BIGTIME

Security Guide

Table of Contents

1 Introduction

2 Infrastructure Security

3 Application Security

5 GDPR and Data Privacy Compliance

6 Risk and Compliance

7 Infrastructure Operations

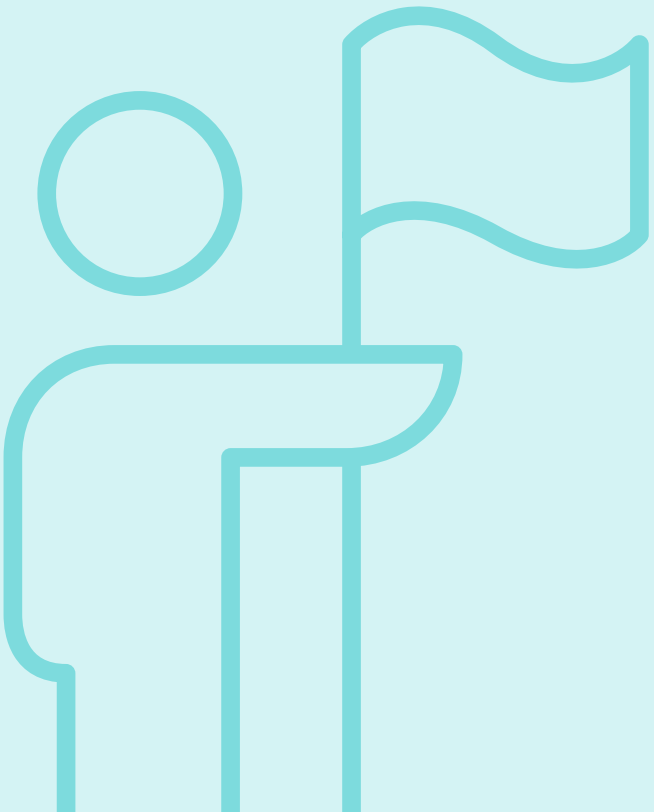
8 BigTime Wallet and Financial Information

Introduction

Infrastructure, Security, and Privacy
Your data is safe with us.

Our team obsesses over your company's privacy and security. We provide industry-leading time-tracking, billing, and project management software for more than 2,500 professional service firms, tracking over $4 billion (USD) of billable time each year.

Our flagship product is a SaaS-based system that is custom-built for the professional services industry, and specifically for accounting, architecture, engineering, consulting, creative, government contracting, IT services, and law firms. In this document, you'll learn about BigTime's security protocols and the lengths we go to in order to ensure your data is secure.



Infrastructure Security

Physical Security

BigTime is built on Amazon Web Services (AWS) and utilizes AWS services such as Shield, Web Application Firewalls, and Guard Duty to help secure our workloads. Even for our internal IT team, access to cloud services is restricted and only available to authorized personnel via secure channels. Throughout the day, while your team is working, our infrastructure group is taking frequent backups, and storing them across redundant locations. Corporate and AWS hosted networks are segregated using VPC, and our Multi-Tenant Environment is secured using a proprietary data access letter.

Because we use Amazon Web Services, the servers your data is stored/processed on are physically secure. "Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors." More information can be found on the AWS website at: http://aws.amazon.com/compliance and https://aws.amazon.com/security/.

Application Security

Multi-tenant Architecture

BigTime is a highly scalable multi-tenant SaaS application, architected from the ground up with security and privacy as cornerstone values. Your "tenant" data is isolated from all other tenants, and our system is hard-coded to prevent access by anyone other than authorized users within your firm. We release code updates and bug fixes to all our customers on a monthly basis, and because we leverage the Agile software development methodology, we are able to deploy improvements with 99.9% uptime. You can learn more about our Service Level Agreement for Premier customers here.

All of our customer's data is segmented at the data-access level, and our automated testing approach incorporates regular security reviews to ensure even malicious users can't access data you haven't authorized them to see. With BigTime, you're in total control of who sees your data.

Software Development Life-Cycle

We implement quality assurance and code review processes to ensure we are always releasing high-quality web and mobile experiences without sacrificing security or customer satisfaction. We leverage both automated and manual testing so we can release the highest quality features possible and ensure that account security is maintained as new features are added and changed.

We use Azure DevOps to facilitate our CI/CD (continuous integration and continuous delivery/deployment) process in development. The Azure platform stores our Git repositories and enables us to conduct code reviews and manage our builds for deployment. In addition, we use automated quality tools to ensure that BigTime maintains best-in-class code which you can rely on for current and future needs.

Account Security

User permissions and Controls

When you add new users to BigTime, we help you make sure their login and access are both tightly controlled and fit best practices. BigTime administrators can customize each user's access levels (by selecting user roles and team assignments), and that security is enforced throughout the product, even with the reporting and BI engines. Our role-based right access allows our customers to tighten down security by the user to ensure their confidential company data is secure from malicious internal activity.

Password Management

We help you enforce best-practices for your user passwords (including complexity, expiration and brute force mitigation). We compare user passwords to common lists to make sure your team doesn't set their password to "password1," and we hash and salt their choices based on industry best practices, so they are never stored in plain text or visible to IT or DBA staff.

When your users login, we track their IP addresses and session data, and we flag or block suspicious or unusual activity -- giving your administrator peace of mind. We also expire idle sessions, so users leaving a computer logged in overnight won't create a security risk.

Project-level Permissions

When you setup BigTime, you can limit user access to only the projects on which they are staffed, giving you the ability to tighten security to a small number of projects. You can even give full-time staff a higher level of access than contract or part-time workers. You can also control what type of data each user-group has access to within a project. For customers that utilize the BigTime Wallet Client Portal, their clients will have access to their invoices and their project teams, but not the rest of the project info.

