BEZPEČNOSTNÍ PODMÍNKY GREEN:CODE S.R.O.

(dále jen „Podmínky“)

1. Úvodní ustanovení

1.1 Tyto Podmínky stanovují minimální bezpečnostní povinnosti Dodavatele při poskytování Služeb Objednateli (Green:Code s.r.o.) na základě Rámcové smlouvy o poskytování služeb (dále jen „Smlouva“) a jednotlivých Dílčích smluv. Podmínky mají povahu obchodních podmínek dle § 1752 a násl. zákona č. 89/2012 Sb., občanského zákoníku, a jsou nedílnou součástí Smlouvy.

1.2 Pojmy psané s velkým počátečním písmenem mají význam stanovený Smlouvou (zejména Objednatel, Dodavatel, Služby, Dílčí smlouva, Objednávka).

1.3 Podmínky se vztahují na všechny činnosti Dodavatele a osob, které Dodavatel zapojí do poskytování Služeb, na všechny informace Objednatele a informace klientů Objednatele, ke kterým Dodavatel získá přístup, a na všechna zařízení, která jsou při poskytování Služeb používána.

1.4 Smlouva a Dílčí smlouva mají v případě rozporu přednost před těmito Podmínkami. Dílčí smlouva nebo bezpečnostní požadavky klienta Objednatele mohou stanovit přísnější bezpečnostní režim; nemohou však tyto Podmínky zmírnit, není-li to v Dílčí smlouvě výslovně sjednáno.

1.5 Objednatel může Dodavateli předávat provozní bezpečnostní pokyny (čl. 14). Provozní pokyn se uplatní v rozsahu, ve kterém není v rozporu se Smlouvou, Dílčí smlouvou ani těmito Podmínkami.

2. Obecná odpovědnost Dodavatele

2.1 Dodavatel chrání důvěrnost, integritu a dostupnost informací Objednatele a informací klientů Objednatele, ke kterým získá přístup v souvislosti se Službami.

2.2 Dodavatel používá informace, přístupy, zařízení a další prostředky Objednatele a klientů Objednatele výhradně pro plnění Služeb. Použití pro vlastní potřebu Dodavatele, pro plnění pro jiné objednatele, pro trénink modelů nebo jiné účely je zakázáno.

2.3 Dodavatel postupuje podle principu „Need to know“ a principu nejnižších oprávnění — žádá a využívá pouze ty přístupy a oprávnění, které nezbytně potřebuje k plnění konkrétní Služby.

2.4 Dodavatel dodržuje platné právní předpisy, smluvní závazky Objednatele vůči klientům, požadavky klientů sdělené Dodavateli a tyto Podmínky.

2.5 Pokud Dodavatel obdrží pokyn Objednatele, který je v rozporu s bezpečnostními požadavky těchto Podmínek, právními předpisy nebo bezpečnostními zájmy Objednatele či jeho klienta, je povinen na rozpor neprodleně upozornit a vyžádat si potvrzení nebo úpravu pokynu.

2.6 Dodavatel jedná tak, aby chránil dobré jméno a oprávněné zájmy Objednatele a jeho klientů.

3. Účty, identity a přístupová oprávnění

3.1 Dodavatel používá pouze účty osobně přidělené konkrétní fyzické osobě, která Služby skutečně vykonává.

3.2 Sdílení účtů, hesel, tokenů, certifikátů a dalších autentizačních prostředků mezi více osobami je zakázáno.

3.3 Dodavatel používá vícefaktorovou autentizaci (MFA) všude, kde je dostupná nebo vyžadovaná Objednatelem.

3.4 Dodavatel nesmí obcházet nebo se pokoušet obejít bezpečnostní kontroly, autentizaci, autorizaci, logování ani filtry komunikace.

3.5 Dodavatel používá přístupy pouze ve schváleném rozsahu a po dobu, kdy je pro plnění Služeb skutečně potřebuje. O ukončení potřeby přístupu neprodleně informuje Objednatele.

3.6 Dodavatel neprodleně oznámí Objednateli každý zjištěný nadbytečný, chybně přidělený nebo neoprávněný přístup k informacím nebo systémům.

3.7 Dodavatel bere na vědomí, že Objednatel je oprávněn okamžitě zablokovat účet, identitu nebo přístup k informačnímu systému při důvodném podezření na bezpečnostní incident nebo zneužití přístupu, a to i bez předchozího upozornění; o blokaci je Dodavatel bez zbytečného odkladu informován.

3.8 Dodavatel nesmí vytvářet, nasazovat ani provozovat technické (servisní) účty, sdílené účty nebo automatizované integrace bez předchozího schválení Objednatele.

