toc182574302)

[3.1 Zkratky 2](#_Toc182574303)

[3.2 Pojmy 2](#_Toc182574304)

[4 Politiky bezpečnosti informací 3](#_Toc182574305)

[4.1 Politika ochrany osobních údajů 3](#_Toc182574306)

[4.2 Politika bezpečnosti komunikační sítě 4](#_Toc182574307)

[4.3 Politika přenosu informací 4](#_Toc182574308)

[5 Vzdálený přístup k zákazníkům a práce s DB zákazníků 5](#_Toc182574309)

[5.1 Vzdálený přístup 5](#_Toc182574310)

[5.1.1 Přístup pomocí TeamViewer – upřednostňovaný způsob přístupu! 5](#_Toc182574311)

[5.1.2 Ostatní způsoby vzdáleného přístupu 6](#_Toc182574312)

[5.2 Práce s DB zákazníků – v počítačových sítích ASOL a zákazníků 6](#_Toc182574313)

[5.2.1 Přístup k DB v počítačové síti zákazníka 6](#_Toc182574314)

[5.2.2 Databáze zákazníků v prostředí počítačové sítě ASOL 6](#_Toc182574315)

[6 Ochrana koncových zařízení v počítačové síti ASOL 8](#_Toc182574316)

[7 Předávání dat 9](#_Toc182574317)

[7.1 FTP Server 9](#_Toc182574318)

[7.2 Další možnosti předávání dat 10](#_Toc182574319)

[8 Provoz IS formou služby bez vlastního HW a SW 10](#_Toc182574320)

[9 Interní politika využívání cloudových služeb 10](#_Toc182574321)

[10 Řízení rizik 11](#_Toc182574322)

[11 Ochrana osobních údajů (GDPR) 11](#_Toc182574323)

# Účel

Tato směrnice popisuje pravidla a postupy, jejichž dodržování zajišťuje bezpečnost počítačové sítě společnosti Asseco Solutions, a.s. (dále jen „ASOL“) a ochranu dat a osobních údajů v této síti, stejně jako ochranu počítačových sítí a osobních dat zákazníků, se kterými pracovníci ASOL mohu pracovat při zajišťování podpory zákazníků, kteří používají její produkty (informační systémy „HELIOS“).

Zajišťuje splnění povinností vyplývajících zejména ze zákona č. 110/2019 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění a Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů; známé pod označením „GDPR“).

# Platnost

Tato směrnice je součástí směrnicové základny integrovaného systému managementu kvality a bezpečnosti informací společnosti Asseco Solutions a.s. (dále jen ASOL) a je závazný pro všechny pracovníky ASOL.

# Použité zkratky a pojmy

## Zkratky

**ASOL** – Společnost Asseco Solutions a.s., IČ: 64949541

**DB** – Databáze ASOL nebo zákazníka

**DPO** – pověřenec pro ochranu osobních údajů (Data Protection Officer)

**IMS** – Incident Management systém – systém evidence a řešení bezpečnostních problémů v počítačové síti ASOL

**IS** – Informační Systém

**TO** – Technické oddělení

**VIS** – Vnitřní informační systém

**VPN** – Virtual private network – zabezpečení přístupu a komunikace mezi počítačovými sítěmi

## Pojmy

**Helpdesk** – systém zajišťující evidenci požadavků Pracovníků ASOL na podporu počítačové sítě

**CLOUD** – provozování IS bez nutnosti zajištění a provozu vlastního HW a SW (např. pomocí služby ERPORT nebo Microsoft Azure)

**Pracovník ASOL** – Zaměstnanec/pracovník ASOL nebo osoba řádně pověřená ze strany ASOL (konzultant, provozní programátor, technik apod.)

