InkWorks
OPERATE MORE EFFICIENTLY

Software Security

Protecting the security of user information and data under management is paramount to InkWorks software operations.

All data within InkWorks software and client sites is stored in databases running on servers not accessible publicly inside a top level security facility. Databases run on servers separate from web servers behind state of the art firewalls only accessible by technical staff through top of the line Checkpoint VPN software running multi-factor authentication.

Web servers are protected by the same firewall and VPN solutions as the database servers. The web servers do not have a public IP address but are instead accessed by the firewall mapping public IP addresses to private LAN addresses. This level of protection forces a potential hacker to attempt to bypass a firewall appliance or to attack by compromising a web server. Bypassing the firewall is highly unlikely as they have been locked down by staff certified in configuration of the system. Client sites run on fully patched Microsoft IIS web servers, SQL servers, and Windows server software to eliminate those security vulnerabilities outside our control.

All servers are monitored for signs of any additional foreign, hacker, or unorthodox activity on a daily basis.