**Plán zabezpečení informací**

**Rozsah:** Tento plán informační bezpečnosti (dále jen "PZI") je začleněn do objednávkového formuláře mezi společností Infor a v něm uvedeným zákazníkem a stanoví aktuální bezpečnostní opatření společnosti Infor, která jsou určena k ochraně:

i. hardware, zařízení a konfigurace systémového softwaru, na kterém společnost Infor poskytuje:

a. Cloudové služby (pro přehlednost Cloudové služby zahrnují i podporu).

b. Profesionální služby, a

c. Podporu s ohledem na On-Premise software

(veškerý takový hardware, zařízení a konfigurace systémového softwaru jsou v tomto ISP souhrnně definovány jako "Systémy" a Cloudové služby, Profesionální služby a Podpora k On-Premise softwaru jsou v tomto PZI souhrnně definovány jako "Služby"); jakož i

ii. Zákaznická data poskytnutá společnosti Infor, a to buď:

a. jako Zákaznická data, nebo

b. jako data poskytnutá společnosti Infor pro účely provádění Profesionálních služeb a/nebo Podpory z prostředí společnosti Infor.

(všechna tato data jsou v této PZI souhrnně definována jako "Data").

**Definice:** Výrazy s velkými písmeny použité v tomto PZI a nedefinované v tomto PZI mají význam, který je těmto výrazům přiřazen ve Smlouvě o softwaru mezi společností Infor a takovým Zákazníkem ("Smlouva").

**Výjimky:** Tento PZI se nevztahuje na: (i) ujednání o profesionálních službách Infor, kdy je zákazníkův on-premise software hostován společností Infor na základě samostatně sjednané smlouvy o profesionálních službách, nebo (ii) kdy společnost Infor poskytuje služby v prostorách zákazníka a/nebo má přístup k zákaznickým systémům. V takových případech Infor dodrží administrativní, technické a fyzické podmínky Zákazníka, jak byly vzájemně dohodnuty ve výkazu práce, a v souvislosti s jakýmkoli takovým přístupem do systémů Zákazníka odpovídá Zákazník za to, že poskytne pracovníkům Infor uživatelská oprávnění a hesla pro přístup do svých systémů a odvolá taková oprávnění a ukončí takový přístup, pokud to Zákazník považuje za vhodné.

1. **Aktualizace:** Bezpečnostní hrozby a opatření určená k ochraně proti těmto bezpečnostním hrozbám se neustále vyvíjejí a společnost Infor může kdykoli změnit tohoto poskytovatele PZI bez předchozího upozornění Zákazníka, pokud společnost Infor udržuje srovnatelnou nebo lepší úroveň zabezpečení systémů a dat v souhrnu. **Obecné bezpečnostní standardy**

Infor udržuje administrativní, technická a fyzická bezpečnostní opatření určená k ochraně před zničením, ztrátou, neoprávněným přístupem nebo změnou Systémů a Dat Zákazníka, která Infor zpracovává na pokyn Zákazníka, a tato opatření jsou: (i) minimálně tak přísná jako opatření, která Infor udržuje pro své vlastní informace podobné povahy; (ii) minimálně tak přísná jako obecně přijímané průmyslové standardy; a jsou (iii) vyžadovaná platnými právními předpisy.

1.1. **Bezpečnostní pracovníci**

Infor určil jednoho nebo více bezpečnostních pracovníků odpovědných za koordinaci a monitorování bezpečnostních opatření v tomto PZI.

1.2. **Řízení přístupu**

Infor zřídí kontrolu přístupu k Datům Zákazníka, včetně následujících opatření:

i. Infor přiřazuje každé osobě s počítačovým přístupem k Datům Zákazníka jedinečné ID.

ii. Infor určuje pracovníky, kteří mohou udělovat, měnit nebo rušit přístup k Datům Zákazníka, a omezuje přístup k Datům Zákazníka na základě minimálních oprávnění. Přístup k Datům Zákazníka je povolen pouze pracovníkům, kteří je „potřebují znát“ za účelem poskytování Předplacených služeb, a Infor vede a aktualizuje záznamy o těchto pracovnících. Takový přístup je zaznamenáván a monitorován.

iii. Infor instruuje své pracovníky, kteří mají přístup k Datům Zákazníka, aby vypínali funkci správce systému, pokud jsou počítače ponechány bez dozoru.