**Servisní zásah** – činnost pracovníka ASOL, která je zaměřena na řešení požadavků zákazníků týkajících se problémů a chyb (vad) v produktech ASOL. Servisní zásah může být realizován například prostřednictvím:

* Vzdáleného přístupu do počítačové sítě zákazníka
* Prací s DB nebo jinými datovými soubory zákazníka v počítačové síti zákazníka nebo v počítačové síti ASOL

**Je v zájmu zákazníka jakožto správce osobních údajů mít ještě před realizací vzdáleného přístupu uzavřenou s ASOL smlouvu o zpracování osobních údajů. ASOL v tomto směru poskytuje zákazníkům podporu formou distribuce vzorového dokumentu „Smlouva o zpracování osobních údajů a Smlouva o podmínkách Sdílení dat“, viz** [**https://www.helios.eu/gdpr**](https://www.helios.eu/gdpr)**.**

**Záznam informací o provedeném servisním zásahu –** každý pracovník ASOL je povinný provést záznam o provedeném servisním zásahu. Tento záznam musí být uložen ve VIS, v pořadači, který tým pracovníka ASOL pro záznam prací pro zákazníky používá – např. Poskytnuté služby, Kauzy hotline, Kontaktní jednání apod. Záznam musí vždy obsahovat informace, kdo, kdy, a jakou práci pro zákazníka provedl. V případě, že během jednoho dne pracovník ASOL provedl pro zákazníka více zásahů, je možné provést pouze jeden záznam, který bude obsahovat souhrnné informace o všech pracovníkem ASOL v daný den provedených zásazích. Pro záznam informací je možné použít následující postupy/nástroje:

* Záznam ve VIS, provedený pracovníkem ASOL
* Log vzdáleného přístupu (VPN klienta, Teamviewer, Terminálového přístupu apod.)
* TeamViewer „Session recording“ – záznam celé relace vzdáleného přístupu a všech aktivit prováděných během vzdáleného přístupu

# Politiky bezpečnosti informací

## Politika ochrany osobních údajů

Společnost nezpracovává a nevyužívá osobní údaje jako primární součást svých obchodních aktivit ani ve velkém rozsahu pro komerční účely. Společnost shromažďuje a zpracovává osobní údaje v omezeném a nezbytném rozsahu odůvodněném oprávněným zájmem, dále v souladu s legislativními požadavky a zásadami systému řízení ochrany osobních údajů (PIMS) podle ISO 27701 k

 následujícím účelům:

* administrace pracovně-právních vztahů, v rozsahu údajů vyplývajících z legislativních požadavků,
* v souvislosti s organizačními a komunikačními potřebami společnosti,
* v souvislosti s plněním smluv pro společnost závazných, uzavíraných s klienty, s dodavateli nebo jinými třetími stranami.

Bezpečnostní politika:

* Osobní údaje jsou chráněny a zpracovávány v souladu s bezpečnostními opatřeními stanovenými ISO 27701 a interní bezpečnostní politikou společnosti
* Žádná data obsahující osobní údaje nejsou volně přístupná. Výjimku tvoří jen základní kontaktní údaje osoby pro účely komunikace uvnitř a navenek.
* Ochrana osobních údajů je zajištěna kombinací fyzického zabezpečení prostor a zabezpečení elektronických systémů.
* Data nacházející se v evidencích obsahujících osobní údaje jsou zpřístupňována jen osobám, z jejichž náplně práce vyplývá potřeba přístupu k osobním údajům. Tyto osoby musí být obeznámeny se zásadami zacházení s osobními údaji a zavázané k jejich dodržování.
* Přidělování přístupových údajů do jednotlivých systémů obsahující osobní údaje je řízené v souladu s politikou přístupu, viz OP Řízení přístupových práv.
* Osobní údaje jsou předávány třetím osobám pouze v odůvodněných případech a v nezbytném rozsahu (plnění povinností společnosti ve vztahu k veřejné správě, plnění smluvních povinností, komunikace společnosti navenek apod.).
* Každá dotčená osoba je oprávněna podat žádost o výmaz, opravu osobních údajů či omezení zpracování osobních údajů nebo nahlásit bezpečností incident v oblasti ochrany osobních údajů. Kontaktní osobou pro tyto účely je DPO.

