Autodesk Tandem & Tandem Connect IT/Data Security

At Autodesk, we are committed to delivering high availability, ensuring our customers can fully harness the power of our cutting-edge products. Autodesk Tandem and Autodesk Tandem Connect, both cloud-based solutions, adhere to Autodesk's rigorous security policies, which you can explore here.

Key Highlights

- **Project Data Storage & Redundancy:** Autodesk Tandem and Tandem Connect are both cloud-based software hosted on AWS, with data centers in the United States and the European Union (EU). This gives customers greater control of their data and helps optimize performance.
- **Data Encryption:** Our data is transmitted over HTTPS protocol through the browser. Tandem Connect can transmit data through HTTPS, BACNET, or MQTT protocols subject to its configuration.
- **System Health:** The Autodesk Tandem and Tandem Connect teams within Autodesk take continuous monitoring of system performance seriously and employ appropriate tools and processes to deliver the service our customers expect. Visit our Health Dashboard to view the real time health status and scheduled maintenance for Autodesk Tandem. We use security technologies like endpoint protection, identity and access management, encryption in transit and at rest, and network and application firewalling.

Visit our Security Advisories page to review vulnerabilities and threat activity that could affect Autodesk products, services, or users.

For additional insights into our security and compliance measures and to request Tandem's SOC2 report, visit the Autodesk Trust Center.

For any questions, comments, or concerns, don't hesitate to get in touch with support here.