Infrastructure & Security

Purpose

Projetech is committed to ensuring confidentiality, integrity, and availability of all customer data. Projetech systems are designed to ensure proper security with technology and Maximo best practices applied. Projetech adheres to a "defense in depth" strategy to provide a layered approach to security.

This document provides an overview of Projetech infrastructure, policies, and controls that ensure customer assets are protected. The scope of this document includes all Projetech cloud infrastructure and customer data.

Security

Projetech has architected a solution to ensure customer data is always protected. Projetech uses data centers that maintain multiple industry compliance certifications (SOC, ISO, CSA STAR). All access to Projetech clouds is encrypted and requires multi-factor authentication. All in-transit web application transactions and file transfers are encrypted using HTTPS\TLS with all at-rest data being encrypted with AES, following FIPS 140-2 best practices.

Projetech employs next-gen firewalls and a SIEM security solution integrated with a 24/7 incident response system. Projetech's solution logging is integrated into a security system that leverages real-time threat intelligence data and is retained for up to 1 year. Projetech has implemented a framework of security controls and policies by obtaining an ISO 27001 certification and has also taken a cloud security focus with an ISO 27017 certification.

Identity & Access Management

Projetech adheres to least access principles for all application and infrastructure access. Only authenticated users are given access to assets where there is a specific need. Projetech offers SAML and Active Directory solutions for secure application and infrastructure access. Access controls are reviewed via external auditors and 3rd party penetration testing.

Infrastructure

Projetech has multiple data centers located in Dallas TX, Washington D.C, and Sydney AU. Projetech runs industry standard virtualization software utilizing encryption at the virtual system layer. All Projetech SANs utilize disk level encryption. All networks are setup to be customer/partner specific with all traffic to or from the network passing through next-gen firewalls. Projetech employs 24/7 multi-layer real-time monitoring of all customer/partner systems which is integrated with a support ticketing system to ensure proper incident response. Networking activity and performance, database performance, Maximo application events and other security-related events are all monitored as part of our service. All infrastructure equipment is built to meet high availability standards of 99.99%. All communication between data centers occurs over dedicated WAN links or VPN tunnels to protect all data in-transit.

Data Backup, Archival, and Disaster Recovery

Projetech places a high priority on data protection. Projetech performs daily backups of all virtual machines and hourly backups of all customer data for a recovery point objective of 2 hours using the 3-2-1 methodology. Backups are replicated to a 2nd data center for disaster recovery (DR) purposes. All backups are copied to a 3rd data center for additional protection. All replication is done between data centers using TLS communication as well as over VPN tunnels to protect all data in flight. All backups use AES-256 encryption in-transit and at-rest. Projetech uses the Dallas and Washington data center's as production and disaster recovery data centers. In the event of a single data center failure, the systems are replicated to the secondary data center in near real time at which point the systems in the secondary data center are turned on, communication between systems is validated, DNS entries are changed to point to the secondary data center, and the system are brought online. The system backups also reside in a third data center. In the event of a failure in two data centers, systems are restored from backup then brought online as described in the preceding process. Projetech uses Veeam and VMWare for our backup and replication processes across all data centers.