Plán informační bezpečnosti

Rozsah působnosti: Tento plán informační bezpečnosti („ISP“) je součástí smluv uzavřených mezi Zákazníkem a společností Infor (dále souhrnně jen „Smlouvy“). V případě jakéhokoli rozporu nebo nesouladu mezi podmínkami tohoto ISP a jakýmikoli jinými podmínkami uvedenými ve Smlouvách má přednost tento ISP. Tento ISP stanoví aktuální bezpečnostní opatření společnosti Infor, která jsou určena k zajištění ochrany obecně pro všechny Zákazníky:

i. hardware, vybavení a konfiguraci systémového softwaru, na kterém společnost Infor poskytuje:

   a. Cloudové služby (pro přehlednost zahrnují Cloudové služby také Podporu)
   b. Profesionální služby a
   c. Podpora týkající se softwaru instalovaného na místě

   (veškerý tento hardware, vybavení a konfigurace systémového softwaru jsou v tomto ISP souhrnně označovány jako „Systémy“, zatímco Cloudové služby, Profesionální služby a Podpora softwaru instalovaného na místě jsou v tomto ISP souhrnně označovány jako „Služby“); a dále

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

   a. jako Zákaznická data, nebo
   b. jako data poskytnutá společnosti Infor za účelem poskytování Profesionálních služeb a/nebo Podpory v rámci prostředí společnosti Infor

   (všechna tato data jsou v tomto ISP souhrnně označována jako „Data“).

Definice: Pojmy psané velkými písmeny, které jsou použity v tomto ISP a nejsou v něm definovány, mají význam, který jim byl přiřazen ve Smlouvě o poskytování softwaru uzavřené mezi společností Infor a daným Zákazníkem (dále jen „Smlouva“).

Výjimky: Tento ISP se nevztahuje: (i) na smlouvy o Profesionálních službách společnosti Infor, v rámci nichž společnost Infor hostuje Zákazníkův Software instalovaný na místě na základě samostatně sjednané smlouvy o Profesionálních službách, ani (ii) na situace, kdy společnost Infor poskytuje služby v prostorách Zákazníka a/nebo jí je umožněn přístup k systémům Zákazníka. V takových případech bude společnost Infor dodržovat administrativní, technické a fyzické podmínky Zákazníka, jak byly vzájemně dohodnuty v popisu práce, a v souvislosti s jakýmkoli takovým přístupem k systémům Zákazníka bude Zákazník odpovědný za poskytnutí uživatelských oprávnění a hesel zaměstnancům společnosti Infor pro přístup k jeho systémům a za zrušení těchto oprávnění a ukončení takového přístupu, jak to Zákazník považuje za vhodné.

Aktualizace: Bezpečnostní hrozby a opatření určená k ochraně před nimi se neustále vyvíjejí a společnost Infor může tuto směrnici kdykoli změnit bez předchozího upozornění Zákazníka, za předpokladu, že společnost Infor zachová celkově srovnatelnou nebo vyšší úroveň zabezpečení Systémů a Dat.

1. Obecné bezpečnostní standardy

Společnost Infor uplatňuje administrativní, technická a fyzická bezpečnostní opatření určená k ochraně před zničením, ztrátou, neoprávněným přístupem nebo pozměněním Systémů a Dat, která jsou: (i) nejméně stejně přísná jako opatření, která společnost Infor uplatňuje pro své vlastní informace podobné povahy; (ii) nejméně stejně přísná jako obecně uznávané standardy v oboru; a (iii) vyžadovaná platnými zákony. Společnost Infor nenese žádnou odpovědnost za operační systémy třetích stran a produkty a služby, které mají interoperabilitu se Systémy a které vyvíjí nebo vyvinul pro sebe Zákazník (a) nebo (b) licencuje na základě vlastních platných licenčních podmínek těchto třetích stran.

1.1. Bezpečnostní pracovníci

Společnost Infor jmenovala jednoho nebo více bezpečnostních pracovníků, kteří jsou odpovědní za koordinaci a sledování bezpečnostních opatření v tomto ISP.