4. Zařízení a používání soukromého zařízení (BYOD)

4.1 Není-li v Dílčí smlouvě dohodnuto jinak, Dodavatel poskytuje Služby z vlastních zařízení. Každé zařízení používané pro poskytování Služeb musí splňovat následující bezpečnostní požadavky:

a) podporovaný operační systém s aktuálními bezpečnostními aktualizacemi a aktualizovanými klíčovými aplikacemi;
b) šifrování systémového disku tam, kde je technicky dostupné;
c) aktivní antimalwarová ochrana schválená Objednatelem;
d) nainstalovaný a aktivní nástroj pro detekci a reakci na bezpečnostní incidenty (EDR) schválený Objednatelem;
e) automatické zamykání zařízení po stanovené době nečinnosti a uzamykání obrazovky při opuštění zařízení;
f) silná autentizace pro přístup do operačního systému (heslo, PIN, biometrie);
g) ochrana zařízení před ztrátou, odcizením a před přístupem dalších osob, včetně rodinných příslušníků.

4.2 Dodavatel nesmí deaktivovat, odinstalovat, blokovat ani modifikovat bezpečnostní nástroje schválené Objednatelem provozované na zařízení. Dodavatel umožní pravidelnou aktualizaci a údržbu těchto nástrojů a vzdálenou intervenci v rámci řešení bezpečnostního incidentu (zejména izolaci zařízení nebo odstranění škodlivého souboru).

4.3 Dodavatel odděluje pracovní a soukromá data v rozsahu odpovídajícím technickým možnostem zařízení (např. samostatný uživatelský profil, samostatná schválená úložiště pro pracovní data, samostatné prohlížeče nebo profily).

4.4 Dodavatel bere na vědomí a souhlasí s tím, že bezpečnostní nástroje schválené Objednatelem mohou pro účely bezpečnosti zpracovávat technické údaje o zařízení (síťová komunikace včetně cílových destinací a portů, vykonávané procesy a jejich artefakty, úpravy souborového systému bez sběru obsahu soukromých dokumentů Dodavatele, systémové logy, informace o hardwarové konfiguraci) a detekovat škodlivý kód. Objednatel neprovádí prostřednictvím těchto nástrojů audiovizuální záznam, záznam obrazovky ani záznam stisků kláves.

4.5 Dodavatel umožní Objednateli přiměřeně ověřit splnění požadavků podle čl. 4.1, a to způsobem dle čl. 12 těchto Podmínek. Objednatel nemá právo na plošný přístup k soukromým datům Dodavatele uloženým na zařízení.

4.6 V případě ztráty, odcizení nebo neoprávněného přístupu k zařízení používanému pro poskytování Služeb postupuje Dodavatel dle čl. 9 těchto Podmínek.

5. Nakládání s informacemi

5.1 Dodavatel respektuje klasifikaci informací stanovenou Objednatelem nebo vlastníkem informace na straně Objednatele či klienta. Veškeré projekty a zakázky pro klienty Objednatele jsou považovány za důvěrné, není-li stanoveno přísnější označení.

5.2 Dodavatel ukládá informace Objednatele a informace klientů Objednatele pouze do úložišť a systémů schválených Objednatelem. Ukládání takových informací na soukromá cloudová úložiště, do soukromého e-mailu, na soukromá média a do neschválených komunikačních služeb je zakázáno.

5.3 Pro pracovní komunikaci Dodavatel používá pouze komunikační kanály schválené Objednatelem. Pro e-mailovou komunikaci s pracovním obsahem používá Dodavatel pouze schváleného e-mailového klienta připojeného k pracovní identitě.

5.4 Přenos důvěrných informací mimo schválená úložiště a kanály vyžaduje schválení Objednatele a probíhá šifrovaně.

5.5 Dodavatel neposkytuje informace Objednatele ani informace klientů Objednatele neoprávněným osobám, včetně jiných pracovníků Dodavatele, kteří se na daném plnění nepodílejí.

5.6 Tisk a vytváření lokálních kopií informací Dodavatel omezuje na nezbytně nutný rozsah; tištěné materiály neponechává bez dohledu a po skončení potřeby je bezpečně skartuje.

5.7 Dodavatel nesmí informace Objednatele a informace klientů Objednatele použít pro jiného objednatele, pro vlastní vývoj nebo komerční produkty, pro trénink nebo doladění modelů umělé inteligence ani pro jiné vlastní účely.

5.8 Po skončení potřeby Dodavatel bezpečně smaže lokální pracovní kopie informací; postup při ukončení spolupráce upravuje čl. 13.