iv. Infor deaktivuje účty zaměstnanců společnosti Infor z aplikací nebo datových úložišť, které obsahují Data Zákazníka, když tito zaměstnanci ukončí pracovní poměr nebo jsou převedeni nebo když již není potřeba, aby měli přístup k těmto Datům Zákazníka. Infor pravidelně reviduje seznam osob a služeb s přístupem k Datům Zákazníka a odstraňuje účty, které již takový přístup nevyžadují. Infor provádí tento přezkum minimálně dvakrát ročně.

v. Infor nepoužívá u žádného Systému výchozí hesla a další bezpečnostní parametry dodávané výrobcem. Infor nařizuje používání systémově vynucených „silných hesel" v souladu s obecně uznávanými nejlepšími odvětvovými postupy u všech Systémů Inforu. Infor vyžaduje, aby všechna hesla a přístupové údaje byly důvěrné a nebyly sdíleny mezi zaměstnanci, a hesla, o nichž je známo, že byla prolomena nebo prozrazena, Infor deaktivuje.

vi. Infor provádí „uzamčení účtu" tím, že deaktivuje účty s přístupem k Datům Zákazníka, pokud účet překročí stanovený počet po sobě jdoucích nesprávných pokusů o zadání hesla.

vii. Vzdálený přístup k Systémům, v nichž jsou uložena Data Zákazníka, vyžaduje dvoufaktorové ověření (např. vyžaduje alespoň dva samostatné faktory pro identifikaci uživatelů).

### 1.3. Detekce a prevence narušení

Infor používá systém detekce narušení/prevence narušení (IDS/IPS), který monitoruje její Systémy a postupy pro případ narušení bezpečnosti a podezřelých aktivit. To zahrnuje podezřelou externí aktivitu (zejména neoprávněné sondování, skenování nebo pokusy o vniknutí) a podezřelou interní aktivitu (zejména neoprávněný přístup správce systému, neoprávněné změny v Systémech, zneužití nebo krádež Systémů nebo nesprávné nakládání s Daty Zákazníka). Infor pravidelně prověřuje protokoly o přístupu a hledá známky škodlivého chování nebo neoprávněného přístupu.

### 1.4. Firewall

Infor udržuje technologii síťového firewallu určenou k ochraně Dat Zákazníka, která jsou přístupna prostřednictvím internetu.

### 1.5. Aktualizace

Infor udržuje Systémy v aktuálním stavu pomocí upgradů, aktualizací, oprav chyb a nových verzí.

### 1.6. Šifrování dat

i. Při přenosu přes veřejné sítě jsou Data Zákazníka šifrována minimálně protokolem TLS 1.2 nebo jeho logickým nástupcem.

ii. Když jsou Data Zákazníka v rámci Systémů v klidovém režimu, jsou šifrována minimálně 256bitovým šifrovacím algoritmem AES nebo jeho logickým nástupcem.

### 1.7. Správa identit

Infor využívá k distribuci zabezpečení model sdíleného zabezpečení. Infor má možnost federovat aplikace v Systémech zpět na poskytovatele správy identit Zákazníka.

### 1.8. Škodlivý software

Infor udržuje v oboru obecně uznávaný standardní antimalwarový/antivirový software a v rámci možností používá funkce ochrany téměř v reálném čase ve snaze poskytovat Cloudové služby, nebo Software On-Premise, které neobsahují žádné „časované bomby", „červy", „viry", „trojské koně", „ochranné kódy", „klíče k destrukci dat" ani jiná programovací zařízení, jejichž účelem je (i) (vzhledem ke Cloudovým službám) upravit , vymazat, poškodit, deaktivovat nebo zabránit Zákazníkovi v přístupu k jeho Datům Zákazníka nebo jej omezit nebo (ii) vzhledem k Softwaru On-Premise, upravit, smazat, poškodit, deaktivovat nebo zakázat data Zákazníka v Softwaru On-Premise.

### 1.9. Fyzická bezpečnost

Zařízení obsahující Systémy:

i. jsou konstrukčně navržena tak, aby odolala nepřízni počasí a dalším přiměřeně předvídatelným přírodním podmínkám;

ii. mají vhodné fyzické ochrany proti vlivům prostředí, které pomáhají chránit Systémy před poškozením kouřem, teplem, vodou, ohněm, vlhkostí nebo kolísáním elektrické energie;

iii. jsou podporována záložními zdroji energie na místě a

iv. mají vhodné kontrolní mechanismy zajišťující, že fyzický přístup k zařízení je umožněn pouze oprávněným pracovníkům.

