

SITRAIN Acceptable Use Policy

September 2021

Pro zobrazení české verze prosím scrollujte dolů 

This Acceptable Use Policy (“AUP”) sets out terms you, and those acting on your behalf, must comply with when using the online services made available by us (“Cloud Services”).

1. Credentials

You will:

- not use a false identity to gain access to the Cloud Services;
- carefully store access credentials and security tokens and protect them from unauthorized access, disclosure or use;
- not gain access to Cloud Services by any means other than your user account or other means permitted by us;
- not circumvent or disclose the authentication or security of your user account, the underlying technology or any host, network, or account related thereto; and
- ensure that any access credentials are not shared with other individuals and used only by the individual who was granted the credentials. We may change access credentials if we determine at our reasonable discretion that a change is necessary.

2. No Illegal, Harmful, or Offensive Use or Content

You will not use, or encourage, promote, facilitate, or instruct others to use, Cloud Services for any illegal, harmful, or offensive use or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Your use of the Cloud Services and your content stored within the Cloud Services will not:

- violate any laws or regulations, or rights of others;
- be harmful to others, or to our reputation, including by offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi or pyramid schemes, phishing, farming, or other deceptive practices;
- enter, store or send hyperlinks, or enable access to external websites or data feeds, including embedded widgets or other means of access, in or as part of your content, for which you have no authorization, or which are illegal;
- be defamatory, obscene, abusive, invasive of privacy otherwise objectionable.

3. No violation of use restrictions

You will not:

- resell, transfer, sublicense, loan, lease or publish Cloud Services, or use Cloud Services in the operation of a business process outsourcing or other outsourcing or a time-sharing service (unless expressly permitted by us);
- reverse engineer, disassemble, decompile, or otherwise modify, create derivative works based on, merge, tamper with, repair, or attempt to discover the source code of, Cloud Services or the underlying technology (except to the extent this restriction conflicts with the applicable law of your jurisdiction);

- access Cloud Services from any location prohibited by or subject to sanctions or license requirements according to applicable sanctions and/or (re-)export control laws and regulations, including those of the European Union, the United States of America and/or any other applicable country(ies), and you will only upload non-controlled content (e.g. classification is “N” in the EU, and “N” for ECCN or “EAR99” in the U.S.), unless permitted otherwise by the applicable (re-)export control laws or respective governmental licenses or approvals.

4. No Abusive Use

You will not:

- use Cloud Services in a way intended to avoid or work around any use limitations and restrictions placed on such Cloud Services (such as access and storage restrictions), monitoring, or to avoid incurring fees;
- access or use Cloud Services for the purpose of conducting a performance test, building a competitive product or service or copying its features or user interface;
- interfere with the proper functioning or security of any of our systems;
- distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations, including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission.

5. No Security Violations

You will not use Cloud Services in a way that could result in or facilitate a threat to the security of Cloud Services or the underlying technology. You will in particular:

- take reasonable precautions against security attacks, viruses and malicious code on your system, on-site hardware, software or services that you use to connect to and/or access Cloud Services;
- not perform any penetration test of or on Cloud Services or the underlying technology without obtaining our express prior written consent; and
- not use devices to access or use Cloud Services that do not comply with industry standard security policies (e.g., password protection, virus protection, update and patch level).

6. Our Monitoring; Reporting and Audit

You acknowledge that we and our subcontractors may monitor your compliance with this AUP through Cloud Services. We reserve the right to investigate any violation of this AUP. If you become aware of any violation of this AUP, you will immediately notify us and provide us with assistance, as requested by us, to stop, mitigate or remedy the violation. We, our subcontractors or authorized agents may conduct an audit of your compliance with this AUP at your premises, workstations and servers upon reasonable advance notice. We may remove, disable access to, or modify any content or resource that violates this AUP or any other agreement we have with you for use of the Cloud Services. We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. If a party that claims that your use of the Cloud Services or your content violates such third party’s rights or any law or regulation, we may share appropriate customer information.

7. Copyright

Siemens will respond to notices of copyright infringement regarding content in accordance with applicable copyright laws.

Podmínky používání SITRAIN

Září 2021

Tyto Podmínky pro přijatelné používání (Acceptable Use Policy, "AUP") stanovují podmínky, které Vy a osoby jednající Vaším jménem musíte dodržovat při používání online služeb, které Vám poskytujeme ("Cloudové služby").

1. Přihlašovací údaje

Zavazujete se:

- nepoužívat falešnou identitu k získání přístupu ke Cloudovým službám;
- pečlivě uchovávat přístupové údaje a bezpečnostní tokeny a chránit je před neoprávněným přístupem, zveřejněním nebo použitím;
- nezískávat přístup ke Cloudovým službám jinými prostředky než prostřednictvím Vašeho uživatelského účtu nebo jiných námi povolených prostředků;
- neobcházet ani nezveřejňovat autentizaci nebo zabezpečení Vašeho uživatelského účtu, základní technologie nebo jakéhokoli hostitele, sítě nebo souvisejícího účtu;
- zajistit, aby přístupové údaje nebyly sdíleny s jinými osobami a byly používány pouze osobou, které byly tyto údaje přiděleny. Můžeme změnit přístupové údaje, pokud na základě našeho rozumného uvážení určíme, že je změna nezbytná.