6. Software, cloudové služby a licence

6.1 Dodavatel používá pro poskytování Služeb pouze software, který je legálně licencovaný pro firemní / komerční použití, je bezpečnostně podporovaný výrobcem a není zařazen do zakázaných kategorií podle aktuálního provozního pokynu Objednatele.

6.2 Dodavatel nesmí instalovat ani používat software, který:

a) je určen k obcházení bezpečnostních opatření (tunelovací nástroje, neschválení VPN klienti, anonymizační sítě);
b) umožňuje vzdálený přístup ke koncovému zařízení mimo nástroje schválené Objednatelem;
c) zasahuje do bezpečnostních mechanismů zařízení na úrovni jádra systému nebo bezpečnostních ovladačů, není-li schválen Objednatelem;
d) je nelegálně získaný, cracknutý, modifikovaný neoficiální cestou nebo pochází z neoficiálních zdrojů;
e) provádí těžbu kryptoměn;
f) je rozšířením internetového prohlížeče s přístupem k přihlašovacím údajům, obsahu formulářů nebo relacím, není-li schváleno Objednatelem.

6.3 Aktuální seznam zakázaných nebo schválených kategorií softwaru a konkrétních nástrojů (včetně schváleného antimalwaru a EDR) je provozním pokynem Objednatele a je Dodavateli předáván a aktualizován způsobem dle čl. 14.

6.4 Použití SaaS nebo cloudových služeb pro plnění Služeb vyžaduje předchozí schválení Objednatele. Schválení je vázáno na konkrétní službu, účel a typ zpracovávaných informací.

6.5 Dodavatel respektuje licenční podmínky proprietárního i open-source softwaru používaného při plnění Služeb. U open-source komponent s licencemi typu copyleft (zejména GPL, AGPL) Dodavatel předem vyhodnotí dopady na klientské řešení a informuje Objednatele.

6.6 Dodavatel odpovídá za veškerý software, knihovny, závislosti a rozšíření, které při plnění Služeb používá, instaluje nebo zařazuje do dodávky.

7. Bezpečný vývoj

7.1 Tento článek se uplatní pouze v rozsahu, ve kterém je předmětem Služeb vývoj softwaru, správa zdrojového kódu, testování, DevOps činnosti nebo provoz aplikací Objednatele nebo jeho klienta.

7.2 Zdrojový kód, konfigurace a související projektová dokumentace musí být uloženy ve verzovaném repozitáři schváleném Objednatelem. Ukládání produkčního zdrojového kódu mimo schválený repozitář (lokální archivy, osobní repozitáře, neschválené veřejné služby) je zakázáno.

7.3 Dodavatel neukládá hesla, klíče, tokeny, certifikáty ani jiná tajemství (secrets) přímo do zdrojového kódu, konfiguračních souborů ve verzovaném úložišti, do logů ani do veřejně přístupných umístění. Pro jejich uložení používá nástroj pro správu secrets schválený Objednatelem.

7.4 Dodavatel kontroluje použité závislosti a knihovny z pohledu licencí a známých zranitelností. Závažné zjištěné zranitelnosti odstraňuje v prioritě a termínu stanoveném Dílčí smlouvou nebo požadavkem klienta.

7.5 Dodavatel respektuje code review a CI/CD kontroly nastavené pro daný projekt. Obcházení branch policies, schvalovacích pravidel, automatických testů a bezpečnostních kontrol je zakázáno.

7.6 Dodavatel nezavádí do zdrojového kódu zadní vrátka, skryté funkce, telemetrii odesílající data mimo schválené prostředí ani jiné nezdokumentované přístupy a mechanismy.

7.7 Dodavatel poskytne součinnost při bezpečnostním testování zadaném Objednatelem nebo klientem (zejména SAST, DAST, SCA, penetrační testy) a při ověřování oprav.

7.8 Seznam komponent softwaru (SBOM) Dodavatel dodá tehdy, je-li to vyžadováno Dílčí smlouvou nebo bezpečnostními požadavky klienta pro konkrétní dodávku.

8. Používání umělé inteligence

8.1 Dodavatel může používat nástroje umělé inteligence pro plnění Služeb pouze v rozsahu schváleném Objednatelem pro daný projekt.

8.2 Do nástrojů umělé inteligence, které nejsou schválené Objednatelem pro daný účel, nesmí Dodavatel vkládat ani jinak zpřístupňovat interní informace Objednatele, informace klientů Objednatele, důvěrné a tajné informace, osobní údaje ani zdrojový kód mimo schválené případy.