## 2. Audit

### 2.1. **Práva na audit**

V rámci svého programu dohledu nad dodavateli si Zákazník a (případně) jeho vládní regulační orgán mohou jednou ročně vyžádat formou poštovního auditu (tj. dotazníku založeného na normě ISO 27001) od Inforu procesní dokumentaci týkající se jejího programu, procesů a kontrolních mechanismů zabezpečení informací. Infor se zavazuje, že v rozsahu, v jakém je taková procesní dokumentace snadno dostupná, poskytne takovou dokumentaci, kterou může Zákazník oprávněně požadovat, pokud taková dokumentace (a) neohrozí důvěrnost, integritu nebo dostupnost dat nebo služeb jiných zákazníků Inforu nebo (b) neporuší důvěrnost, integritu a dostupnost dat nebo služeb třetích stran, které poskytují Zákazníkovi jménem Inforu Předplatitelské služby. Procesní dokumentace poskytovaná Inforem nebude zahrnovat důkazy (např. zejména důkaz o školení, důkaz o testování, výsledky hodnocení rizik). Infor odpoví na dotazník do 30 dnů; pokud tento časový rámec nelze dodržet, bude Infor spolupracovat se Zákazníkem s cílem dosáhnout dohody o poskytnutí odpovědí. Veškerá taková dokumentace představuje důvěrné informace Inforu. Infor nebude brát v úvahu zjištění Zákazníka vyplývající z tohoto poštovního auditu.

### 2.2. **Audit třetí stranou**

Jednou za každých 12 měsíců během Předplaceného období je Infor povinen na své náklady najmout řádně kvalifikovaného nezávislého auditora, který provede prověrku návrhu a provozní účinnosti definovaných kontrolních cílů a kontrolních činností v souvislosti s Cloudovými službami (s výjimkou Podpory) Infor nechá takového auditora připravit zprávu typu SOC I typu 2 pro všechny Cloudové služby a pro mnohoúčelové Cloudové služby pouze zprávu typu SOC II typu 2 („Zpráva o auditu“). Zpráva o auditu představuje důvěrné informace Inforu, avšak je k dispozici Zákazníkovi na portálu podpory Inforu. Zákazník může sdílet kopii takové Zprávy o auditu se svými auditory a regulačními orgány za předpokladu, že auditoři a regulační orgány jsou informováni o tom, že taková Zpráva o auditu představuje důvěrné informace Inforu a musí být odpovídajícím způsobem chráněna.

Kromě toho Infor jednou za 12 měsíců během Předplaceného období na své náklady zapojí řádně kvalifikovaného nezávislého auditora k provádění revize své informační bezpečnosti související s určitými mnohoúčelovými Cloudovými službami uvedený na trust.infor.com stejně jako Podporu pro jakýkoli Software On Premise a Cloudové služby v souladu s mezinárodní normou pro standardizaci (ISO) 27001. Infor zajistí, aby tento auditor vypracoval zprávu v souladu s touto normou. Zpráva o auditu nebude Zákazníkovi k dispozici; Zákazník může nicméně kdykoli získat kopii výsledného certifikátu na webové stránce společnosti Infor týkající se cloudového zabezpečení (trust.infor.com). Certifikát bude označovat software, který je předmětem zprávy. Součástí této certifikace ISO 27001 je manuál o řízení informační bezpečnosti pro software zahrnutý v certifikaci a související Podpora, které pomáhají zajistit ochranu, důvěrnost, integritu a dostupnost aktiv Infor používaných k poskytování těchto služeb.

## 3. Řízení změn

Infor má zaveden proces řízení změn, který řídí identifikaci a implementaci změn v rámci zdrojů pro poskytování Cloudových Služeb Inforu, aby zabraňoval nežádoucím změnám zdrojového kódu aplikace, rozhraní, operačních systémů nebo back-endovým změnám dat v rámci stávajících polí a tabulek. Všechny požadované změny zdrojů pro poskytování Cloudových Služeb Inforu se musejí řídit procesem řízení změn implementace. Infor dokumentuje a uchovává podrobné záznamy o dodržování tohoto procesu, jako např. systém ticketů a záznamy o testovacích postupech pro každou změnu, zahrnující mimo jiné datum a čas každé takové změny a popis povahy změny.Segregace údajů o zákaznících; žádné zneužití

## 4. Segregace dat; Zákaz zneužití

### 4.1. Segregace

Data Zákazníka jsou vhodnými technickými prostředky logicky oddělena od dat Inforu a dat jakéhokoli jiného zákazníka Inforu.

