Název dokumentu:	**SMĚRNICE Bezpečnost počítačové sítě a ochrana osobních údajů**
Garant dokumentu:	Vedoucí technického oddělení

OBSAH:

1 ÚČEL

Tato směrnice popisuje pravidla a postupy, jejichž dodržování zajišťuje bezpečnost počítačové sítě společnostíAnsuzs r.o. a ochranu dat a osobních údajů v této síti, stejně jako ochranu počítačových sítí a osobních dat zákazníků, se kterými pracovníci mohou pracovat při zajišťování podpory zákazníkům.

Dokument 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“).

2 PLATNOST

Tato směrnice je součástí směrnicové základny integrovaného systému managementu kvality a informační bezpečnosti společnostíAnsuz s r.o. (dále jen ANS) a je závazný pro všechny pracovníky ANS.

3 POUŽITÉ ZKRATKY A POJMY

3.1 Zkratky

ANS – Ansuz, s.r.o.

ASOL – Asseco Solutions, a.s.

DB – databáze ANS nebo zákazníka

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

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

IS – informační systém

TO – technické oddělení

VPN – Virtual Private Network – zabezpečení přístupu a komunikace mezi počítačovými sítěmi

3.2 Pojmy

Helpdesk – vnitřní systém pro evidenci požadavků uživatelů

- ANS - zadání požadavku zasláním požadavku na mail helios@ansuz.cz

Technické oddělení – pracovníci technického oddělení ANS.

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

Pracovníci – osoby vykonávající pracovní činnost pro společnosti na základě smluvního vztahu.

Servisní zásah – činnost pracovníka, která je zaměřena na řešení požadavků zákazníků týkajících se problémů a chyb (vad) v produktech ASOL a ANS. Servisní zásah může být realizován dle pravidel uvedených v kap. 5 této směrnice.

Je v zájmu zákazníka jakožto správce osobních údajů mít ještě před realizací vzdáleného přístupu uzavřenou smlouvu o zpracování osobních údajů s ANS. V tomto směru je poskytován zákazníkům vzorový dokument „Smlouva o zpracování osobních údajů a Smlouva o podmínkách Sdílení dat“

Záznam informací o provedeném servisním zásahu – každý pracovník je povinný provést záznam o provedeném servisním zásahu. Tento záznam musí být uložen. Záznam musí vždy obsahovat

informace, kdo, kdy, a jakou práci pro zákazníka provedl. V případě, že během jednoho dne pracovník provedl pro zákazníka více zásahů, je možné provést pouze jeden záznam, který bude obsahovat souhrnné informace o všech pracovníkem v daný den provedených zásazích. Pro záznam informací je možné použít následující postupy/nástroje:

- Záznam, provedený pracovníkem
- Log vzdáleného přístupu (VPN klienta, RustDesk, Terminálového přístupu apod.)
- RustDesk „Session recording“ – záznam celé relace vzdáleného přístupu a všech aktivit prováděných během vzdáleného přístupu

4 POLITIKY INFORMAČNÍ BEZPEČNOSTI

4.1 Politika ochrany osobních údajů

Společnosti nezpracovávají a nevyužívají osobní údaje jako primární součást svých obchodních aktivit ani ve velkém rozsahu pro komerční účely. Společnosti shromažďují a zpracovávají 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.
- 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 ANS.

4.2 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 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 stanovená pravidla.

4.3 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 *@ansuz.cz. 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 není povolen.

4.4 Politika využívání cloudových služeb

- Pracovníci mohou využívat pouze ty cloudové služby, které jsou výhradně spravovány technickým oddělením.
- Pro interní účely je využíváno prostředí Microsoft 365, Google Cloud a ERPORT.
- Každý zaměstnanec, který má přístup na tyto služby, přistupuje vlastním uživatelským účtem a příslušnou licencí.
- 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

5 VZDÁLENÝ PŘÍSTUP K ZÁKAZNÍKŮM A PRÁCE S DB ZÁKAZNÍKŮ

5.1 Vzdálený přístup

Vzdálený přístup do počítačové sítě zákazníka je nezbytným předpokladem včasného řešení požadavků zákazníků týkajících se problémů a chyb (vad) v produktech ASOL nebo ANS. 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, a to až po schválení vedoucím technického oddělení.
- Pracovník používá, pokud to konfigurace na straně zákazníka umožňuje, pro zásah vždy svoje unikátní přístupové informace (např. jméno a heslo).
- Pracovník smí provádět na serverech zákazníka pouze činnosti přímo související s účelem zřízení vzdáleného přístupu.

5.1.1 Přístup pomocí RustDesk– upřednostňovaný způsob přístupu!

Pro vzdálený přístup do počítačové sítě zákazníka je přednostně používán software RustDesk a Rychlý pomocník. Připojení je plně řízeno zákazníkem a zákazník v reálném čase vidí, jakou činnost pracovník na jeho PC vykonává.

Vzhledem k možnost záznamu veškerých aktivit pracovníka 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 upřednostňován a nabízen zákazníkovi jako doporučení.