1.2. Řízení přístupu

Společnost Infor zavádí opatření pro řízení přístupu k Datům, která zahrnují mimo jiné následující opatření:

i. Společnost Infor přiděluje jedinečné identifikační číslo každé osobě, která má počítačový přístup k Datům.

ii. Společnost Infor určuje zaměstnance, kteří mohou udělovat, měnit nebo rušit přístup k Datům, a omezuje přístup k Datům na základě principu nejnižšího možného oprávnění. Přístup k Datům je povolen pouze zaměstnancům, kteří mají „potřebu znát“ pro poskytování Služeb, a společnost Infor vede a aktualizuje záznamy o těchto zaměstnancích. Přístup k Datům je zaznamenáván a monitorován.

iii. Společnost Infor nařizuje svým zaměstnancům s přístupem k Datům, aby deaktivovali administrativní relace, když jsou počítače ponechány bez dozoru.

iv. Společnost Infor deaktivuje účty svých zaměstnanců v aplikacích nebo úložištích Dat, která obsahují Data, pokud jsou tito zaměstnanci propuštěni nebo přeřazeni, nebo pokud již přístup k těmto Datům nepotřebují. Společnost Infor pravidelně kontroluje seznam osob a Služeb s přístupem k Datům a odstraňuje účty, které již takový přístup nevyžadují. Společnost Infor provádí tuto kontrolu minimálně dvakrát ročně.

v. Společnost Infor nepoužívá výchozí nastavení dodaná výrobcem pro hesla a další bezpečnostní parametry na žádných Systémech. Společnost Infor na všech svých Systémech vyžaduje používání systémově vynucených „silných hesel“ v souladu s obecně uznávanými osvědčenými postupy v oboru. Společnost Infor vyžaduje, aby všechna hesla a přístupové údaje byly uchovávány v tajnosti a nebyly sdíleny mezi zaměstnanci, a deaktivuje hesla, o nichž je známo, že byla poškozena nebo prozrazena.

vi. Společnost Infor udržuje „blokování účtu“ tím, že deaktivuje účty s přístupem k Datům, pokud účet překročí stanovený počet po sobě jdoucích nesprávných pokusů o zadání hesla.

vii. Vzdálený přístup k Systémům obsahujícím Data vyžaduje dvoufaktorovou autentizaci (tj. vyžaduje alespoň dva samostatné faktory pro identifikaci uživatelů).

1.3. Detekce a prevence narušení

Společnost Infor využívá systém detekce a prevence narušení (IDS/IPS) k monitorování svých Systémů a postupů z hlediska bezpečnostních narušení, porušení a podezřelých aktivit. To zahrnuje podezřelé externí aktivity (včetně, ale bez omezení, neoprávněných sond, skenování nebo pokusů o vniknutí) a podezřelé interní aktivity (včetně, ale bez omezení, neoprávněného přístupu správce systému, neoprávněných změn v Systémech, zneužití nebo krádeže Systémů či nesprávného zacházení s Data). Společnost Infor pravidelně kontroluje přístupové protokoly, zda neobsahují známky škodlivého chování nebo neoprávněného přístupu.

1.4. Firewall

Společnost Infor zavedla a spravuje technologie síťových firewallů, jejichž účelem je ochrana Dat přístupných z internetu.

1.5. Aktualizace

Společnost Infor zajišťuje aktuálnost Systémů prostřednictvím upgradů, aktualizací, oprav chyb a nových verzí.

1.6. Šifrování Dat

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

ii. Pokud jsou Data uložena v Systémech, jsou šifrována minimálně 256bitovým algoritmem AES nebo jeho logickým nástupcem (s výjimkou případů Podpory týkajících se řešení platforem IBM Series i nebo Z, která společnost Infor prodává).

1.7. Správa identit

Společnost Infor využívá model sdíleného zabezpečení, který rozděluje odpovědnost za správu identit. Infor je schopen propojit aplikace v Systémech s poskytovatelem správy identit Zákazníka za účelem ověřování.