### 4.2. Zákaz zneužití; souhrnné statistiky

Data Zákazníka představují důvěrné informace Zákazníka a Zákazník vlastní veškerá majetková práva ke svým Datům Zákazníka. Infor nebude komerčně využívat Data Zákazníka a nebude přistupovat k Datům Zákazníka jinak, než jak je to nutné k provádění Předplacených služeb a plnění svých povinností v souladu se Smlouvou.

Infor může shromažďovat Souhrnné statistiky, které jsou výhradním vlastnictvím Inforu a nepovažují se za Data Zákazníka. „Souhrnné statistiky“ jsou statistické údaje a informace o výkonu, generované prostřednictvím nástrojů a přihlašovacích systémů, týkající se používání a provozu Předplaceného softwaru a Předplacených služeb Zákazníkem.

**5. Správa aktiv**

Infor má zaveden formální proces správy aktiv, který zahrnuje

i. vedení soupisu aktiv používaných k poskytování Předplacených služeb („Aktiva“), stanovení jasného vlastnictví a kontroly nad Aktivy, schopnost identifikovat Aktiva a řídit jejich vrácení, zničení nebo odstranění Dat Zákazníka z příslušných Aktiv; a

ii. postupy určené k ochraně Aktiv před hrozbami a zranitelnostmi, ať už interními nebo externími, úmyslnými nebo náhodnými.

**6. Skenování zranitelnosti a testování prostupnosti**

Infor udržuje proces řízení Zranitelností za účelem kontroly rizik vyplývajících ze zneužití zveřejněných nebo identifikovaných chyb nebo slabých míst, které by mohly být zneužity (náhodně nebo úmyslně) a vést k újmě nebo neoprávněnému přístupu do Systémů („Zranitelnosti“). Infor bude Zranitelnosti řešit v rámci obecně uznávaných standardních časových rámců. Infor odstraní nebo zmírní Zranitelnosti způsobem odpovídajícím riziku, které tyto Zranitelnosti představují, v souladu s definovaným rámcem Inforu, který je v souladu s obecně uznávanými průmyslovými standardy.

Infor každoročně na vlastní náklady zapojí nezávislou třetí stranu, která provede penetrační testování pro vícenásobné cloudové služby, včetně manuálního testování, za účelem vyhodnocení bezpečnostních kontrol Systémů s více uživateli podle obecně uznávaných standardních metodik.

U Předplaceného softwaru pro více uživatelů se před vydáním kódu a v průběhu celého životního cyklu produktu Cloud Services (tj. ve vývojovém a produkčním prostředí) provádí testování zabezpečení, včetně skenování zdrojového kódu a skenování Zranitelností, přispívající k identifikaci potenciálních Zranitelností, které je třeba odstranit nebo zmírnit. Každoročně se provádí testování víceuživatelských cloudových služeb s cílem identifikovat Zranitelnosti, které je třeba odstranit nebo zmírnit.

**7. Reakce na incidenty v oblasti zabezpečení informací**

Pokud Infor zjistí, že Data Zákazníka byla nebo by mohla být předmětem zneužití nebo zveřejnění, které tento PZI nepovoluje („Incident v zabezpečení informací“), Infor: (i) neprodleně a bez zbytečného odkladu (v každém případě do 48 hodin od okamžiku, kdy se o takovém Incidentu v zabezpečení informací dozví) oznámí Zákazníkovi výskyt takového Incidentu v zabezpečení informací; (ii) prošetří a provede přiměřenou analýzu příčiny (příčin) takového Incidentu v zabezpečení informací; (iii) pravidelně bude poskytovat Zákazníkovi aktuální informace o probíhajícím šetření; (iv) vypracuje a implementuje vhodný plán nápravy příčiny takového Incidentu v zabezpečení informací v rozsahu, v jakém je taková příčina pod kontrolou Inforu; a (v) bude spolupracovat při přiměřeném vyšetřování Zákazníka nebo jeho snahou splnit jakékoli oznamovací nebo jiné právní požadavky vztahujících se k takovému Incidentu v zabezpečení informací. Na žádost Zákazníka a na jeho náklady poskytne Infor v případě Incidentu v zabezpečení informací Zákazníkovi (v rozsahu povoleném ze zákona a s výhradou patřičného zachování mlčenlivosti) kopie záznamů o příslušné činnosti Systémů (výhradně s ohledem na Incident v zabezpečení informací, pokud se týká Zákazníka) pro jejich použití v jakémkoli soudním nebo jiném zákonném řízení Zákazníka nebo při jakémkoli jeho vládním vyšetřování.

