Zabezpečení dat v CODEXISu

Vaše data na bezpečném místě

CODEXIS®

Obsah

Information Security Management System 3

Nástroje ochrany zákaznických dat 4
Zabezpečení koncových bodů
Zabezpečení sítě a hardening serverů
Šifrování dat
Data při používání AI nástrojů
Fyzická bezpečnost
Uchovávání a likvidace dat

Řízení incidentů a zajištění kontinuity provozu 8
Monitoring systémů, logování a alerting
Zajištění kontinuity provozu

Nezávislé hodnocení 9

Školení bezpečnosti 9

Závěr 10

CODEXIS®

Information Security Management System

Jsme pevně přesvědčeni, že ochrana dat našich zákazníků je základním aspektem našich produktů. Náš specializovaný tým bezpečnostních expertů, který úzce spolupracuje s kolegy napříč všemi odděleními, přijímá komplexní opatření k identifikaci a minimalizaci rizik, zavádí špičkové postupy v oboru a neustále zlepšuje naše bezpečnostní protokoly.
Zavazujeme se udržovat vysoké standardy ochrany dat, abychom zajistili, že citlivé informace našich klientů zůstanou bezpečné a důvěrné. Tento důraz na bezpečnost dat odráží naše trvalé úsilí poskytovat našim zákazníkům spolehlivé služby.

ATLAS GROUP udržuje systém řízení bezpečnosti informací (ISMS), který je navržen tak, aby chránil důvěrnost, integritu a dostupnost dat. Tento program využívá širokou škálu bezpečnostních nástrojů pro síťovou i koncovou ochranu, aby zabránil neoprávněnému přístupu k zákaznickým datům.
Klíčovou součástí je soubor bezpečnostních opatření, které pokrývají oblasti jako řízení přístupů, řízení rizik, řízení změn, reakce na incidenty a další. Tyto opatření jsou minimálně jednou ročně aktualizovány, aby reflektovaly aktuální hrozby a osvědčené postupy v oboru.
Podobný přístup odpovídá průmyslovým standardům pro ISMS, které zahrnují dokumentaci a posouzení aktuálního stavu bezpečnosti, zavedení bezpečnostního řízení, pravidelné hodnocení rizik, zajištění kontinuity provozu a pravidelné školení zaměstnanců v oblasti bezpečnosti informací.
Pravidelná aktualizace opatření a procesů, včetně auditů a testování reakce na incidenty, zajišťuje, že ochrana dat zůstává efektivní a v souladu s globálními standardy a legislativními požadavky.
Díky tomuto komplexnímu systému je zajištěno, že zákaznická data jsou chráněna před neoprávněným přístupem, ztrátou i zneužitím, a to v souladu s nejlepšími praktikami v oblasti kybernetické bezpečnosti.

Náš bezpečnostní program je v souladu se směrnicemi normy ISO 27001. Společnost ATLAS Consulting je certifikována podle ISO 27001, ISO 27017 a ISO 27018 a tyto certifikáty lze na vyžádání poskytnout.

CODEXIS®

Nástroje ochrany zákaznických dat

Zabezpečení koncových bodů

Na firemních pracovních stanicích, notebocích ani vyměnitelných médiích neukládáme žádná zákaznická data. Zákaznická data jsou uložena pouze v produkčním prostředí, které podléhá přísným kontrolám a monitoringu.

Přístup do produkčního prostředí:
Týmy provozu a vývoje používají vyhrazené počítače s následujícími přísnými zásadami pro přístup do produkčního prostředí:

- Přísná omezení instalace softwaru
- Požadavky na silná uživatelská hesla
- Automatické uzamykání obrazovky
- Použití počítačů je omezeno pouze na úkoly související s provozem
- Řízení přístupu na základě rolí: Přístup s minimálními oprávněními odpovídajícími pracovní náplni.
- Zákaz mobilních zařízení: Přístup k důležitým systémům není povolen z vlastních zařízení zaměstnanců (BYOD).

Zabezpečení sítě a hardening serverů

Zákaznická data jsou logicky oddělena a šifrována jak při uložení, tak při přenosu. Dodržujeme standardní průmyslové postupy pro poskytovatele cloudových SaaS služeb, a to včetně využití multi-tenantní databáze, která umožňuje bezpečné sdílení infrastruktury mezi více zákazníky při zachování jejich datové izolace a integrity.
CODEXIS je provozován na vlastních serverech společnosti ATLAS GROUP, které se nacházejí ve vlastních objektech chráněných nepřetržitou fyzickou ostrahou 24/7.

