Tektronix®

Security at TekCloud

Learn How TekCloud Manages Security

Tektronix maintains and enforces internal security policies covering: Data Access, Security Incident Response, System Access, Risk Management, and Vulnerability Management.

1. Data is encrypted at rest and in transit (TLS).
2. TekCloud's backend network leverages Amazon Virtual Private Cloud (VPC) providing a certain level of isolation between the different organizations.
3. Tektronix access control measures such as IP filtering enable us to control what IP traffic will be allowed into and out of our network. Identity and Access Management (IAM) ensures that the right users have the appropriate access to technology resources. Multi-factor authentication (MFA) can be used in TekCloud to ensure that users are authenticated by requiring at least two pieces of evidence be provided to prove their identity.

TekCloud delivers assurance for their data and privacy as our users create the next generation of technology.

1. TekCloud follows all GDPR and CCPA requirements. We will not use any users' personal data without their permission.
2. TekCloud follows all Payment Card Industry Data Security Standard (PCI DSS) requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.
3. TekCloud uses a certified PCI-Service Provider Level 1 payment service. We do not store any payment data.
4. Read the Tektronix Privacy Policy here.

Assurance via Availability and Regional Distribution: We strive for 99.99% service uptime. Our services scale on demand to ensure a quick response, regardless of the load. Data is continuously backed up on AWS.

090822 61W-73939-0