1.8. Škodlivý software

Společnost Infor využívá obecně uznávaný antimalwarový a antivirový software odpovídající průmyslovým standardům a v rámci možností využívá funkce ochrany v téměř reálném čase, aby zajistila poskytování Cloudových služeb nebo Software instalovaného na místě, které neobsahují žádné „časované bomby“, „červy“, „viry“, „ trojské koně“, „ochranné kódy“, „klíče pro zničení dat“ ani jiná programová zařízení, která mají za cíl (i) v případě Cloudových služeb upravovat, mazat, poškodit, deaktivovat nebo znemožnit přístup k Datům Zákazníka nebo zabránit či omezit přístup Zákazníka k Datům Zákazníka, nebo (ii) v případě Software instalovaného na místě upravovat, mazat, poškodit, deaktivovat nebo znemožnit přístup k Datům Zákazníka v rámci Software instalovaného na místě.

1.9. Fyzická bezpečnost

Prostory, v nichž jsou Systémy umístěny:

i. budou konstrukčně navrženy tak, aby odolaly nepříznivým povětrnostním podmínkám a jiným přiměřeně předvídatelným přírodním jevům;

ii. budou vybaveny vhodnými fyzickými ochrannými opatřeními, která pomohou chránit Systémy před poškozením způsobeným kouřem, teplem, vodou, ohněm, vlhkostí nebo výkyvy v napájení`

iii. budou podporovány záložními systémy výroby elektrické energie na místě; a

iv. budou vybaveny vhodnými kontrolními mechanismy navrženými tak, aby fyzický přístup do prostor byl povolen pouze oprávněnému personálu.

2. Audit

2.1. Právo na audit

V rámci svého programu dohledu nad dodavateli může Zákazník a (v příslušných případech) jeho dohledový orgán veřejné moci jednou ročně v rámci poštovního auditu (tj. dotazníku založeného na normě ISO 27001) požádat společnost Infor o procesní dokumentaci týkající se jejího programu informační bezpečnosti, procesů a kontrolních mechanismů. Společnost Infor souhlasí s tím, že v rozsahu, v jakém je taková procesní dokumentace k dispozici, poskytne Zákazníkovi dokumentaci, o kterou může Zákazník přiměřeně požádat, pokud tato dokumentace: (a) neohrožuje důvěrnost, integritu nebo dostupnost dat či služeb jiných zákazníků společnosti Infor nebo (b) neporušuje důvěrnost, integritu a dostupnost dat či služeb třetích stran poskytujících Služeb Zákazníkovi jménem společnosti Infor. Procedurální dokumentace poskytnutá společností Infor nebude zahrnovat důkazy (například, ale nikoli výlučně, doklady o školení, doklady o testování, výsledky posouzení rizik). Společnost Infor odpoví na dotazník do 30 dnů; pokud tento termín nelze dodržet, bude společnost Infor spolupracovat se Zákazníkem na stanovení vzájemně dohodnutého přiměřeného termínu pro dokončení. Veškerá taková dokumentace bude představovat Důvěrné informace společnosti Infor. Společnost Infor nebude brát v úvahu zjištění Zákazníka vyplývající z tohoto poštovního auditu.

2.2. Audit prováděný třetí stranou

Jednou za 12 měsíců v Období předplatného společnost Infor na své náklady pověří řádně kvalifikovaného nezávislého auditora, aby provedl přezkum koncepce a provozní účinnosti definovaných kontrolních cílů a kontrolních činností společnosti Infor v souvislosti s Cloudovými službami (s výjimkou Podpory). Společnost Infor zajistí, aby takový auditor vypracoval zprávu SOC I typu 2 pro všechny Cloudové služby a, pouze pro cloudové služby s více nájemci, zprávu SOC II typu 2 (společně dále jen „Auditorská zpráva“). Auditorská zpráva je důvěrnou informací společnosti Infor, je však Zákazníkovi k dispozici na portálu podpory společnosti Infor. Zákazník může sdílet kopii takovéto Auditorské zprávy se svými auditory a regulačními orgány za předpokladu, že tito auditoři a regulační orgány jsou informováni o tom, že se jedná o Důvěrné informace společnosti Infor, které musí být odpovídajícím způsobem chráněny.