## Politika bezpečnosti komunikační sítě

Cílem politiky bezpečnosti komunikační sítě je zajistit ochranu informací v sítích a podpůrném síťovém vybavení pro zpracování informací.

Bezpečnostní politika:

* Při elektronickém přenosu prostřednictvím sítě nebo internetu je třeba používat bezpečnostní mechanismus WPA2.
* Pracovní stanice či mobilní zařízení musí být připojeno k internetu pouze pomocí zabezpečené a důvěryhodné sítě.
	+ Připojení z veřejných sítí je povoleno prostřednictvím VPN.
	+ Na zařízení musí být aktivní firewall.
* Pro přístup k vnitřní síti ASOL je nutné použít připojení VPN. Po provedení práce se uživatel musí z VPN odhlásit.
* Musí být uplatňováno zaznamenávání činnosti formou logů a monitorování umožňující zaznamenávání a detekci činností.
	+ Logy by měly být nakonfigurovány tak, aby zaznamenávaly informace o aktivitách všech privilegovaných účtů a důležitých aktivitách běžných uživatelských účtů.
	+ Logy musí být přístupné pouze TO a oprávněným uživatelům.
	+ Logy by měly být při archivaci bezpečně uloženy.
	+ Úpravy logů jsou přísně zakázány, měly by být chráněny před jakoukoli úpravou a neoprávněným zásahem.
* Přístup do sítě a systémů v síti a přístupová hesla musí splňovat pravidla uvedená v OP Řízení přístupových práv.

## Politika přenosu informací

Cílem politiky přenosu informací je zachovat bezpečnost informací v rámci přenosu informací mezi společností a externím subjektem. Tato politika se nevztahuje na informace veřejného charakteru.

Bezpečnostní politika:

* Informace přenášeny elektronicky je nutné chránit před neoprávněným přístupem a změnou. Je povinností k přenosu informací používat pouze bezpečné, spolehlivé a dostupné aplikace/služby.
	+ Musí být nainstalován software pro detekci a ochranu před malwarem, který může být přenesen prostřednictvím elektronických komunikací.
	+ Informace sdělovány prostřednictvím e-mailu musí být odesílány a přijímány na e-mailovou adresu @assecosol.com. Není povoleno k přijímání a k odesílání informací používat osobní e mailové adresy. Informace s omezeným přístupem musí být zašifrovány, u interních informací je šifrování doporučeno.
	+ Interní informace je možné přenášet prostřednictvím mobilního zařízení pouze na firemní telefonní čísla. Informace s omezeným přístupem není povoleno sdělovat prostřednictvím SMS.
* Přenos informací v tištěné podobě musí splňovat pravidla uvedená ve Směrnici pro řízení dokumentace a Příručce bezpečnosti informací.

# Vzdálený přístup k zákazníkům a práce s DB zákazníků

## Vzdálený přístup

Vzdálený přístup do počítačové sítě zákazníka je nezbytným předpokladem včasného řešení požadavků zákazníků týkajících se problémů a chyb (vad) v produktech ASOL. Rychlost odezvy na takové požadavky zákazníků je smluvně definována a stanovené lhůty často znemožňují řešení požadavků osobní návštěvou u zákazníka.

Z důvodu zajištění bezpečnosti počítačových sítí, dat i osobních údajů je nutné definovat možné způsoby připojení a je nutné dodržovat následující pravidla postupy.

* Pro vzdálený přístup je možné využít pouze dále definované způsoby přístupu – jiný způsob připojení je možný pouze ze závažných důvodů zákazníka akceptovaných ASOL
* Pracovník ASOL používá, pokud to konfigurace na straně zákazníka umožňuje, pro zásah vždy svoje unikátní přístupové informace (např. jméno a heslo)
* Pracovník ASOL smí provádět na serverech zákazníka pouze činnosti přímo související s účelem zřízení vzdáleného přístupu

### Přístup pomocí TeamViewer – upřednostňovaný způsob přístupu!

Pro vzdálený přístup ASOL do počítačové sítě zákazníka je přednostně používán software TeamViewer.

