DataCurrent

Security Statement

(http://www.datacurrent.ca/contact-us-2/)

Smart City Water (SCW) is dedicated to protecting all customer data using industry best standards.

Many of our biggest customers demand the highest levels of data security, and have tested our services to verify that it meets their standards. Our most important concern is the protection and reliability of customer data.

Our servers are protected by high-end firewall systems, and scans are performed regularly to ensure that any vulnerabilities are quickly found and patched. All services have quick failover points and redundant hardware, with complete backups performed nightly.

Most important is our confidential system component design. Access to our systems is restricted to specific individuals, whose access is monitored and audited for compliance.

SCW uses Transport Layer Security (TLS) encryption (also known as HTTPS) for all transmitted data. We can also protect surveys with passwords and HTTP referrer checking. Our services are hosted by trusted data centers that are independently audited using the industry standard SSAE-16 method.

SCW deploys the general requirements set forth by many Federal Acts, including the FISMA Act of 2002. We meet or exceed the minimum requirements as outlined in FIPS Publication 200.

Since our subscribers control their users and their data, it is important for the users to practice sound security practices by using strong account passwords and restricting access to their accounts to authorized persons. Smart City Water safeguards all customer data, and uses secure data centers to ensure the highest protection requirements.