Kromě toho společnost Infor každoročně na své náklady pověří řádně kvalifikovaného nezávislého auditora, aby provedl přezkum její informační bezpečnosti v souvislosti s určitými Cloudovými službami s více nájemci uvedenými na stránkách trust.infor.com, jakož i s Podporou pro Software instalovaný na místě i Cloudové služby, a to v každém případě podle normy Mezinárodní organizace pro normalizaci (ISO) 27001. Společnost Infor zajistí, aby tento auditor vypracoval Auditorskou zprávu v souladu s uvedenou normou. Auditorská zpráva nebude Zákazníkovi k dispozici; Zákazník však může kdykoli získat kopii výsledného certifikátu na stránkách společnosti Infor věnovaných bezpečnosti cloudu (trust.infor.com). Certifikát bude identifikovat software, který je předmětem zprávy. V rámci této certifikace ISO 27001 společnost Infor vede příručku Systému řízení bezpečnosti informací pro software zahrnutý v certifikaci a související Podporu, která pomáhá zajistit ochranu, důvěrnost, integritu a dostupnost aktiv společnosti Infor používaných k poskytování těchto Služeb.

Další certifikáty od třetích stran jsou k dispozici na adrese trust.infor.com.

3. Řízení změn u Cloudových služeb

Společnost Infor dodržuje proces řízení změn, který upravuje identifikaci a implementaci změn v rámci zdrojů poskytování Cloudových služeb Infor, aby se zabránilo nežádoucím změnám zdrojového kódu aplikací, rozhraní, operačních systémů nebo změnám dat v existujících polích a tabulkách na straně back-endu. Všechny požadované změny v rámci zdrojů poskytování Cloudových služeb společnosti Infor musí podléhat procesu řízení změn při implementaci. Společnost Infor dokumentuje a uchovává podrobné záznamy o dodržování tohoto procesu, například prostřednictvím systému ticketingu, a záznamy o testovacích postupech pro jakoukoli změnu, včetně, ale bez omezení, data a času takové změny a popisu povahy změny.

4. Segregace Dat; zákaz zneužití

4.1. Segregace

Data jsou pomocí vhodných technických prostředků logicky oddělena od dat společnosti Infor i od dat všech ostatních zákazníků společnosti Infor.

4.2. Zákaz zneužití; souhrnné statistiky

Data představují Důvěrné informace Zákazníka a Zákazník je vlastníkem všech majetkových práv k těmto datům. Společnost Infor nebude data komerčně využívat a nebude k nim přistupovat jinak než v míře nezbytné k poskytování Služeb a plnění svých povinností v souladu se Smlouvou.

Společnost Infor shromažďuje statistické údaje a informace o výkonu, generované prostřednictvím měřicích a protokolovacích Systémů, týkající se využívání a provozu Služeb ze strany Zákazníka („Souhrnné statistiky“). Souhrnné statistiky jsou výhradním vlastnictvím společnosti Infor a nejsou považovány za Data.

5. Správa aktiv

Společnost Infor má zavedený formální proces správy aktiv, který zahrnuje vedení:

i. soupisu Aktiv používaných k poskytování Služeb („Aktiva“), jehož účelem je identifikovat a jasně stanovit vlastnictví a kontrolu nad těmito Aktivy;

ii. postupů určených ke správě vrácení, likvidace nebo odstranění Dat z příslušných Aktiv; a

iii. postupů určených k ochraně Aktiv před hrozbami a zranitelnostmi, ať už vnitřními či vnějšími, úmyslnými či náhodnými.

