Data Security

CityBase is committed to maintaining a world-class information security program. Security is treated as a core product feature, and not just an add-on. We are dedicated to constantly improving our multifaceted security program to support our platform, and the people and businesses that rely on it.

The CityBase Approach

Adhere to Industry Security Standards

All assessments are completed by an independent accredited third party. CityBase is a PCI Level-1 Compliant Service Provider and is SOC 1 & SOC 2 certified. CityBase systems never store sensitive cardholder data.

Encrypt Customer Data to Avoid Data Breaches

CityBase has never experienced a data breach. We ensure security for all levels of data and encrypt data while at rest and in motion. To protect sensitive data in transit, CityBase uses TLS 1.2. Sensitive customer data at rest is encrypted using AES265 encryption.

Fully Cloud-Based Technology

All CityBase applications are 100% cloud-based, using three fully redundant, geographically distributed AWS data centers to support our platform.

Proactive Monitoring for Security Events

Next-generation cloud security monitoring and alerting tools are used for all critical infrastructure components and payment systems. These tools, including Wazuh, Uptycs, CrowdStrike, and the ELK Stack, provide proactive alerting and response capabilities to inspect all inbound and outbound traffic, and flag and block any suspicious IP address.

Maintain a Multi-Faceted Disaster Recovery Plan (DRP)

CityBase maintains a Disaster Recovery Plan that includes steps to ensure the safety of employees, re-establish essential services, and mitigate any impact on customers throughout the emergency condition, disaster declaration, and recovery process.