SECURITY STANDARDS AND PRACTICES

1010data ensures the security of your data with technology and best practices

1010data takes a holistic approach to securing access and customer data. We do this with a multi-level approach that incorporates company policies, integrated security practices, compliance features, physical security, secure data transmission, and secure system design. As each customer need is unique, we are happy to consult with you on any specific security requirements.

1010DATA CORPORATE SECURITY POLICIES

1010data's technical controls strictly define who can access data. Key elements include:

- 1010data developers have access to databases only when required for their job
- Analysts are assigned to specific customers and only access data with the customer's permission
- System administrators have access to raw physical segments of data for technical purposes but do not have logical access to data in usable tables
- Data is never loaded by 1010data onto portable or removable storage, desktops or laptops
- Servers containing the primary 1010data database software and customer data are not connected to the internet
- Firewalls and intrusion detection software are monitored 24 hours a day
- Security patches are installed promptly when applicable to our systems
- 1010data maintains complete, auditable logs of all user interactions involving customer data including user account, IP address, and tables accessed

INTEGRATED 1010DATA SECURITY PRACTICES

The way 1010data handles sensitive data makes the platform more secure, and makes our customers less likely to be attacked or breached.

- 1010data provides customers with granular permissioning to allow for user and group level control over access to tables, rows, and columns
- We strongly recommend that only data with analytical value be loaded onto the system
- Without a specific written agreement, 1010data does not accept information restricted by applicable data privacy laws, including PII and HIPAA PHI, unless de-identified using an approved hashing, tokenization, or encryption mechanism. Examples of such data include credit card and social security numbers

1010DATA COMPLIANCE FEATURES

The 1010data platform supports multiple compliance requirements:

- SOC 2 Type II Certified - dedicated information security director, two person approval for any security changes, confidentiality provision in our contracts (all data is 100% confidential by default and the customer has complete control over any party access to any data)

- HIPAA compliant - servers containing HIPAA PHI data comply with federal security standards and are held in locked cabinets with an audit trail for cabinet opening
- Support for SAML (Security Assertion Markup Language) authentication – customers that implement a SAML Identity Provider can authenticate user access

PHYSICAL AND LOGICAL SECURITY

1010data houses all customer data at SSAE16-certified Equinix data centers. Equinix is an industry leader and imposes high standards for security and environmental controls. Equinix is annually audited for compliance with all necessary security measures. Furthermore, 1010data limits access to physical servers to mission-critical IT staff only for physical maintenance and upgrades. IT staff do not have access to customer data unless necessary to resolve customer issues.

DATA TRANSPORT SECURITY

Electronic transit of customer data and all electronic interactions between users and the 1010data platform are highly secure.

- For browser interactions, transmissions use a Transport Layer Security (TLS) connection. TLS is the successor to the Secure Socket Layer (SSL) security standard
- Daily data loading is done using PGP-encrypted and signed batch files, which are sent over an encrypted connection using a Secure File Transfer Protocol (SFTP) session
- Data files transmitted by customers to 1010data are backed up in the state received

1010DATA IS SECURE BY DESIGN

There are several aspects of the 1010data platform that make it inherently more secure. These include:

- The 1010data platform utilizes a novel stateful architecture that provides each user a unique private instance of the database and allocated working session
- 1010data is not an SQL or RDBMS database, therefore it is not susceptible to SQL injection attacks
- 1010data is an in-memory columnar database broken into proprietary segments leveraging MPP architecture. The data is difficult to reconstruct without proprietary 1010data software
- The 1010data platform is the product of proprietary development and relies on a small number of underlying operating system services (such as file system and networking)

RECOMMENDED BEST PRACTICES FOR CUSTOMERS

As stewards of customer data, we strive to do the best job possible of empowering you, the data owner, to exercise control over the access levels provided to your employees to minimize exposure and risk. Recommended best practices:

- Limit access to the 1010data platform to only those who require access to fulfill their jobs
- Ensure anyone with 1010data platform access has updated malware protection installed locally on their computer
- Set appropriate password strength and lifecycle rules to ensure passwords are hard to brute force
- When a user password is reset by an administrator, users should be required to change their password on the next login
- Never load sensitive data onto the 1010data platform unless it's required for analysis

FOR MORE INFORMATION

For more information about 1010data's security practices and standards, contact 1010data today.

1010DATA™
MORE POWER TO YOU

+1 212.405.1010
info@1010data.com
www.1010data.com

v 08.01.16