Dodatek č. 1 k licenční smlouvě a smlouvě o poskytování služby webové aplikace eQuip ze dne 16.09.2024

který níže uvedeného dne, měsíce a roku uzavřely ve smyslu ust. § 2586 a násl. zák. č. 89/2012 Sb., občanského zákoníku tyto smluvní strany

Software production s.r.o.
se sídlem Denisovo nábřeží 2568/6, Východní předměstí, 301 00 Plzeň
IČ: 279 73 956
DIČ CZ27973956
zapsaná v obchodním rejstříku vedeném Krajským soudem v Plzni, sp.zn. C 19541
Telefon: +420 374 802 452
email: info@sopr.cz
Zastoupená Petrem Suchým, jednatelem
jako Poskytovatel

a

Středisko sociálních služeb města Kopřivnice, příspěvková organizace
se sídlem ul. Česká 320, 74221 Kopřivnice
IČ: 60798891
Telefon: 733 554 919
email: reditel@sssmk.cz
Zastoupená Mgr. Renatou Volnou, MBA
jako Uživatel

uzavírají po vzájemné domluvě níže uvedeného dne, měsíce a roku tento Dodatek č.1 k licenční smlouvě a smlouvě o poskytování služby webové aplikace eQuip ze dne 16.09.2024

I.
Předmět dodatku

Předmětem tohoto dodatku č.1 jsou závazky poskytovatele informačního systému eQuip (dále jen „**Aplikace“**) vyplývající z požadavků Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.

Poskytovatel se zavazuje zavést a udržovat technická a organizační opatření dle §14 zákona o kybernetické bezpečnosti. Níže je uveden popis těchto opatření, případně jsou popsány možnosti, které uživatel může využít k zajištění kybernetické bezpečnosti, dle své preferované volby.

II.
Řízení přístupů + Vícefaktorová autentizace

Druhotné ověření identity lze realizovat jednou z následujících možností, nebo jejich kombinací:

- prostřednictvím klientského certifikátu – přihlášení je možné pouze z důvěryhodných zařízení, které mají nainstalovaný certifikát

- dvoufaktorové ověření pomocí jednorázového hesla (OTP)
- autentizační proces služby Microsoft Entra ID.

Přihlášení do aplikace, je zaznamenáváno a monitorováno. Stejně tak je průběžně sledována a evidována veškerá uživatelská činnost prováděná po úspěšném přihlášení. Monitorování slouží k zajištění bezpečnosti, odhalování neoprávněných přístupů a ochraně integrity aplikace.
Uživatelé mají přístup do jednotlivých částí aplikace řízeny uživatelskými právy. Každá část aplikace má jednoznačně určená oprávnění pro povolení přístupu.

III.
Šifrování dat v klidu a při přenosu

Data jsou šifrována na úrovni souborového systému jednotlivých virtuálních strojů, případně na úrovni celého datového úložiště (datapoolu) hypervizoru. Při výměně fyzického datového nosiče jsou veškerá data na tomto nosiči bezpečným způsobem nenávratně zničena. Zálohovací soubory jsou šifrovány algoritmem AES-256.

Přenos dat mezi uživateli a servery probíhá výhradně prostřednictvím šifrovaných protokolů Transport Layer Security (TLS) verze 1.2 nebo 1.3, případně jiných ekvivalentně bezpečných protokolů, pokud daná služba TLS nevyužívá. Použití starších, nebezpečných verzí protokolu není aplikací povoleno. Konkrétní protokol a jeho verze se volí automaticky podle možností a konfigurace klientského zařízení.

IV.
Evidence a detekce bezpečnostních událostí

Bezpečnostní události jsou identifikovány na základě různých zdrojů, mezi které patří:

- nahlášení podnětu od uživatele nebo externího subjektu
- zjištění při interní kontrole poskytovatele
- oznámení zaměstnanců poskytovatele
- výsledky provedeného auditu
- hlášení z monitorovacích systémů

Po zjištění bezpečnostní události je provedena její analýza s cílem určit rozsah, závažnost a naléhavost dopadu na aplikaci a obě smluvní strany. Veškeré bezpečnostní události, včetně jejich vyhodnocení a přijatých opatření, jsou evidovány v interním dokumentu poskytovatele, který slouží k monitorování, prevenci a zajištění bezpečnosti informací a dat poskytovatele.

V.
Patch management a řízení zranitelností

Aktualizace operačních systémů se provádí plánovanými odstávkami, které vyžadují dočasné přerušení provozu, jsou prováděny v době nejnižší vytíženosti aplikace, aby byl minimalizován dopad na uživatele. Jsou hlášeny minimálně 24 hodin před provedením

odstávky prostřednictvím aplikace. Je tím ovlivněna celková dostupnost aplikace na 99,7%, což je cca 2 hodiny odstávky měsíčně.
Veškeré klíčové informace týkající se jednotlivých služeb operačních systémů a serverů, včetně stavu jejich aktualizací, záloh a doby uchování logů, jsou evidovány v interním dokumentu poskytovatele. Poskytovatel provádí interní penetrační testy všech klíčových služeb čtvrtletně, vždy před jednáním výboru pro řízení kybernetické bezpečnosti, s cílem ověřit bezpečnostní stav systémů a identifikovat případná rizika. Výsledky těchto testů jsou zaznamenávány a využívány k plánování opatření pro zajištění kontinuální ochrany informací a dat Poskytovatele.