8.3 Použití umělé inteligence nesmí porušovat autorská práva, licenční podmínky, ochranu osobních údajů ani smluvní závazky Objednatele vůči klientovi.

8.4 Výstupy nástrojů umělé inteligence musí být před použitím v dodávce odborně zkontrolovány Dodavatelem. Dodavatel odpovídá za výstup stejně, jako kdyby jej vytvořil bez použití umělé inteligence.

8.5 Použití umělé inteligence nesmí obcházet bezpečnostní, kvalitativní, testovací ani schvalovací procesy stanovené Smlouvou, Dílčí smlouvou nebo provozním pokynem.

8.6 Pokud Dodavatel použije umělou inteligenci při vývoji nebo zpracování informací klienta a povaha činnosti to vyžaduje, je povinen tuto skutečnost transparentně sdělit Objednateli.

9. Bezpečnostní incidenty a zranitelnosti

9.1 Dodavatel je povinen bezodkladně, nejpozději však do 24 hodin od zjištění nebo důvodného podezření, oznámit Objednateli každý bezpečnostní incident, který se týká informací nebo systémů Objednatele nebo jeho klientů.

9.2 Za bezpečnostní incident se považuje zejména: kompromitace nebo podezření na kompromitaci pracovního účtu, infekce malwarem, úspěšný phishing, ztráta nebo odcizení zařízení používaného k plnění Služeb, únik nebo neoprávněné zveřejnění informací Objednatele nebo informací klienta, omyl při sdílení informací s neoprávněnou osobou, neoprávněný přístup k informacím nebo systémům, ztráta autentizačního prostředku (heslo, token, certifikát).

9.3 Hlášení podle čl. 9.1 Dodavatel provádí na e-mailovou adresu security@greencode.cz nebo jiným kanálem stanoveným Objednatelem.

9.4 Do okamžiku, než Dodavatel obdrží pokyny Objednatele, je povinen:

a) zachovat dostupné logy, záznamy a další důkazní materiály související s incidentem;
b) neprovádět nevratné kroky (formátování, přeinstalace, mazání), pokud to situace umožňuje, ledaže okamžité zamezení dalšího šíření vyžaduje opak;
c) bez zbytečného odkladu omezit přístup kompromitovaného účtu nebo zařízení k informacím Objednatele.

9.5 Dodavatel poskytne Objednateli součinnost při zamezení šíření, technické analýze, odstranění příčiny, obnově a nápravných opatřeních, včetně předání relevantních logů a artefaktů.

9.6 Dodavatel oznámí Objednateli také zjištěnou závažnou zranitelnost nebo chybnou konfiguraci v informacích nebo systémech Objednatele nebo klienta, ke kterým má v rámci poskytování Služeb přístup.

10. Subdodavatelé a další osoby

10.1 Zapojení dalších osob na straně Dodavatele do plnění Služeb vyžaduje předchozí písemný souhlas Objednatele v souladu se Smlouvou.

10.2 Dodavatel zaváže každou takovou další osobu k povinnostem v rozsahu těchto Podmínek a odpovídá za její jednání jako za vlastní.

10.3 Dodavatel neposkytne další osobě širší přístup k informacím a systémům Objednatele nebo klienta, než je nezbytné pro plnění části Služeb, kterou daná osoba zajišťuje.

11. Fyzická bezpečnost

11.1 Při pohybu v prostorách Objednatele nebo klienta Dodavatel používá pouze osobně přidělené přístupové prostředky (přístupová karta, mobilní aplikace, identifikační prostředek). Půjčování těchto prostředků jiným osobám je zakázáno.

11.2 Dodavatel nevpouští do prostor Objednatele osoby, které nezná nebo jejichž oprávnění ke vstupu si nemůže ověřit. Doprovod návštěv zajišťuje pouze v rozsahu, ke kterému je oprávněn.

11.3 Při opuštění pracoviště Dodavatel uzamyká pracovní stanici. Tištěné materiály a média odkládá tak, aby nebyly přístupné neoprávněným osobám.

11.4 Ztrátu přístupového prostředku, zařízení nebo média Dodavatel bezodkladně oznámí způsobem dle čl. 9.

11.5 V prostorách klienta Objednatele se Dodavatel řídí navíc bezpečnostními pravidly klienta, která mu byla sdělena.

12. Kontrola a prokazování souladu

12.1 Objednatel je oprávněn přiměřeně ověřit, zda Dodavatel plní povinnosti podle těchto Podmínek a podle provozních pokynů Objednatele. Ověření Objednatel provádí zejména:

a) bezpečnostním dotazníkem nebo čestným prohlášením Dodavatele;
b) doložením konfigurace zařízení (např. snímek obrazovky, výpis nastavení);
c) výstupem ze schváleného bezpečnostního nástroje provozovaného na zařízení Dodavatele;
d) doložením nápravy zjištěného nedostatku;
e) cílenou kontrolou při bezpečnostním incidentu nebo důvodném podezření na něj.