Šifrování dat

Pro CODEXIS využíváme pokročilé šifrovací mechanismy k ochraně dat našich zákazníků. Náš systém implementuje robustní opatření a protokoly, které chrání celý životní cyklus citlivých informací, včetně vytváření, ukládání, načítání a likvidace tajných údajů, jako jsou šifrovací klíče a přihlašovací údaje servisních účtů.

Šifrovací postupy CODEXIS jsou navrženy tak, aby poskytovaly:

- Důvěrnost: Kódování dat, aby v případě zachycení nebyla srozumitelná neoprávněným osobám.
- Autentizaci: Ověření původu šifrovaných dat, tedy že data skutečně pocházejí od deklarovaného odesílatele.
- Integritu: Ověření, že data nebyla po zašifrování nijak změněna nebo poškozena.

Implementací těchto bezpečnostních opatření CODEXIS potvrzuje svůj závazek chránit citlivé informace zákazníků a udržovat nejvyšší standardy bezpečnosti dat v naší aplikaci.

Přenos dat

Šifrování TLS 1.3:	End-to-end ochrana pomocí nejnovějšího přenosového protokolu.
Bezpečný protokol:	Přenos souborů probíhá výhradně přes HTTPS.
Integrita dat:	Kryptografické hašování zajišťuje ochranu proti neoprávněným změnám během přenosu.

Data v úložišti

Úložiště:	Šifrované databáze AES-256 na vlastních úložištích
Oddělení dat:	Sdílené schéma s rozlišením prostoru pro jednotlivé klienty
Fyzická bezpečnost:	ISO 27001, fyzická ostraha 24/7/365 vlastních prostorů

Data při používání AI nástrojů

- Naše funkce využívající umělou inteligenci jsou postaveny na OpenAI API.
- Bez učení na datech zákazníků: Data odeslaná prostřednictvím OpenAI API nejsou využívána k trénování jazykových modelů.
- Šifrování dat: Všechna data jsou během přenosu šifrována (TLS 1.3), což minimalizuje riziko neoprávněného přístupu.
- Využíváme standardní 30denní retenci dat v rámci ochrany proti zneužití (abuse monitoring).
- Soulad s předpisy: OpenAI dodržuje předpisy, jako jsou GDPR, CCPA, SOC 2 a další standardy ochrany dat.

Uzamčení AI v CODEXISu (AI locked-in)

Co to znamená

- Ve výchozím (bezpečném) režimu jsou veškeré AI operace (např. sumarizace, odpovědi na dotazy, klasifikace) prováděny pouze nad daty, ke kterým má uživatel přístup. Nedochází ke sdílení dat mezi uživateli.
- AI má přístup pouze k datům, ke kterým má daný uživatel oprávnění, a pracuje s minimálním nutným kontextem (princip minimalizace dat).
- Žádná data z tenantního obsahu nejsou používána k tréninku modelů ani k jejich vylepšování.

Technické zarámování

- Všechny AI komponenty běží v řízeném prostředí CODEXIS s komunikací na minimum nezbytných třetích stran (OpenAI a AWS)
- Šifrování dat v klidu i při přenosu (TLS) je standardem; přístupy jsou chráněny ověřením a role-based kontrolou (RBAC/ABAC).
- Auditovatelnost: každá AI operace je logována (kdo, kdy, nad jakým obsahem, jaký typ operace) s možností exportu logů.

Fyzická bezpečnost

- Přístup pouze pro oprávněný personál
- RFID – náš bezpečnostní systém využívá technologii radiofrekvenční identifikace k povolení nebo odepření přístupu do chráněných prostor v našich objektech.
- Kontrola přístupu je kombinována s kamerovým dohledem (monitorování a záznam fyzických přístupových bodů).

Uchovávání a likvidace dat

Data jsou obecně uchovávána na dobu neurčitou, a to až do chvíle, kdy zákazník provede jejich smazání, nebo požádá o jejich smazání, nebo do doby vypršení smlouvy mezi zákazníkem a ATLAS GROUP.
V případě ukončení smlouvy jsou veškerá data i zákaznický účet nevratně smazány do 30 dnů od data vypršení licence CODEXIS. Po uplynutí této lhůty již data nelze obnovit, a to ani v případě, že zákazník uzavře nové předplatné služby CODEXIS.
Zpracování osobních údajů probíhá v souladu s platnými právními předpisy, zejména s obecným nařízením o ochraně osobních údajů (GDPR). Uživatelé mají kdykoli právo požádat o přístup ke svým osobním údajům, jejich opravu, přenositelnost nebo výmaz.
Data jsou zálohována každých 24 hodin.