6. Skenování zranitelností a penetrační testování

Společnost Infor uplatňuje proces správy zranitelností, jehož cílem je vyhledávat rizika vyplývající ze zneužití zveřejněných nebo identifikovaných chyb či slabých míst, která by mohla být (náhodně či úmyslně) využita a vést k poškození nebo neoprávněnému přístupu k Systémům („Zranitelnosti“). Společnost Infor bude řešit Zranitelnosti v lhůtách odpovídajících obecně uznávaným standardům v oboru. Společnost Infor odstraní nebo zmírní Zranitelnosti způsobem úměrným riziku, které tyto Zranitelnosti představují, v souladu s definovaným rámcem společnosti Infor, který je v souladu s obecně přijímanými průmyslovými standardy.

Společnost Infor každoročně na vlastní náklady najímá nezávislou třetí stranu, aby provedla penetrační testování pro Cloudové služby s více nájemci, včetně manuálního testování lidmi, s cílem vyhodnotit bezpečnostní kontroly Systémů podle obecně přijímaných metodik průmyslových standardů.

U Softwaru s předplatným pro více nájemců se před vydáním kódu a po celou dobu životního cyklu produktu Cloudových služeb (tj. ve vývojových a produkčních prostředích) provádějí bezpečnostní testy, včetně skenování zdrojového kódu a skenování Zranitelností, aby se identifikovaly potenciální Zranitelnosti k nápravě nebo zmírnění. Každoročně se provádějí penetrační testy Cloudových služeb pro více nájemců s cílem identifikovat Zranitelnosti k nápravě nebo zmírnění.

7. **Reakce na incidenty v oblasti informační bezpečnosti**Pokud se společnost Infor dozví, že Data byla nebo lze důvodně předpokládat, že byla předmětem použití nebo zveřejnění, které není povoleno touto Smlouvou (dále jen „Incident v oblasti informační bezpečnosti“), je povinna: (i) neprodleně a bez zbytečného odkladu (v každém případě do 48 hodin od zjištění takového Incidentu v oblasti informační bezpečnosti) informovat dotčeného Zákazníka o výskytu takového Incidentu v oblasti informační bezpečnosti; (ii) prošetří a provede přiměřenou analýzu příčin takového Incidentu v oblasti informační bezpečnosti; (iii) bude Zákazníkovi pravidelně poskytovat informace o průběhu vyšetřování; (iv) vypracuje a provede vhodný plán k nápravě příčiny takového Incidentu v oblasti bezpečnosti informací v rozsahu, v jakém je tato příčina v rámci kontroly společnosti Infor; a (v) bude spolupracovat s přiměřeným vyšetřováním Zákazníka nebo s jeho snahami o splnění jakýchkoli oznamovacích nebo jiných regulačních požadavků platných pro takový Incident v oblasti bezpečnosti informací. Na žádost Zákazníka a na jeho náklady v případě Incidentu v oblasti bezpečnosti informací společnost Infor dodá (v rozsahu povoleném zákonem a s výhradou příslušných opatření na ochranu důvěrnosti) Zákazníkovi kopie záznamů o příslušné činnosti Systémů (výhradně s ohledem na Incident v oblasti bezpečnosti informací, který se týká Zákazníka) k použití v jakémkoli právním nebo regulačním řízení Zákazníka nebo v jakémkoli vládním vyšetřování Zákazníka.

8. **Protokolování a monitorování**Společnost Infor monitoruje zdroje využívané k poskytování Služeb pomocí sady nástrojů, které jsou speciálně nakonfigurovány pro správu protokolů a výstrah. Záznamy protokolů jsou fyzicky i virtuálně zabezpečeny, aby se zabránilo jejich neoprávněné manipulaci. Citlivé informace a hesla se za žádných okolností neprotokolují. Kromě zaznamenávání informací souvisejících se Službami umožňují monitorovací nástroje správcům sledovat aktivitu uživatelů při přihlašování do Systému a odhlašování z něj.

9. **Bezpečnost a školení v oblasti lidských zdrojů**Zaměstnanci společnosti Infor poskytující Služby podléhají povinnosti mlčenlivosti, jsou informováni o hrozbách a rizicích v oblasti informační bezpečnosti, absolvují alespoň jednou ročně obecné školení v oblasti bezpečnosti a jsou vybaveni tak, aby mohli poskytovat podporu pro zásady informační bezpečnosti organizace jak obecně, tak v rámci svých konkrétních pracovních povinností.