TeamViewer je integrován do systémů HELIOS a na jehož využívání má ASOL zakoupené licence. Připojení je plně řízeno zákazníkem a zákazník v reálném čase vidí, jakou činnost Pracovník ASOL na jeho PC vykonává. Zároveň TeamViewer obsahuje vlastní logování připojení.

Vzhledem k možnost záznamu veškerých aktivit Pracovníka ASOL v počítačové síti zákazníka a možnosti využití nejen v součinnosti se zákazníkem (přístup musí být zákazníkem povolen a může být i kdykoliv ukončen), ale i bezobslužný přístup (zákazník povolí přístup do svojí sítě a předá přístupové informace - důležité při požadavku zákazníka na zásah mimo pracovní dobu zákazníka, a tedy bez jeho součinnosti v době přístupu) je tento způsob ASOL upřednostňován a nabízen zákazníkovi jako doporučení ASOL.

Bezpečnost použití TeamViewer je následující:

* Šifrování – TeamViewer pracuje s šifrováním 2048 RSA založeným na výměně veřejných a soukromých klíčů a šifrováním relací AES (256 bitů). Tato technika je založena na stejných standardech jako https/SSL a splňuje aktuální bezpečnostní normy. Výměna klíčů také zabezpečuje plnou ochranu údajů mezi klienty. To znamená, že ani směrovací servery ASOL nemohou datový proud přečíst.
* Zabezpečení přístupu – Kromě automaticky vytvářené dynamické identifikace Partner ID vytváří TeamViewer heslo relace, které je při každém spuštění programu jiné, aby tak poskytoval další zabezpečení proti neoprávněnému přístupu do systému. Další funkce související se zabezpečením (např. přenos souborů) vyžadují další, manuální potvrzení od vzdáleného partnera. Není možné ovládat počítač zákazníka „neviditelně“. Z důvodu ochrany údajů uložených na vzdáleném počítači musí být uživatel vzdáleného počítače informován o pokusu o přístup.

Zodpovědnosti při konfiguraci připojení:

* Ve fázi zřizování přístupu se zavazují obě strany (ASOL i zákazník) spolupracovat a bez zbytečných průtahů implementovat potřebné softwarové vybavení jak na straně serveru, tak i na straně klienta, a přizpůsobit síťovou infrastrukturu tak, aby bylo možné navázat síťové spojení mezi klientem a serverem.
* ASOL je zodpovědná za zabezpečení přístupů do sítě zákazníka pouze těm Pracovníkům ASOL, kteří jsou pověřeni pracovat na úkolech souvisejících s poskytováním služeb sjednaným se zákazníkem.
* Zákazník je zodpovědný za nepřetržitý běh softwarového a jiného vybavení potřebného na síťové spojení a nesmí bez předešlého informování ASOL měnit konfiguraci klienta stejně jako síťové infrastruktury, která by měla dopad na vzdálený přístup.
* ASOL nezodpovídá za škody způsobené v případě výpadku služeb ISP zákazníka.

### Ostatní způsoby vzdáleného přístupu

**V případě požadavku zákazníka na jiný způsob vzdáleného přístupu mimo TeamViewer (technické důvody, striktně definované postupy na straně zákazníka apod.) je možné využít i jiné způsoby vzdáleného přístupu – např.:**

* VPN přístup

Z důvodu bezpečnosti se na PC/NTB Pracovníka ASOL pro připojení k síti zákazníka pomocí VPN používá např. SW OpenVPN klient (též Sophos SSL VPN klient) apod.