**8. Protokolování a monitorování**

Infor monitoruje své prostředky používané k poskytování Předplacených služeb pomocí sady nástrojů, speciálně nakonfigurovaných pro správu protokolů a výstrah. Záznamy protokolů jsou fyzicky i virtuálně zabezpečeny, aby bylo zabráněno jejich neoprávněné manipulaci. Citlivé informace a hesla nejsou zaznamenávány za žádných okolností. Kromě zachycování informací souvisejících se službami umožňují monitorovací nástroje správcům sledovat činnost uživatelů při vstupu do systému a výstupu z něj.

**9. Zabezpečení lidských zdrojů**

Pracovníci Inforu poskytující Předplacené služby podléhají povinnosti mlčenlivosti, jsou obeznámeni s hrozbami a problémy zabezpečení informací, absolvují alespoň jednou ročně obecné bezpečnostní školení a jsou připraveni podporovat organizační zásady zabezpečení informací obecně i v rámci svých specifických pracovních funkcí.

**10. Kontroly koncových zařízení (notebooky, pracovní stanoviště a mobilní zařízení Inforu)**

Infor má zavedena obecně uznávaná bezpečnostní opatření pro ochranu koncových bodů, včetně automatizace

správy záplat aplikací a operačních systémů a antivirové ochrany.

## 11. Vrácení a zničení dat

### 11.1. Vrácení dat

Po ukončení nebo vypršení platnosti Cloudových Služeb Infor neprodleně (do 3-5 pracovních dnů po obdržení písemné žádosti Zákazníka prostřednictvím standardního ticketu na podporu) zpřístupní Zákazníkovi veškerá Data Zákazníka ve formě exportu původní databáze poskytovaného prostřednictvím služby zabezpečeného přenosu souborů společnosti společnosti Infor. Pokud Zákazník požaduje vrácení Dat Zákazníka v alternativním formátu nebo požaduje jiné asistenční služby při ukončení, Infor a Zákazník se vzájemně dohodnou na rozsahu těchto asistenčních služeb při ukončení a na poplatcích a nákladech splatných v souvislosti s těmito asistenčními službami při ukončení. Před ukončením má Zákazník přístup k údajům Zákazníka prostřednictvím rozhraní aplikace a Zákazník může požádat prostřednictvím portálu podpory o kopie záloh dat až dvakrát za období 12 měsíců; další žádosti budou podléhat poplatkům.

Dále pro lepší srozumitelnost, vrácení nebo zničení osobních údajů bude probíhat v souladu s podmínkami Smlouvy o ochraně údajů.

### 11.2. Zničení dat

Infor trvale odstraní všechny (online nebo síťově přístupné) instance Dat Zákazníka do 30 dnů po ukončení nebo vypršení platnosti Cloudových služeb. Infor použije obecně přijímané odvětvové standardní procesy pro likvidaci hardwaru a fyzických komponent obsahujících Data Zákazníka. Veškerá úložiště jsou před nasazením nebo vyřazením z produkčního prostředí Inforu elektronicky vymazána (vynulována).

## 12. Subdodavatelé

Subdodavatelé Inforu poskytující Inforu zboží a služby v souvislosti s Cloudovými službami musí Inforu poskytovat takové zboží a služby za podmínek podstatně podobných těm, jež jsou uvedeny v tomto PZI. Před zapojením takové třetí strany do provádění jakýchkoli Cloudových služeb podle této Smlouvy Infor takového subdodavatele s přiměřenou pečlivostí prověří ve snaze zajistit, že taková třetí strana může splnit povinnosti týkající se mlčenlivosti a zabezpečení podle této Smlouvy. V rámci podpory poskytované Cloudovým službám je Infor odpovědný za všechny činnosti svých subdodavatelů.

*Odmítnutí odpovědnosti: Následující produkty mohou mít další nebo odlišné bezpečnostní podmínky: Anael (SaaS) (Francie); Nexus AppXpress (SaaS), Nexus Live Visibility (SaaS), Nexus Factory Management (SaaS), Nexus Inventory Management (SaaS), Nexus Supply Chain Finance (SaaS), Nexus Supply Collaboration (SaaS), Nexus Transportation Management (SaaS), Nexus Supply Chain Visibility (SaaS), Nexus Procure to Pay (SaaS), Nexus Supply Chain Intelligence (SaaS); BPCS/LX , XA , System 21 (SaaS).*