Acceptable Use Policy

July 2021

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 countr(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 / DMCA**. Siemens will respond to notices of copyright infringement regarding content in accordance with its Copyright Policy. The Copyright Policy is available at https://www.siemens.com/sw-terms/dmca.