10. **Řízení koncových zařízení (notebooky, pracovní stanice a mobilní zařízení společnosti Infor)**Společnost Infor zavádí bezpečnostní opatření v souladu s obecně uznávanými postupy v oboru za účelem ochrany koncových zařízení, včetně automatizace správy oprav aplikací a operačních systémů a antivirové ochrany.

11. **Vrácení a smazání Dat**

    11.1. **Vrácení**Po ukončení nebo vypršení platnosti Cloudových služeb společnost Infor neprodleně (do 3–5 pracovních dnů od obdržení písemné žádosti Zákazníka podané prostřednictvím standardního tiketu Podpory, přičemž tato Žádost musí být podána do 30 dnů od ukončení (10 dnů v případě single-tenant)) zpřístupní Zákazníkovi veškerá Data Zákazníka ve formě nativního exportu databáze prostřednictvím zabezpečené služby pro přenos souborů společnosti Infor. Pokud Zákazník požaduje vrácení Dat Zákazníka v alternativním formátu nebo vyžaduje jakékoli jiné služby související s ukončením, společnost Infor a Zákazník se vzájemně dohodnou na rozsahu těchto služeb a na poplatcích a nákladech,

které jsou za tyto služby splatné. Před ukončením má Zákazník přístup k Datům Zákazníka prostřednictvím aplikačních rozhraní a společnost Infor vrátí na žádost Zákazníka podanou prostřednictvím portálu Podpory kopie záloh dat až dvakrát za 12měsíční období jako nativní export databáze poskytnutý prostřednictvím služby bezpečného přenosu souborů společnosti Infor; další žádosti budou zpoplatněny.

Pro větší jasnost bude vrácení nebo smazání Osobních údajů v souladu s podmínkami Smlouvy o ochraně osobních údajů.

Data pro systémy výnosů (např. Infor Document Management, Infor EzRMS nebo Infor Hospitality Price Optimizer) jsou při ukončení smazána a nejsou předána Zákazníkovi.

11.2. SmazáníS výjimkou případů, kdy Zákazník požádá o Asistenci při přechodu, společnost Infor trvale smaže všechny (online nebo v síti dostupné) instance Zákaznických dat do 35 dnů od ukončení nebo vypršení platnosti Cloudových služeb v souladu s normou NIST 800-88.

Data poskytnutá společnosti Infor za účelem poskytování Podpory (tj. prostřednictvím žádosti o Podporu zaznamenané na portálu Podpory) jsou vymazána pět let od data uzavření žádosti o podporu. Jméno a kontaktní údaje jednotlivého Zákazníka (např. e-mailová adresa uživatele, jméno a telefonní číslo) použité ke správě životního cyklu žádosti o Podporu jsou při ukončení Podpory deaktivovány a anonymizovány.

12. Subdodavatelé

Subdodavatelé společnosti Infor, kteří společnosti Infor dodávají zboží a poskytují služby v souvislosti se Službami společnosti Infor, jsou povinni toto zboží a služby poskytovat za podmínek, které jsou v podstatě podobné podmínkám stanoveným v těchto podmínkách poskytování služeb (ISP). Před zapojením takového externího subdodavatele k poskytování jakýchkoli služeb podle této Smlouvy je společnost Infor povinna provést s přiměřenou péčí prověrku této třetí strany, aby se ujistila, že je tato třetí strana schopna dodržovat povinnosti týkající se důvěrnosti a bezpečnosti stanovené v této smlouvě. Společnost Infor nese odpovědnost za veškeré činnosti svých subdodavatelů při poskytování Služeb.

*Upozornění: Následující produkty mohou mít dodatečné nebo odlišné bezpečnostní podmínky: Acumen Invest (Infor Trade Promotions Management) and Acumen Radar (Infor Strategic Pricing Management)**,** Anael (SaaS) (France); 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).*