VI.
Logování

Záznamy o běhu aplikace a činnostech uživatelů, jsou ukládány do hlavní databáze. Jejich procházení je možné prostřednictvím aplikace nebo stažením zálohy dat a procházením surových dat.

Záznamy o běhu serverových operačních systémů jsou ukládány na serverech. Nejdůležitější z těchto záznamů jsou prostřednictvím rsyslog přenášeny do logovacího nástroje Loki/Promtail. Seznam přenesených záznamů a doba jejich uchování je vedena v interním dokumentu poskytovatele. Nejkratší doba logování je 3 měsíce. Nejkratší doba sledovaných metrik je 6 měsíců. Záznamy jsou dostupné v systému Grafana. Kde lze filtrovat podle specifických výskytů a časových období, což umožňuje odhalit relevantní informace pro analýzu a bezpečnostní dohled.

VII.
Zálohování

Zálohy serverů jsou prováděny v souladu s interním dokumentem Poskytovatele. Zálohy jsou uchovávány na několika místech. Několik verzí záloh zůstává uloženo přímo na serveru podle dostupné kapacity úložiště. Pokud není možné ponechat starší verze záloh na serveru a zálohování probíhá přímo, je využita funkce snapshotů pro verzování starších záloh na Network Attached Storage (NAS).
Zálohy dokumentů uložených na S3 object storage (S3) a dalších zdrojích neuchovávají historické verze na zdrojovém serveru; pro jejich verzování se rovněž používá funkce snapshotů s častějším vytvářením na NASu. Zálohy databází jsou uchovávány na uložišti WEDOS Internet, a.s. a na NASu. Zálohy serverů, dat a síťových prvků jsou uloženy na NASu. Doba uchování záloh je stanovena v interním dokumentu poskytovatele, který rovněž popisuje jejich obsah.
Servery provozované u INTERNET CZ, a.s. mají nastavené pravidelné automatické vytváření snapshotů prostřednictvím naplánované úlohy.
Obrazy disků virtuálních strojů, které běží v proxmox clusteru, jsou vytvářeny denně a uchovávány u INTERNET CZ, a.s. Následně jsou tyto obrazy synchronizovány na zálohovací server umístěný v sídle Poskytovatele, čímž je zajištěna možnost kompletní obnovy dat.
Minimální doba uchování všech záloh je stanovena na 14 dní.

a. Monitorování záloh

Proces vytváření záloh a jejich nahrávání na NAS je průběžně monitorován a v případě chyby jsou administrátoři poskytovatele okamžitě upozorněni.
Pokud nastane chyba při vytváření zálohy na serveru, skript generuje upozornění. Administrátor poskytovatele ji neprodleně řeší a případně zálohu spouští znovu.
Nejdůležitější zálohy jsou dále kontrolovány z hlediska konzistence souborů pomocí algoritmu SHA-256 a SHA-512 a sekundárně i kontrolou velikosti souborů a jejich odlišností od historických verzí. V případě zjištění nesrovnalosti administrátor poskytovatele určí, ve které části procesu došlo k chybě, a nahraje konzistentní zálohu.

b. Testování záloh

Zálohy databáze, jsou pravidelně obnovovány automatickým skriptem a testovány v sídle poskytovatele. Databáze je každý týden stažena ze zálohovacího pole na vývojový server a obnovena do testovacího prostředí na další týden, čímž se ověřuje konzistence dat.

c. Obnova dat

Obnova dat probíhá podle rozsahu požadované obnovy a dostupného času. Pokud je to možné, obnovuje se pouze část dat nezbytná pro provoz aplikace. Část dat lze obnovit kopírováním ze záloh uložených na serveru, přičemž se využívají záložní kopie nebo několik předchozích verzí záloh podle možností úložiště serveru.
V případě potřeby lze obnovit server pomocí předchozího snapshotu, který vrátí celý server do stavu v okamžiku vytvoření snapshotu.
K obnově dat lze rovněž využít kompletní obraz (image) virtuálního stroje, který je uchováván na dvou geograficky odlišných místech.
Pokud je nutné provést kompletní obnovu celého serveru, připraví se nový server a následně se nahrají nejaktuálnější verze dat na daný server ze záloh na NAsu. Server je znovu nakonfigurován a jsou na něj instalovány potřebné služby. Tento postup se považuje za poslední řešení obnovy, vzhledem k jeho časové náročnosti.
Při obnově se vždy zvolí možnost, která je nejrychlejší a nejvhodnější pro danou situaci, s ohledem na maximální zachování dat.
Cílový čas/doba zotavení (RTO) - cílový bod obnovení/zotavení (RPO) jsou stanoveny na maximálně 24 hodin od okamžiku zjištění incidentu.