12.2 Kontrola podle čl. 12.1 musí být přiměřená riziku, omezena na rozsah relevantní pro ochranu informací a systémů Objednatele a jeho klientů a vedena způsobem, který minimalizuje přístup k soukromým datům Dodavatele.

12.3 Dodavatel poskytuje součinnost při auditu prováděném klientem Objednatele, který věcně souvisí s konkrétní Dílčí smlouvou, a to v rozsahu odpovídajícím prokazování plnění bezpečnostních povinností; náklady takové součinnosti se řídí Smlouvou a Dílčí smlouvou.

13. Ukončení spolupráce

13.1 Ke dni ukončení Smlouvy nebo Dílčí smlouvy, případně dříve na pokyn Objednatele, Dodavatel:

a) přestává používat přístupy k informacím a systémům Objednatele a klientů Objednatele;
b) vrací zařízení, přístupové karty, certifikáty, tokeny a další prostředky předané Objednatelem;
c) předává Objednateli rozpracovanou práci, zdrojový kód, dokumentaci a další výstupy ve stavu odpovídajícím poslední dohodě;
d) odstraňuje lokální i jiné kopie informací Objednatele a informací klientů Objednatele uložené na zařízeních Dodavatele, pokud jejich uchování nevyžaduje právní předpis.

13.2 Dodavatel na vyžádání Objednatele písemně potvrdí, že povinnosti podle čl. 13.1 splnil.

13.3 Povinnost mlčenlivosti a ochrany informací podle Smlouvy trvá i po ukončení spolupráce.

14. Provozní pokyny a výjimky

14.1 Objednatel může Dodavateli předávat aktuální provozní bezpečnostní pokyny, zejména seznam zakázaných nebo schválených kategorií softwaru, seznam schválených bezpečnostních nástrojů, klasifikační pravidla, kontaktní kanály a konkrétní požadavky klienta. Provozní pokyn nemůže rozšířit smluvní povinnosti, finanční náklady ani rozsah odpovědnosti Dodavatele nad rámec těchto Podmínek a Dílčí smlouvy.

14.2 Výjimka z konkrétního požadavku těchto Podmínek musí být předem písemně schválena Bezpečnostním manažerem Objednatele. Výjimka může být časově omezená a vázaná na kompenzační opatření.

14.3 Při bezprostředním bezpečnostním riziku je Objednatel oprávněn dočasně omezit nebo zablokovat přístup Dodavatele k informacím nebo systémům. O důvodu a předpokládaném rozsahu informuje Dodavatele bez zbytečného odkladu.

14.4 Zjištěný nesoulad Dodavatel odstraní bez zbytečného odkladu po výzvě Objednatele; v případě závažného nedostatku přijme okamžité opatření ke zmírnění rizika ještě před úplnou nápravou.

15. Změny Podmínek

15.1 Objednatel je oprávněn tyto Podmínky v přiměřeném rozsahu jednostranně změnit postupem dle Smlouvy, zejména z důvodu vývoje bezpečnostních hrozeb, změn právních požadavků nebo požadavků klientů Objednatele.

15.2 Změna Podmínek je Dodavateli oznámena nejméně 30 dní před nabytím účinnosti způsobem stanoveným Smlouvou. Nevypoví-li Dodavatel Smlouvu postupem dle Smlouvy, nabývá změna účinnosti dnem v ní uvedeným. Vypoví-li Dodavatel Smlouvu z důvodu nesouhlasu se změnou Podmínek, řídí se vztah Smluvních stran do uplynutí výpovědní doby dosavadním zněním Podmínek.

15.3 Aktuální i archivní verze Podmínek jsou zveřejněny na https://www.greencode.cz/legal/terms. Každá verze obsahuje číslo verze a datum účinnosti.

16. Závěrečná ustanovení

16.1 Důsledky porušení těchto Podmínek se řídí Smlouvou. Tyto Podmínky nezavádějí samostatné smluvní pokuty.

16.2 V případě rozporu mezi českým zněním a jazykovými překlady těchto Podmínek je rozhodné české znění.

Historie verzí:

Verze	Účinnost od	Popis změny
1.0	[DOPLNIT]	První vydání