Řízení incidentů a zajištění kontinuity provozu

Monitoring systémů, logování a alerting

ATLAS GROUP má zavedeno rozsáhlé monitorování, dohled a upozorňování v produkčním prostředí. Pro účely logování a monitorování využíváme několik specializovaných nástrojů.

Nastavení alertů je součástí non-stop monitorování aplikace. Na kritické alerty je reagováno okamžitě. CODEXIS využívá rozsáhlý systém monitorování, který automaticky upozorní specializovaný dohledový tým zajišťující provoz aplikací, jenž je k dispozici 24/7/365. V případě událostí ovlivňujících dostupnost služby CODEXIS neprodleně zahájí kroky k obnovení provozu s maximální možnou prioritou, dokud není služba plně obnovena.

Zajištění kontinuity provozu

ATLAS GROUP má vypracovaný Plán kontinuity provozu a obnovy. Tento plán obsahuje strategii a kroky pro obnovení klíčových aplikačních funkcí – včetně přechodu na záložní lokality, zajištění komunikace mezi klíčovými členy týmu a využití provozních postupů pro obnovu ze záloh. Plány každoročně testujeme a revidujeme. Náš plán kontinuity provozu a obnovy, včetně procesů a postupů, je auditován v rámci certifikací ISO 27001, ISO 27017 a ISO 27018.

3 způsoby, jak nás kontaktovat v případě dotazu z oblasti bezpečnosti, nebo při bezpečnostním incidentu:

Pomocí e-mailu na naše klientské centrum: klientske.centrum@atlasgroup.cz

Telefonátem na naše klientské centrum: +420 596 613 333

Kontaktováním obchodního zástupce, který prodej CODEXIS zprostředkoval.

CODEXIS®

Nezávislé hodnocení

Souhlad s bezpečnostními standardy

CODEXIS je provozováno v souladu s platnými zákony a předpisy, včetně GDPR.
Společnost ATLAS Consulting je certifikována podle ISO 27001, ISO 27017 a ISO 27018. Všechny certifikace jsou k dispozici na požádání.

Náš interní systém řízení bezpečnosti je každoročně přezkoumáván a aktualizován. Celý ISMS je auditován externím auditorem každé 2 roky.

Řízení zranitelností

Vývojový tým CODEXIS pravidelně kontroluje zranitelnosti napříč různými vektory. Před nasazením softwaru je kód skenován na chyby a zranitelnosti. CODEXIS také provádí časté skenování na úrovni aplikací, na koncových bodech a v síti.

ATLAS GROUP najímá třetí stranu, která každoročně provádí externí penetrační test. Zranitelnosti jsou hodnoceny na základě metodologie OWASP.

Reakce a náprava zranitelností ze strany ATLAS GROUP závisí na závažnosti a vyhodnocení rizika plynoucího z nálezů. ATLAS GROUP má stanované vlastní SLA na vyřešení podle závažnosti zranitelností. Souhrn výsledků penetračních testů lze poskytnout na požádání.

Školení bezpečnosti

Ve společnosti ATLAS GROU udržujeme komplexní program školení o bezpečnosti, jehož cílem je zajistit, aby všichni zaměstnanci rozuměli našim robustním bezpečnostním opatřením a postupům a dodržovali je. Náš program zahrnuje:

Hlavní složky školení

- Pravidla a opatření informační bezpečnosti
- Osobní odpovědnost a povinnosti
- Praktická bezpečnostní opatření (např. správa hesel)
- Postupy eskalace pro bezpečnostní problémy

Frekvence školení

- Povinné každoroční školení o bezpečnosti pro všechny zaměstnance
- Školení specifické pro jednotlivé role pro externí pracovníky
- Neustálé posilování klíčových konceptů po celý rok

Investováním do našeho programu školení o bezpečnosti CODEXIS prokazuje svůj závazek vytvářet kulturu zaměřenou na bezpečnost, chránit citlivá data a udržovat důvěru našich klientů.

Závěr

Naším cílem je umožnit jednotlivcům a organizacím strukturovat, organizovat a maximalizovat hodnotu z jejich dat. Proto ochranu vašeho soukromí a bezpečnosti považujeme za nejvyšší prioritu. Jsme odhodláni neustále vyvíjet nejlepší postupy na podporu tohoto principu.

Náš bezpečnostní tým je tu, aby odpověděl na jakékoli dotazy, které můžete mít. Můžete nás kontaktovat e-mailem na adrese klientske.centrum@atlasgroup.cz nebo se obrátit na svého obchodního zástupce.

CODEXIS®