2. Zákaz nelegálního, škodlivého nebo urážlivého použití či obsahu

Nebudete používat, podporovat, propagovat, usnadňovat ani instruovat ostatní k používání Cloudových služeb pro jakékoli nelegální, škodlivé nebo urážlivé účely, ani k přenosu, ukládání, zobrazování, distribuci nebo jinému zpřístupňování obsahu, který je nelegální, škodlivý, podvodný, porušující práva nebo urážlivý. Vaše používání Cloudových služeb a Váš obsah uložený v rámci Cloudových služeb nesmí:

- porušovat žádné zákony, předpisy nebo práva jiných osob;
- být škodlivé pro ostatní nebo pro naši pověst, včetně nabízení nebo šíření podvodného zboží, služeb, schémat nebo propagací, schémat rychlého zbohatnutí, Ponziho nebo pyramidových schémat, phishingu, farmingu nebo jiných klamavých praktik;
- vkládat, ukládat nebo odesílat hypertextové odkazy nebo umožňovat přístup k externím webovým stránkám nebo datovým zdrojům, včetně vložených widgetů nebo jiných prostředků přístupu, jako součást Vašeho obsahu, k nimž nemáte oprávnění nebo které jsou nelegální;
- být hanlivé, obscénní, urážlivé, narušující soukromí nebo jinak nevhodné.

3. Zákaz porušování omezení použití

Zavazujete se:

- neprodávat, nepřevádět, neposkytovat sublicence, nepůjčovat, nepronajímat ani nepublikovat Cloudové služby, ani nepoužívat Cloudové služby při provozování outsourcingu obchodních procesů nebo jiného outsourcingu nebo služby časového sdílení (pokud to výslovně nepovolíme);
- neprovádět zpětné inženýrství, nerozebírat, nedekompilovat ani jinak neupravovat, nevytvářet odvozená díla, neslučovat, nezasahovat, neopravovat ani se nepokoušet objevit zdrojový kód Cloudových služeb nebo základní technologie (s výjimkou případů, kdy je toto omezení v rozporu s platnými zákony Vaší jurisdikce);
- nepřístupovat ke Cloudovým službám z míst zakázaných nebo podléhajících sankcím či licenčním požadavkům podle platných sankčních a/nebo (re-)exportních kontrolních zákonů a předpisů, včetně

zákonů Evropské unie, Spojených států amerických a/nebo jakékoli jiné platné země, a budete nahrávat pouze nekontrolovaný obsah (např. klasifikace "N" v EU a "N" pro ECCN nebo "EAR99" v USA), pokud není povoleno jinak příslušnými (re-)exportními kontrolními zákony nebo příslušnými vládními licencemi či schváleními.

4. Zákaz zneužívání

Zavazujete se:

- nepoužívat Cloudové služby způsobem, který má za cíl vyhnout se nebo obejít jakákoli omezení použití a omezení kladená na takové Cloudové služby (jako jsou omezení přístupu a ukládání), monitorování nebo vyhnout se poplatkům;
- nepřistupovat k Cloudovým službám ani je nepoužívat za účelem provádění výkonnostních testů, vytváření konkurenčního produktu nebo služby nebo kopírování jejich funkcí nebo uživatelského rozhraní;
- nezasahovat do řádného fungování nebo zabezpečení našich systémů;
- nešířit, nepublikovat, neodesílat ani neusnadňovat odesílání nevyžádaných hromadných e-mailů nebo jiných zpráv, propagací, reklam nebo nabídek, včetně komerční reklamy a informačních oznámení. Nebudete měnit ani zakrývat hlavičky e-mailů ani přebírat identitu odesílatele bez výslovného souhlasu odesílatele.

5. Zákaz porušování bezpečnosti

Nebudete používat Cloudové služby způsobem, který by mohl vést k ohrožení nebo usnadnění ohrožení bezpečnosti Cloudových služeb nebo základní technologie. Zejména:

- přijmete přiměřená preventivní opatření proti bezpečnostním útokům, virům a škodlivému kódu ve Vašem systému, hardwaru na místě, softwaru nebo službách, které používáte k připojení k Cloudovým službám a/nebo k přístupu k nim;
- nebudete provádět žádné penetrační testy Cloudových služeb nebo základní technologie bez získání našeho výslovného předchozího písemného souhlasu;
- nebudete používat zařízení pro přístup k Cloudovým službám nebo jejich používání, která nejsou v souladu s oborovými standardními bezpečnostními zásadami (např. ochrana heslem, ochrana proti virům, aktualizace a úroveň záplat).

6. Naše monitorování; Hlášení a audit

Berete na vědomí, že my a naši subdodavatelé můžeme monitorovat Vaše dodržování těchto AUP prostřednictvím Cloudových služeb. Vyrazujeme si právo vyšetřit jakékoli porušení těchto AUP. Pokud se dozvíte o jakémkoli porušení těchto AUP, okamžitě nás o tom budete informovat a poskytnete nám pomoc, kterou požadujeme, k zastavení, zmírnění nebo nápravě porušení. My, naši subdodavatelé nebo pověřeni zástupci můžeme provést audit Vašeho dodržování těchto AUP ve Vašich prostorách, na pracovních stanicích a serverech po přiměřeném předchozím oznámení. Můžeme odstranit, zakázat přístup nebo upravit jakýkoli obsah nebo zdroj, který porušuje tyto AUP nebo jakoukoli jinou smlouvu, kterou s Vámi máme pro používání Cloudových služeb. Můžeme nahlásit jakoukoli činnost, o níž se domníváme, že porušuje jakýkoli zákon nebo předpis, příslušným orgánům činným v trestním řízení, regulačním orgánům nebo jiným příslušným třetím stranám. Pokud strana tvrdí, že Vaše používání Cloudových služeb nebo Váš obsah porušuje práva takové třetí strany nebo jakýkoli zákon či předpis, můžeme sdílet příslušné informace o zákazníkovi.

7. Autorská práva

Siemens bude reagovat na oznámení o porušení autorských práv týkajících se obsahu v souladu s platnými zákony o autorských právech.