AXION ACCEPTABLE USE POLICY

MAGYAR MASTER — Tervezet v1

1. Cél és hatály

Jelen Acceptable Use Policy / Elfogadható Felhasználási Szabályzat („AUP”) meghatározza az Axion Szolgáltatás megengedett és tiltott felhasználásának alapvető szabályait. Az AUP az Axion Általános Szerződési Feltételeivel, Adatkezelési Tájékoztatójával és más alkalmazandó szabályzatokkal együtt értelmezendő.

Az AUP az Axion valamennyi olyan funkciójára alkalmazandó, amely AI-modelleket, orchestrationt, webes kutatást, dokumentum- vagy fájlfeldolgozást, kódlétrehozást vagy kódfuttatást, sandboxot, Connected Service-t, külső integrációt vagy Actiont használ.

A Felhasználó felel azért, hogy saját használata, Inputjai, utasításai, integrációi, alkalmazásai és az Axion segítségével végzett műveletei megfeleljenek az alkalmazandó jognak és jelen AUP-nak.

2. Megengedett felhasználás

Az Axion jogszerű és felelős célokra használható, többek között kutatásra, információk összefoglalására és elemzésére, dokumentumok létrehozására és feldolgozására, programozásra és szoftverfejlesztésre, üzleti és kreatív munkafolyamatokra, oktatásra és tanulásra, valamint más olyan feladatokra, amelyek nem sértik jelen AUP-t.

Biztonsági, kiberbiztonsági, kutatási vagy tesztelési felhasználás megengedett lehet, ha az jogszerű, megfelelő felhatalmazáson alapul, kontrollált környezetben történik, és nem irányul jogosulatlan hozzáférésre, károkozásra, malware terjesztésére vagy más személy rendszerének megzavarására.

Az, hogy egy felhasználási mód általánosságban megengedett kategóriába tartozik, nem tesz jogszerűvé vagy elfogadhatóvá egy konkrét, károkozó vagy jogsértő végrehajtást.

3. Illegális, káros és visszaélésszerű tevékenységek

Tilos az Axiont bűncselekmény, jogellenes tevékenység, csalás, megtévesztés, lopás, zsarolás, jogellenes kereskedelem vagy más személyek, szervezetek vagy rendszerek károsításának előkészítésére, elősegítésére, végrehajtására vagy elrejtésére használni.

Tilos a Szolgáltatást olyan utasítások, workflow-k, kódok, dokumentumok vagy automatizmusok létrehozására vagy működtetésére használni, amelyek elsődleges célja jogellenes vagy káros tevékenység érdemi megkönnyítése.

Az Axion korlátozhat vagy megtagadhat olyan kéréseket, amelyek teljesítése a Szolgáltatás, a Felhasználó vagy harmadik személy biztonságát veszélyeztetné, vagy az alkalmazandó jogba, jelen AUP-ba vagy egy kötelező provider policyba ütközne.

4. Gyermekek kizsákmányolása és szexuális visszaélés

Szigorúan tilos gyermekek szexuális kizsákmányolásához vagy bántalmazásához kapcsolódó tartalom létrehozása, megszerzése, átalakítása, terjesztése, elősegítése vagy elrejtése, ideértve a gyermekek szexualizálását és grooming célú használatot.

Ez a tilalom attól függetlenül alkalmazandó, hogy a tartalom valós, szintetikus, módosított vagy AI által generált.

5. Erőszak, terrorizmus és veszélyes tevékenységek

Tilos az Axion használata terrorizmus, erőszakos szélsőségesség, célzott fizikai erőszak, súlyos sérülés vagy mások elleni erőszak érdemi elősegítésére, szervezésére vagy végrehajtására.

Tilos olyan fegyverek, robbanóanyagok, vegyi, biológiai, radiológiai vagy nukleáris fegyverek vagy más veszélyes eszközök létrehozásának, megszerzésének vagy alkalmazásának érdemi elősegítése, amely jogellenes vagy személyek, szervezetek vagy a társadalom károsítására irányul.

6. Önkárosítás és veszélyeztetés

Tilos az Axiont önkárosítás, öngyilkosság, súlyos önveszélyeztetés vagy más személy veszélyeztetésének ösztönzésére, optimalizálására vagy gyakorlati végrehajtásának elősegítésére használni.

Az Axion támogathat olyan biztonságos, megelőző, oktatási vagy segítségkérést támogató felhasználást, amely nem segíti elő a károkozást.

7. Kiberbiztonság, malware és rendszer-visszaélés

Tilos jogosulatlan hozzáférés, credential theft, phishing, malware, ransomware, botnet, destructive payload, command-and-control infrastruktúra, szolgáltatásmegtagadási támadás vagy más rosszindulatú cyber activity létrehozása, telepítése, működtetése vagy érdemi elősegítése.

Tilos más személy rendszerének, fiókjának, hálózatának, adatainak vagy szolgáltatásának engedély nélküli feltörése, megfigyelése, megzavarása vagy károsítása.