Single Sign-on (SSO)

We also support Single Sign-on (SSO) authentication through Intuit, Google, Azure Active Directory (Azure AD), OneLogin, and Okta for greater security and compliance. Admins have the option to enable strong passwords, which will indicate to a user how strong or weak their BigTime password is when they create it. If a user's password has been forgotten or compromised, admins have the ability to reset it and generate a temporary password.

GDPR and Data Privacy Compliance

While most of the data stored in BigTime is confidential, some data is consider “personal” (eg - email addresses, home address/phone and even “name” in some jurisdictions). BigTime has a privacy workbook that your implementation manager can help you work through to determine your exposure to GDPR or privacy risk, and we help document, manage and report on PII within the system. These GDPR compliance features have been created to help your firm’s privacy officer manage those complex requirements.

User Permission: Personal Data Access

You control which users have access to Personal Data within the system with a specific rights grant. Users must have that right in order to access PII within BigTime (email, home address, and phone number(s), etc). This is enforced in both staff profile page(s) and within the reporting/BI engines.

Ability to “Forget” Staffer

Once your firm no longer needs the PII for terminated employees, the system allows your privacy team to “forget” it. Instead of simply deactivating a staffer, forgetting them will actively remove all PII from your system (including user name). Note that you can still see business data (eg - time/expenses logged against a project), but you will not be able to see the name of the staffer who logged that data.

Privacy Policy Notification

GDPR (and other privacy regulations) may require you to disclose the way a user’s PII is used or stored, and BigTime makes this easy to accomplish. Not only do we have a customizable privacy notice which users can accept at login, we keep track of changes to that policy over time, and we ask users to re-accept it when you make updates so you stay in compliance.

Risk and Compliance

BigTime encrypts data in transit via TLS 1.2 and encrypts all data at rest and all backups with SHA-256 encryption. The Domain Name System (DNS) is hosted through CloudFlare, an industry leader in DDoS prevention. Personally identifiable information (PII) and sensitive information are encrypted at the table level in our database. Extensive logging is in place to help alert to security incidents. BigTime undergoes semi-annual application penetration assessments as well as network penetration assessments. We also participate in additional audits as required by our partners.

Employees of BigTime undergo annual security awareness training through our security training partner. Developers and technical staff undergo additional training regarding OWASP vulnerabilities and best practices. All corporate systems are encrypted with BitLocker, secured with antivirus, and managed via Intune. BigTime maintains written security policies. All changes to code and infrastructure are peer-reviewed and go through a change management review process.

Independent Audit

BigTime meets or exceeds the standards of SSAE 16 (SOC1 Type II), and we have been SOC compliant since 2019. We are audited throughout the year to ensure that we maintain that compliance, and our system must undergo regular penetration testing from a certified third party in order to maintain that certification. Both reports are available to potential customers, as well as the SOC II compliance report issued to our AWS hosting service (note that an MNDA is required in order to download those reports).

Privacy Compliance

BigTime maintains a privacy policy (https://www.bigtime.net/privacy-policy/). Access to production data is restricted and client data does not leave our cloud. Data can be removed from the system upon client request.

Infrastructure Operations

99.9% Uptime

BigTime has a specific weekly maintenance window within which any system patches or regular updates are performed. Most of the time, our updates require no downtime. If downtime is required, we provide in-app notifications to admins ahead of time. Downtime is scheduled to have minimal impact on the work day in the US, and generally takes place between 9pm and 12am Central Time. BigTime boasts 99.9% uptime with an average response time of 150 milliseconds.

Business Continuity

BigTime leverages AWS to provide a high degree of availability and fault tolerance. Our Elastic Load Balancers (ELB) route traffic to a cluster of servers located across multiple redundant Availability Zones. Customer data is backed up multiple times per day, and shipped from our primary datacenter (AWS East) to multiple off-site locations, including our disaster recovery site which houses a live-updated standby copy of your data.

24x7x365 Monitoring and Protection

BigTime's application performance and security is monitored automatically, and our US-based Operations team is notified of problems automatically, so we can take care of them before they become serious enough that they degrade your team's performance. Note that this monitoring system is validated as a part of our annual third-party audits, and our senior team is updated regularly by the Operations team.

Security

BigTime continuously monitors systems, conducting tests for intrusions and attacks. We monitor all Common Vulnerabilities and Exposures for our environment, and generally patch critical vulnerabilities within 24-hours. To detect security vulnerabilities, BigTime uses a combination of automated scanning, penetration testing, and third-party security research.

BigTime Wallet and Financial Information

Protecting you and your client's data is a top priority, that's why we ensure BigTime Wallet is one of the industry's most secure payment processors. Here's how we take all necessary steps to safeguard your business and secure your sensitive payment data.

Secure Partner

Our payment processing partner (Stax) is a Level 1 PCI Service Provider. Level 1 is the highest level of PCI compliance. They are audited by a certified third party in order to maintain that level of compliance. They offer the tools and insights needed to each one of their members so they can stay PCI compliant. Stax provides multiple tools to empower small- to mid-sized businesses to maintain their own PCI compliance through self-assessment questionnaires, partnership with Approved Scanning Vendors (ASV), and intuitive compliance portals. The Stax team is always available to help with this process.

End-to-End Encryption and Tokenization

Feel protected on every transaction. BigTime Wallet encrypts all card information and, once the transaction is complete, never stores the data. Our modern tokenization prevents others from any interception or viewing the data.

Fraud Prevention

Proactive prevention is key. We have additional technologies within BigTime Wallet to specifically monitor and investigate accounts for any potential unauthorized charges. Our partnership with Know Your Customer and Customer Identification Program works to verify merchants, their businesses, and their funding accounts.

GDPR Compatible

Our solution is aligned and committed to transparency, data protection, and accuracy to remain GDPR compatible.