HELIOS ACCEPTABLE USE POLICY

Last Updated: March 8, 2021

Tx3 Helios provides a secure, high performing environment for customers to run business applications. In order to maintain operations, Tx3 requires you, the end user, not to misuse or abuse any system or service. This policy describes areas of misuse or abuse, and by using a system in the Helios environment, you agree to these terms, and must comply with all applicable national and international laws/regulations.

Additionally, Tx3 reserve the right to remove/disable access, or modify content, if Tx3 deems an action is in violation of this or any other policy/agreement.

The system is provided only for its intended use. Restrict use to appropriately trained users, monitoring and controlling their access. Notify Tx3 of unauthorized activity or security breach.

Do not perform any harmful activities that can be categorized in the areas below.

Misuse/Abuse

- Do not perform any activity that disrupts, interferes with, or impedes operation or has the potential to do so.
- Do not perform or enable any Actions/automation/activities that disrupt Network or Server operation, including Denial of Service attacks, intentionally harmful queries/reports, monitoring, crawling, mail bombing, broadcast attacks, flooding techniques, or any attempt to overload a system.
- Uploading any harmful data or components such as a virus, trojan horse, worm, etc.
- Do not permit or enable unauthorized 3rd party access or encourage a 3rd party to violate any item in these service agreements.
- Do not impersonate another user
- Do not avoid or attempt to work around protective system restrictions through manual or electronic means.
- Do not use contact information or any other information obtained from this service to contact others without their permission or to use such information outside of this service.
- Do not consume storage that is unrelated to system or its purpose. For example, uploading video, music, or any other information unrelated the business.

Illegal or Fraudulent activities

- Do not share/transfer/provide access to another person. Keep login information confidential.
- Do not misrepresent or violate privacy of others
- Do not attempt or provide unauthorized access to any other person.
- No Infringement Activity such as:
  - Attempting to reverse engineer, hack, disable, modify or copy any part of the system or access the system for the purposes of building a competitive product.
  - Using the system to send unsolicited communications, advertisements, or spam
  - Do not exploit the system by attempting to sublicense, resell, or share access.
- No Falsifying Origin via techniques such as forging TCP-IP packet headers, email headers or any part of a message describing its origin/route.

Inappropriate activity

- Inappropriate communication, uploading inappropriate content.
- Do not upload/transmit unlawful data or information that could violate copyrights, trademarks, or Intellectual Property.
- Do not upload or send offensive content or engage in any activity that incites violence or hatred.
- Do not upload or disseminate any information or communication that is deceptive, fraudulent, illegal, obscene, indecent, harassing, or harmful to others.
- Do not abuse email or messaging functionality