* Terminálový přístup

Pro připojení ke vzdálené ploše Windows pomocí veřejné IP zákazníka lze využít výhradně Remote Desktop klienta integrovaného v operačním systému Windows. Z důvodu nízké úrovně zabezpečení není tento způsob doporučen.

* Microsoft Teams

V tomto případě je možné použít „sdílení plochy počítače“.

**Při používání takových jiných způsobů vzdáleného přístupu za bezpečnost odpovídá Pracovník ASOL, který takový jiný způsob přístupu používá.**

## Práce s DB zákazníků – v počítačových sítích ASOL a zákazníků

Přístup k DB zákazníka je nezbytným předpokladem řešení specifických problémů hlášených zákazníky, které vyžadují otestování ze strany ASOL přímo v počítačové síti zákazníka nebo v prostředí počítačové sítě ASOL, kde je možné využití vývojových nástrojů, které není možné u zákazníka instalovat z technických nebo licenčních důvodů. Vzhledem k ochraně dat a osobních údajů v DB je nutné dodržovat následující pravidla a postupy.

* Při předávání a práci s DB je nutné dodržovat definované postupy a úložiště/servery
* Pracovník ASOL používá, pokud to konfigurace na straně zákazníka umožňuje, pro zásah vždy svoje unikátní přístupové informace (např. jméno a heslo)
* Pracovník ASOL smí na serverech zákazníka provádět pouze činnosti související s účelem poskytnutí DB

### Přístup k DB v počítačové síti zákazníka

Přístup je možný pomocí vzdáleného přístupu – popis v bodu 4.1.

### Databáze zákazníků v prostředí počítačové sítě ASOL

DB zákazníka je možné předávat následujícími způsoby:

* Zabezpečený FTP server ASOL

Pracovník ASOL, který potřebuje doručit zákazníkovu databázi prostřednictvím zabezpečeného FTP serveru, zaregistruje na Helpdesk servisní požadavek, ve kterém požádá TO o vytvoření přístupu pro daného zákazníka na zabezpečený FTP server. Požadavek lze zadat pouze přímo na <https://helpdesk>.asol.local pomocí služby „Přenos zákaznické DB“, kde pracovník vyplní formulář, který musí obsahovat tyto informace:

1. **Název organizace, která databázi poskytuje**

*Název je potřebný pro správné pojmenování přihlašovacího účtu na FTP*

1. **Kontaktní email, na který bude zaslán postup na připojení k FTP**

*Na tuto adresu budou zaslány instrukce pro zákazníka, včetně návodu, jak se k FTP připojit*

1. **Kontaktní telefon, na který budou zaslány přihlašovací údaje na FTP**

*Z důvodu bezpečnosti není žádoucí posílat přihlašovací údaje emailem spolu s adresou FTP serveru, proto budou zákazníkovi, který bude nahrání databáze provádět, zaslány přihlašovací údaje v SMS*

1. **Verze MS SQL Serveru, na kterém má být databáze obnovena**

*Aby technické oddělení mohlo databázi obnovit, je nutné mu poskytnout informaci, jaká verze MS SQL Serveru má být pro obnovení použita.*

*Na databázovém serveru se nacházejí následující instance MS SQL Serveru:*

|  |  |
| --- | --- |
| *Pro iNuvio a Pantheon**SQLSRV2016**SQLSRV2017**SQLSRV2019**SQLSRV2022* | *Pro Nephrite**GREEN2016**GREEN2017**GREEN2019**GREEN2022* |

1. **Seznam uživatelů ASOL, kteří mohou do databáze přistupovat**

*Technické oddělení standardně nastavuje oprávnění „public“ na instanci a „db\_owner“ na databázi. Má-li být nastaveno jinak, též je potřeba úroveň oprávnění do požadavku specifikovat.*