Bezpečnost použití RustDesk je následující:

- Šifrování – RustDesk využívá end-to-end šifrování (E2EE) založené na asymetrické kryptografii (typicky RSA encryption) pro výměnu klíčů a symetrické šifrování relace (AES-256 encryption). Veškerá komunikace mezi klienty je šifrována a servery nemají přístup k obsahu přenášených dat.
- Zabezpečení přístupu – Přístup ke vzdálenému zařízení je chráněn pomocí ID a hesla relace. Heslo může být jednorázové (mění se při každém spuštění) nebo trvalé dle konfigurace. Pro zvýšení bezpečnosti je nastaven whitelist povolených zařízení, dvoufaktorové ověření (2FA) a další omezení přístupu. Uživatel vzdáleného zařízení má kontrolu nad tím, kdo se připojí.
- Vlastní infrastruktura (self-hosting) – RustDesk umožňuje provoz vlastního serveru (HBBS/HBBr), což znamená, že veškerá signalizace i relay komunikace může probíhat v rámci vlastní infrastruktury (např. on-premise nebo ve firemním cloudu). Tím lze eliminovat závislost na veřejných serverech a splnit přísnější bezpečnostní nebo legislativní požadavky (např. GDPR, interní compliance). Zodpovědnosti při konfiguraci připojení:
- Ve fázi zřizování přístupu se zavazují obě strany (ANS 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.

- ANS je zodpovědná za zabezpečení přístupů do sítě zákazníka pouze těm pracovníkům, 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 měnit konfiguraci klienta stejně jako síťové infrastruktury, která by měla dopad na vzdálený přístup.
- ANS nezodpovídá za škody způsobené v případě výpadku služeb ISP zákazníka.

5.1.2 Ostatní způsoby vzdáleného přístupu

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

- VPN přístup
- Terminálový přístup
- Rychlý pomocník

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, který takový jiný způsob přístupu používá.

5.2 Práce s DB zákazníků – v počítačových sítích ANS a zákazníků

Přístup k DB zákazníka je nezbytným předpokladem řešení specifických problémů hlášených zákazníky, které vyžadují otestování ze strany ANS přímo v počítačové síti zákazníka nebo v prostředí počítačové sítě ANS, 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 používá, pokud to konfigurace na straně zákazníka umožňuje, pro zásah vždy svoje unikátní přístupové informace (např. jméno a heslo).
- Pracovník smí na serverech zákazníka provádět pouze činnosti související s účelem poskytnutí DB.

5.2.1 Přístup k DB v počítačové síti zákazníka

Přístup je možný pomocí vzdáleného přístupu – popis v kap. 5.1 této směrnice.

5.2.2 Databáze zákazníků v prostředí počítačové sítě ANS

DB zákazníka je možné předávat následujícími způsoby:

- Zabezpečený FTP server

Pracovník, 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 do helpdesku 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

2) 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

3) 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

4) 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 Easy
SQLSRV2016
SQLSRV2017
SQLSRV2019
SQLSRV2022

5) 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.

6) Souhlas zákazníka s uložením databáze

Bez souhlasu zákazníka s uložením databáze do prostředí ANS, nelze databázi v našem prostředí využívat. Proto je nutné uložit zákazníkův souhlas přiložen i s termínem, do kdy může být databáze v naší síti uložena. Souhlas může být v libovolném formátu, např. souhlasný email od zákazníka, naskenovaný dokument apod.

7) 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.

8) 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 a rychlejší odbavení požadavku. Pokud požadavek ID nemá, vyplňte pouze „N".

9) 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 ANS 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 ANS (technikem) přemístěna na zabezpečený databázový server, který je již přístupný dalším relevantním Pracovníkům (konzultantům či vývojářům), řešícím problémy zákazníka.

V případě požadavku pracovníka na umístění databáze na jiném místě v počítačové síti ANS 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, který DB na jiné místo ukládá. Nezbytnou podmínkou umístění DB na takovém jiném místě je požadavek pracovníka 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 obdrží od zákazníka databázi na přenosném úložišti, je tento pracovník povinen informovat 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 ANS neb dokonce mimo tuto síť.

- Vzdálené připojení (VPN, RDP, RustDesk apod.)

Je popsáno v kap. 5.1 této směrnice.

Pracovník je povinen informovat 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 ANS nebo dokonce mimo tuto síť.

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

Výjimečné řešení, použitelné výhradně ze závažných důvodů zákazníka akceptovaných ANS. 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 ANS 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 ANS doručit (ideálně zabezpečený FTP server ANS).

6 PŘEDÁVÁNÍ DAT

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

6.1 FTP Server

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

- Každý pracovník, 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).

6.2 Další možnosti předávání dat

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

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

Společnosti zodpovídají pouze za bezpečnost dat umístěných nebo předávaných pomocí definovaných a zabezpečených úložišť.

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 nebo skupiny pracovníků zajistí TO opět na základě požadavku zaslaného do helpdesku. Za bezpečnost dat (omezení přístupu dalších pracovníků, zákaz předání dat jiným pracovníkům nebo mimo firmu, smazání dat ihned po skončení důvodu jejich použití) zodpovídá pracovník, který s daty pracuje.

Zároveň doporučujeme data předávaná pomocí elektronické pošty předávat zašifrovaná.

7 PROVOZ IS FORMOU SLUŽBY BEZ VLASTNÍHO HW A SW

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

Bezpečnost je založena na definici poskytovatele datového centra.

Společnostmi 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 Microsoft - https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

8 ŘÍZENÍ RIZIK

Rizika jsou řízena v souladu se Směrnicí pro řízení kvality.

9 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 (zejména s operativním pokynem pro Zpracování osobních údajů kontaktních osob).