Jogszerű defensive security, saját rendszer tesztelése, engedélyezett penetrációs teszt, CTF, malware analysis és biztonsági oktatás megengedett lehet, amennyiben megfelelő jogosultság, scope és biztonságos környezet áll fenn.

8. Az Axion és a provider-biztonsági rendszerek megkerülése

Tilos az Axion hozzáférési korlátozásainak, rate limitjeinek, security controljainak, policy enforcementjének, jogosultsági határainak vagy más védelmi mechanizmusainak jogosulatlan megkerülése, kikapcsolása vagy manipulálása.

Tilos prompt injection, jailbreak, tool manipulation vagy más technika alkalmazása abból a célból, hogy a Felhasználó jogosulatlan rendszerutasítást, secretet, más Felhasználó adatát vagy olyan erőforrást szerezzen meg, amelyhez nincs hozzáférési joga.

Biztonsági kutatás vagy hibajelentés céljából végzett kontrollált vizsgálat kizárólag az Axion által engedélyezett keretek, scope és alkalmazandó szabályok szerint végezhető.

9. Adatvédelem, személyes adatok és megfigyelés

Tilos személyes adatok, biometrikus adatok, hitelesítési adatok vagy más érzékeny információk jogellenes megszerzése, összegyűjtése, deanonymizálása, közzététele vagy felhasználása.

Tilos személyek beleegyezés vagy más megfelelő jogalap nélküli követése, megfigyelése vagy profilozása, ha azt az alkalmazandó jog tiltja.

A Felhasználó kizárólag olyan harmadik személyre vonatkozó adatot, Connected Service adatot vagy szervezeti adatot tehet elérhetővé az Axion számára, amelynek feldolgozására megfelelő jogosultsággal és jogalappal rendelkezik.

10. Zaklatás, gyűlölet és kizsákmányolás

Tilos az Axion használata célzott zaklatás, megfélemlítés, stalking, fenyegetés, bántalmazás, kizsákmányolás vagy személyek illetve védett csoportok elleni gyűlölet és erőszak elősegítésére.

Tilos más személy sebezhetőségének olyan kihasználása vagy manipulációja, amely jelentős fizikai, pszichológiai, pénzügyi vagy más kárral járhat.

11. Szexuális tartalom és beleegyezés nélküli intim tartalom

Tilos gyermekeket érintő bármilyen szexuális tartalom, valamint beleegyezés nélküli intim vagy szexuális tartalom létrehozása, módosítása, terjesztése vagy elősegítése.

Az Axion korlátozhat más explicit szexuális vagy pornográf felhasználást is a Szolgáltatás biztonsági követelményei és az alkalmazandó upstream provider policyk alapján.

12. Csalás, megtévesztés, impersonation és spam

Tilos csalás, scam, phishing, hamis személyazonosság, megtévesztő impersonation, hamis dokumentum vagy más megtévesztő gyakorlat létrehozása vagy elősegítése, ha annak célja mások megtévesztése, jogainak megsértése vagy jogtalan előny szerzése.

Tilos kéretlen tömeges üzenetek, spam vagy megtévesztő automatizált kommunikáció létrehozására vagy terjesztésére használni az Axiont.

AI által létrehozott tartalom eredetét nem szabad megtévesztő módon kizárólag ember által létrehozottként feltüntetni, ha ez mások megtévesztésére szolgál vagy az alkalmazandó jog/termékpolicy disclosure-t ír elő.

13. Szellemi tulajdon és mások jogai

Tilos az Axion használata szerzői jog, védjegy, üzleti titok, személyiségi jog, adatvédelmi jog vagy más harmadik személyi jog tudatos megsértésére vagy kijátszására.

A Felhasználó felel azért, hogy az Axion számára biztosított Input, fájl, adat, kód és más tartalom használatához szükséges jogokkal rendelkezzen, és az Outputot jogszerű módon használja fel.

14. Magas hatású és szabályozott döntések

Az Axion nem használható megfelelő emberi felügyelet nélkül olyan kizárólag vagy lényegében automatizált döntés meghozatalára, amely egy természetes személy jogaira, jogi helyzetére, életlehetőségeire vagy alapvető érdekeire jelentős hátrányos hatással lehet.

Ez különösen releváns lehet foglalkoztatás, hitelezés és pénzügy, biztosítás, egészségügy, lakhatás, oktatás, jogi szolgáltatások, szociális ellátás és más magas kockázatú területeken.

A Felhasználó felel a szükséges szakmai felülvizsgálatért, emberi felügyeletért, jogalapért, tájékoztatásért, auditálhatóságért és az alkalmazandó AI- és ágazati szabályok betartásáért.

15. Connected Services, Actions és külső rendszerek

A Felhasználó kizárólag olyan Connected Service-hez, fiókhoz, mailboxhoz, fájlhoz, naptárhoz, repositoryhoz, API-hoz vagy más külső rendszerhez kapcsolhatja az Axiont, amelynek használatára megfelelő jogosultsággal rendelkezik.