1. **Souhlas zákazníka s uložením databáze**

*Bez souhlasu zákazníka s uložením databáze do prostředí Asseco Solutions, nelze databázi v našem prostředí využívat. Proto je nutné založit ve VISu na dané organizaci nové kontaktní jednání s názvem "DB souhlas", kde musí být zákazníkův souhlas přiložen i s termínem, do kdy může být databáze v naší síti uložena. Do požadavku v Helpdesku je následně potřeba přiložit odkaz na tento záznam. Souhlas může být v libovolném formátu, např. souhlasný email od zákazníka, naskenovaný dokument apod.*

1. **Přibližná doba uložení databáze**

*Doba uložení DB musí být definována v bodu 6), tedy jednoznačně odsouhlasena zákazníkem. Maximální akceptovatelná délka platnosti souhlasu s uložením DB je 1 rok. Po uplynutí této lhůty je potřeba souhlas prodloužit. V případě neprodloužení souhlasu bude DB automaticky smazána.*

1. **ID hotline/požadavku**

*V případě, že je přenos DB navázán na kauzu hotline nebo požadavek na vývoj, uveďte prosím jejich ID pro snazší dohledání souvislostí ve VISu a rychlejší odbavení požadavku. Pokud požadavek ID nemá, vyplňte pouze „N“.*

1. **Poznámka**

*Nepovinné pole pro případné upřesňující informace.*

Následně zákazník obdrží své unikátní přístupové údaje, jejichž délka platnosti je definována rovněž v požadavku na Helpdesku. Po uplynutí této doby je účet zákazníka smazán.

Na tento FTP server má v ASOL přístup pouze Technické oddělení a veškeré přístupy jsou zaznamenávány – evidence, který technik konkrétní databázi ze serveru stáhl.

Po nahrání databáze zákazníkem na zabezpečený FTP server je tato databáze Pracovníkem ASOL (technikem) přemístěna na zabezpečený databázový server, který je již přístupný dalším relevantním Pracovníkům ASOL (konzultantům či vývojářům), řešícím problémy zákazníka.

**V případě požadavku Pracovníka ASOL na umístění databáze na jiném místě v počítačové síti ASOL než na k tomu účelu připraveném zabezpečeném SQL Serveru, za bezpečnost dat (omezení přístupu k DB, smazání DB ihned po vyřešení problému, zákaz předání DB jinam, záznam práce s DB) odpovídá Pracovník ASOL, který DB na jiné místo ukládá. Nezbytnou podmínkou umístění DB na takovém jiném místě je požadavek Pracovníka ASOL zaslaný do Helpdesku, který obsahuje údaje o zákazníkovi, důvodu jiného umístění DB a doby trvání umístění DB.**

* Přenosné úložiště (NTB, flashdisk, externí HDD, CD, DVD)

V případě, že Pracovník ASOL obdrží od zákazníka databázi na přenosném úložišti, je tento Pracovník ASOL povinen informovat prostřednictvím Helpdesku TO a neprodleně databázi nahrát na databázový server a veškeré úpravy a testování databáze provádět již na tomto serveru a neponechávat databázi na svém PC/NTB, ani jiných místech v počítačové síti ASOL neb dokonce mimo tuto síť.

* Vzdálené připojení (VPN, RDP, TeamViewer apod.)

Je popsáno v bodu 4.1.

Pracovník ASOL je povinen informovat prostřednictvím Helpdesku TO a neprodleně databázi nahrát na databázový server a veškeré úpravy a testování databáze provádět již na tomto serveru a neponechávat databázi na svém PC/NTB, ani jiných místech v počítačové síti ASOL nebo dokonce mimo tuto síť.

* Datové úložiště zákazníka (jiné FTP, Sharepoint, OneDrive, webový odkaz apod.)

