



Security Policy

This document outlines some of the mechanisms and processes we have implemented to help ensure that your data is protected. Our security practices are grouped in four different areas: Physical Security, Network Security, People Processes, and Redundancy and Business Continuity.

Physical Security

Our data centers are hosted in some of the most secure facilities available today in locations that are protected from physical and logical attacks.

Controlled Entrance. Access to Stillwater Insurance Services data centers is tightly restricted to a small group of pre-authorized personnel.

Secure Authentication. Secure authentication must be used to enter a Stillwater Insurance Services data center. All entries are logged.

Network Security

Our network security team and infrastructure helps protect your data against the most sophisticated electronic attacks. The following is a subset of our network security practices. These are intentionally stated in a very general way, since even knowing what tactics we use is something hackers crave. If your organization requires further detail on our network security, please contact us.

128/256-bit SSL. The communication between your computer and our servers is encrypted using strong 128-bit keys (256-bit keys in many cases). What this means is that even if the information traveling between your computer and our servers were to be intercepted, it would be difficult for anyone to make any sense of it.

IDS/IPS. Our network is gated and screened by highly powerful and certified Intrusion Detection / Intrusion Prevention Systems.

Control and Audit. All accesses are controlled and also audited.

Secured OS. Stillwater Insurance Services applications run inside a secured, operating system engineered for security that minimizes vulnerabilities.

Virus Scanning. Traffic coming into Stillwater Insurance Services Servers is automatically scanned for harmful viruses using state of the art virus scanning protocols that are updated regularly.

People Processes

Designing and running data center infrastructure requires not just technology, but a disciplined approach to processes. This includes policies about escalation, management, knowledge sharing, risk, as well as the day-to-day operations.

Select Employees. Only employees with the highest clearance have access to our data center data. Employee access is logged, and passwords are strictly regulated. We limit access to customer data to only a select few of these employees who need such access to provide support and troubleshooting on our customers' behalf.

Audits. Audits are regularly performed, and the whole process is reviewed by management.

As-Needed Basis. Accessing data center information as well as customer data is done on an as-needed only basis, and only when approved by the customer (i.e. as part of a support incident), or by senior security management to provide support and maintenance.

Redundancy and Business Continuity

One of the fundamental philosophies of computing is the acknowledgment and assumption that computer resources will at some point fail. We have designed our systems and infrastructure with that in mind.

Clustered Architecture. Stillwater Insurance Services run on a clustered architecture. That means a server can fail without a noticeable impact on the system or our services. The system has been designed knowing that server will eventually fail, and we have implemented our infrastructure to account for that.

Internet Redundancy. Stillwater Insurance Services is connected to the world – and you – through multiple ISPs. So if any one fails or experiences a delay, you can still reliably get to your applications and information.

Redundant Network Devices. Stillwater Insurance Services run on redundant network devices (switches, routers, security gateways) to avoid any single point of failure at any level on the internal network.

Data Protection & Back-up. User data is backed-up periodically across multiple servers, helping protect the data in the event of hardware failure or disaster.

While we cannot list all the details of our infrastructure for security reasons, rest assured that Stillwater Insurance Services' security practices, policies and infrastructure are proven and reliable.

For more information about Stillwater Insurance Services and our Security, please contact us.