VIII.
Bezpečnost vývoje aplikace

Při vývoji aplikace jsou uplatňovány následující principy:

- Bezpečnost již při návrhu: Bezpečnostní požadavky jsou definovány a zohledněny již ve fázi návrhu architektury aplikace.
- Bezpečnost ve výchozím nastavení: Aplikace je konfigurována tak, aby byla ve výchozím stavu bezpečná.
- Plánování a analýza: Identifikace bezpečnostních rizik spojených s novou funkcionalitou.
- Bezpečnost knihoven je revidována v rámci pravidelných interních penetračních testů.

- Ověření bezpečnosti nových funkcionalit je prováděno v rámci testování předprodukční verzí. Proces zahrnuje klasifikaci dopadu změn a při vyšším riziku, je testování prováděno vícestupňově, více osobami s odpovídajícími zkušenostmi pro vyhodnocení rizika.
- Jsou používány nástroje pro správu verzí
- Procesy při vývoji a nasazení nových verzí, jsou popsány vnitřními dokumenty poskytovatele, podle kterých se vývojáři a správci řídí.
- Zaměstnanci poskytovatele pravidelně prochází školením kybernetické bezpečnosti.

IX.
Hlášení incidentů

V případě bezpečnostního incidentu poskytovatel neprodleně provede analýzu jeho dopadu. Pokud je na základě této analýzy zjištěno, že došlo k úniku citlivých informací nebo k jinému závažnému incidentu, je poskytovatel povinen nahlásit kybernetický incident Uživateli do 72 hodin od jeho zjištění, a to prostřednictvím datové schránky Uživatele. Poskytovatel následně ohlásí incident Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB), poskytne veškeré záznamy o incidentu a související auditní výstupy. Poskytovatel bude součinný při řešení incidentu s NÚKIB.

X.
Místo uložení dat

Provoz virtuálních serverů, úložiště S3, housing serverů a správa domén je zajišťována společností INTERNET CZ, a.s. v datacentru Ktiš na území České republiky. Společnost INTERNET CZ, a.s. splňuje certifikace ISO 9001 a ISO 27001.
Zálohy databázového serveru jsou uchovávány v datacentru společnosti WEDOS Internet, a.s., které je umístěno v Hluboké nad Vltavou na území České republiky. WEDOS Internet, a.s. splňuje certifikace ISO 9001, ISO 14001, ISO 21017, ISO 27018 a ISO 27001
V sídle poskytovatele jsou využívány vlastní hardwarové prostředky pro uchování záloh a zároveň jako testovací prostředí pro aplikaci.

XI.
Subdodavatelé

Nový subdodavatel hardwarové infrastruktury může být zapojen pouze se souhlasem Uživatele.
Smluvní vztah se subdodavatelem obsahuje stejné závazky, ve vztahu ke kybernetické bezpečnosti, jako závazky poskytovatele vůči Uživateli.

XII.
Práva uživatele

a. NIS2 audit

Uživatel má právo požadovat poskytnutí aktuálních auditních zpráv systému, či na vlastní náklady nechat provést bezpečnostní audit aplikace na kopii produkčního systému aplikace,

který bude podle časových a technických možností poskytovatele připraven pro účely vlastního auditu Uživatele.

b. Export dat

Aplikace obsahuje funkci pro vytvoření aktuální kopie veškerých dat databáze v otevřeném formátu MySQL a zálohu všech vložených dokumentů.

XIII.
Výmaz dat po ukončení využívání aplikace

Přístup do aplikace je zachován minimálně 14 dní po ukončení smlouvy. Do 30 dnů po skončení se musí Uživatel vyjádřit k tomu, zda chce data zachovat v režimu pouze pro čtení, a pak se podepisuje nová smlouva, nebo chce data smazat. Pokud se Uživatel nevyjádří do 30 dnů od ukončení smlouvy jsou data smazána.
Smazání dat se provádí „anonymizací“, při které jsou smazány veškeré textové kolonky.

XIV.
Odpovědnost za škody

Poskytovatel odpovídá za škody způsobené porušením bezpečnostních povinností.
Poskytovatel odpovídá za škody způsobené bezpečnostním incidentem, pokud vznikl jeho vinou.
Poskytovatel odpovídá za škody způsobené nedostupností služby, mimo garantovaný rozsah dostupnosti.
Garantovaná dostupnost aplikace je 99,7% času. Jsou do ní započítány servisní odstávky cca 2 hodiny měsíčně.

Ostatní ujednání zůstávají beze změn.

V Plzni dne 10.03.2026

[redacted]

_____
za Poskytovatele

[redacted]

_____
za Uživatele