Výjimečné řešení, použitelné výhradně ze závažných důvodů zákazníka akceptovaných ASOL. Zákazníka je v takovém případě nutné informovat o riziku, že se jeho databáze dostává do rukou třetí strany a jeho data jsou snáze zneužitelná, protože ASOL nemá plnou kontrolu nad případným smazáním databáze z úložiště, či naopak nechtěným dlouhodobým uchováním databáze v rukou třetí strany. V tomto případě je nezbytné nabídnout zákazníkovi jinou, bezpečnější cestu, jak databázi do prostředí ASOL doručit (ideálně zabezpečený FTP server ASOL).

# Ochrana koncových zařízení v počítačové síti ASOL

Počítače, notebooky i mobilní zařízení (tablety a mobilní telefony), které se připojují do počítačové sítě ASOL používají dále definovanou ochranu. Instalaci a konfiguraci provádí TO.

* Stolní počítače
	+ Trend Micro Deep Security Agent
	+ pravidelně aktualizována virová databáze
	+ skenování hrozeb v reálném čase
* Notebooky
	+ Trend Micro Deep Security Agent
		- Schopnost aktualizovat virové databázi i mimo firemní síť
		- Skenování hrozeb v reálném čase
	+ Bitlocker – povinné šifrování pro všechny notebooky, na kterých uživatelé pracují s firemními daty a daty zákazníků na lokálním disku
* BYOD – bring your own device – použití vlastních zařízení Pracovníků ASOL v počítačové síti ASOL je zakázáno
* Mobilní telefony
	+ Trend Micro Mobile Security – povinné zabezpečení mobilních zařízení používaných Pracovníky ASOL
	+ Antivirus a šifrování mobilních zařízení
	+ Povinnost zabezpečit mobilní telefon či tablet prostředky ASOL se týká i všech soukromých zařízení, využívaných pro firemní účely, a obsahují tudíž firemní data
* Vzdálené připojení Pracovníků ASOL do počítačové sítě ASOL
	+ Každý Pracovník ASOL má právo připojení do firemní sítě pomocí VPN, o povolení netřeba žádat
	+ Pro připojení se používá výhradně Sophos Connect a OpenVPN
	+ Pro připojení je použito dvoufázové ověření pomocí autentikátoru spárovaného s QR kódem vygenerovaným při instalaci VPN klienta
	+ Pracovník ASOL se připojí k interní síti doménovým loginem a certifikátem X.509 vygenerovaným na firewallu Sophos při instalaci VPN klienta a šestimístným kódem, vygenerovaným výše zmíněným autentikátorem

# Předávání dat

Jedná se o přenos dat v rámci ASOL a mezi ASOL a externími subjekty.

## FTP Server

Pro předávání DB a obecně dat (včetně osobních údajů) se zákazníky firmy ASOL TO poskytuje zabezpečený FTP server-protokol FTPS / SFTP.

* každý Pracovník ASOL, který potřebuje přistupovat na server (primárně pouze administrátoři v rámci TO) používá vlastní účet
* zákazník vždy obdrží unikátní jednorázový přístup
* adresářová struktura rozdělena podle zákazníků, vždy s příslušnými právy
* změny provedené na serveru jsou zaznamenávány (logovány)
* **V případě nutnosti – požadavku vedoucího týmu, na možnost přístupu jiných Pracovníků ASOL (než pracovníků TO) na FTP server je nezbytnou podmínkou požadavek vedoucího týmu zaslaný do Helpdesku, který obsahuje údaje o zákazníkovi a Pracovníkovi ASOL, který přístup bude používat. Za bezpečnost dat (omezení přístupu k DB, smazání DB ihned po vyřešení problému, zákaz předání DB jinam, záznam práce s DB) v takovém případě odpovídá Pracovník ASOL, který přístup používá.**

## Další možnosti předávání dat

Další možnosti předávání dat a DB jsou popsány v bodu 5.2.2. Pokud zákazník použije pro předání jiný způsob, je nutné zákazníka a TO ASOL neprodleně informovat o porušení bezpečnostních zásad, data neprodleně umístit na bezpečné úložiště a z jiného umístění data neprodleně smazat.