Tilos az Axion Actions vagy más végrehajtási képességeinek használata jogosulatlan üzenetküldésre, fájlmódosításra, adatkinyerésre, tranzakcióra, account operationre vagy más külső hatás kiváltására.

Ahol az Axion confirmationt vagy más User approvalt kér egy külső hatású művelethez, tilos e kontroll megtévesztő vagy technikai megkerülésére törekedni.

16. Kód, sandbox és User-operated applications

Az Axion segítségével létrehozott vagy futtatott kód, workflow és User-operated application nem használható jelen AUP megkerülésére. Ugyanazok a korlátozások alkalmazandók akkor is, ha a tiltott műveletet közvetlen prompt helyett generált kód, automatizmus, agent vagy külső alkalmazás hajtja végre.

A Felhasználó felel a generált kód és alkalmazás production használat előtti felülvizsgálatáért, teszteléséért, jogosultságaiért, adatkezeléséért és biztonságos konfigurációjáért.

Tilos sandboxot vagy code-execution környezetet más rendszerek jogosulatlan támadására, erőforrásokkal való visszaélésre, malware futtatására vagy tiltott tartalom infrastruktúrájaként használni.

17. Biztonsági, oktatási, tudományos és közérdekű kivételek

Egy egyébként érzékeny téma elemzése megengedett lehet, ha annak célja egyértelműen jogszerű biztonsági, oktatási, dokumentációs, tudományos, újságírói vagy más közérdekű felhasználás, és a kérés nem nyújt olyan gyakorlati segítséget, amely érdemben növeli a károkozás képességét.

Az Axion az ilyen kérések teljesítését korlátozhatja, biztonságosabb formára alakíthatja vagy megtagadhatja, ha a kockázat, a kontextus vagy valamely alkalmazandó provider policy ezt indokolja.

18. Provider policyk és funkcióspecifikus korlátozások

Az Axion több külső AI-, cloud-, search-, sandbox- és más technológiai providert használhat. Egyes funkciókra ezért az adott provider kötelező használati vagy biztonsági szabályai is alkalmazandók.

Ha egy Axion-funkció technikai vagy szerződéses okból szigorúbb provider-korlátozás alá esik, az Axion az adott funkciónál ezt a szigorúbb korlátozást alkalmazhatja akkor is, ha ugyanaz a felhasználás egy másik Axion-funkciónál általánosságban nem lenne tiltott.

A Felhasználó nem jogosult arra, hogy az Axiont provider policyk, safety filterek vagy más kötelező korlátozások megkerülésére használja.

19. Enforcement és intézkedések

Az Axion az AUP megsértésének megelőzése, felismerése és kivizsgálása érdekében alkalmazhat automatizált és manuális biztonsági, abuse-prevention és policy enforcement kontrollokat az alkalmazandó joggal és az Adatkezelési Tájékoztatóval összhangban.

Az Axion a jogsértés vagy kockázat jellegétől, súlyosságától és ismétlődésétől függően megtagadhat vagy korlátozhat egy kérést vagy funkciót, figyelmeztetést adhat, ideiglenesen korlátozhatja a hozzáférést, felfüggesztheti vagy megszüntetheti az Accountot, illetve megteheti a jogszabály vagy szerződés által szükséges egyéb intézkedést.

Súlyos vagy sürgős biztonsági kockázat esetén az Axion előzetes értesítés nélkül is alkalmazhat azonnali védelmi intézkedést, ha ezt az alkalmazandó jog és az ÁSZF lehetővé teszi.

20. Bejelentés, módosítás és elsőbbség

Feltételezett visszaélés, biztonsági probléma vagy AUP-sértés a support@axionaiapp.com címen jelezhető.

Az Axion az AUP-t a Szolgáltatás, a technológiai képességek, a jogszabályok, a fenyegetési környezet vagy a provider-követelmények változásával módosíthatja. A hatályos verzió a Szolgáltatáshoz kapcsolódó jogi felületen kerül közzétételre.

Ha jelen AUP és valamely kötelező jogszabály között eltérés van, a kötelező jogszabály alkalmazandó. Ha egy konkrét Axion-funkcióra kötelező provider policy szigorúbb korlátozást ír elő, az Axion az adott funkció tekintetében a szigorúbb szabályt alkalmazhatja.

[LAUNCH REQUIREMENT: a publikus verzió előtt össze kell vetni az AUP-t az Axion végleges ÁSZF-ével, a productionben ténylegesen használt AI/cloud provider policykkal, az EU AI Act alkalmazandó tiltott gyakorlatokra vonatkozó követelményeivel, valamint az Axion enforcement és appeal/support folyamatával. A publikus verzióból minden belső marker eltávolítandó.]

Utolsó frissítés: [DÁTUM]
Hatálybalépés: [DÁTUM]
Verzió: [VERZIÓ]