ASOL nemůže předat data zákazníků partnerům. Pokud je partner potřebuje zpracovávat, tak je musí získat přímo od zákazníka, případně je zpracovávat v prostředí ASOL.

ASOL a TO zodpovídá pouze za bezpečnost dat umístěných nebo předávaných pomocí definovaných a zabezpečených úložišť.

Výjimkou je možnost **předávání dat prostřednictvím elektronické pošty, které je například v produktu HELIOS Red integrováno.**

**Prostřednictvím elektronické pošty je možné data předávat, je však nezbytná data od zákazníka zasílat pouze na definované mailové adresy (potřebné poštovní schránky na základě požadavku jednotlivých týmů zaslaných do Helpdesku zajistí a zabezpečí TO). Přístup do takových poštovních schránek pro jednotlivé Pracovníky ASOL nebo skupiny Pracovníků ASOL zajistí TO opět na základě požadavku zaslaného do Helpdesku. Za bezpečnost dat (omezení přístupu dalších Pracovníků ASOL, zákaz předání dat jiným Pracovníkům ASOL nebo mimo firmu, smazání dat ihned po skončení důvodu jejich použití) zodpovídá Pracovník ASOL, který s daty pracuje.**

**Zároveň doporučujeme data předávaná pomocí elektronické pošty předávat zašifrovaná.**

# Provoz IS formou služby bez vlastního HW a SW

ASOL nabízí svým zákazníkům možnost poskytnutí informačního systému včetně potřebného HW a SW formou služby. V takové případě ASOL, jako dodavatel, instaluje informační systém do datového centra poskytovatele. Do tohoto prostředí mají přístup výhradně uživatelé definovaní zákazníkem jako jeho pracovníci a definovaní Pracovníci ASOL, kteří provádějí správu.

Bezpečnost je založena na definici poskytovatele datového centra.

Společností ASOL jsou poskytovány dvě platformy řešení:

* ERPORT – poskytovatelem je ASOL a její smluvní partner, společnost Geetoo CZ s.r.o., IČ 26846993)
* Prostředí Microsoft Azure – řešení firmy Microsoft – podrobně viz stránky Micosoft - <https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx>

# Interní politika využívání cloudových služeb

* Zaměstnanci mohou využívat pouze ty cloudové služby, které jsou výhradně spravovány Technickým oddělením.
* Pro interní účely je využíváno prostředí Microsoft 365 a JIRA.
* Každý zaměstnanec, který má přístup na tyto služby, přistupuje vlastním uživatelským účtem a příslušnou licencí.
* Přístupy pro externí spolupracovníky jsou řízeny na základě požadavků v helpdeskovém systému Requestor, nebo správcem JIRA.
* Bezpečnost je založena na pravidelné analýze rizik, kterou provádí mezinárodní IT skupina ve spolupráci s externím dodavatelem, kdy na základě těchto analýz jsou přijímána příslušná opatření.
* Pro zabezpečení Microsoft 365 je využívána licence Microsoft 365 E3 a přídavná licence E5 Security Addon. Bližší popis jednotlivých zabezpečovacích prvků - <https://m365maps.com/files/Microsoft-365-Enterprise-All.htm>

# Řízení rizik

Rizika jsou řízena ve VIS v souladu se Směrnicí pro řízení kvality. ASOL provozuje IMS – Helpdesk pro evidenci bezpečnostních incidentů zjištěných uživateli a správci počítačové sítě (Pracovníky ASOL), jejich ověření TO ASOL a další zpracování, včetně případného řešení.

# Ochrana osobních údajů (GDPR)

V případě práce s osobními údaji je zapotřebí postupovat v souladu se zákonem č. 110/2019 Sb. o zpracování osobních údajů a nařízením evropského parlamentu a rady (EU) 2016/679 a z toho vycházející řízené dokumentace ASOL(zejména s operativním pokynem pro Zpracování osobních údajů kontaktních osob).