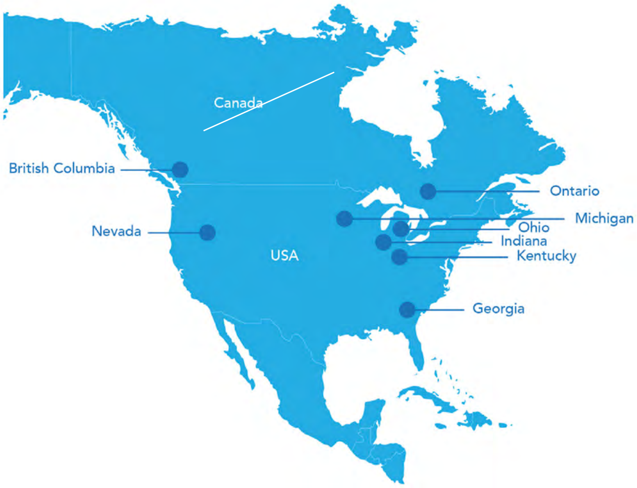
doxim®

Doxim Data

| Security Measures



At Doxim, we take our responsibility to protect our clients' sensitive information very seriously. That's why all Doxim's SaaS solutions are housed in state-of-the-art data centres with built-in redundancy and high availability.

Reduce your operational burden and hardware costs and ensure business continuity in the event of an emergency by selecting Doxim's scalable, flexible SaaS-based solutions. Focus on business growth, knowing we'll take care of the rest.

Data Availability & Security

Doxim software and client data are safely housed in secure data centers. Systems and processes within these environments have been audited to verify redundancy, security, processing integrity, confidentiality, and privacy.

Data Centres Across North America

In Canada, our secure data centres are located in Ontario, and British Columbia. In the US, our data centres are located in North Carolina, Arkansas, and Michigan.

Application-Level Security

Doxim software offers robust security using role-based permissioning, so users only see data relevant to their role in the organization. For example, an individual advisor would be restricted to seeing only their block of business, while a senior compliance staff member would have broader access.

Penetration & Vulnerability Testing

All SaaS products and systems are put through penetration and vulnerability assessments prior to release.

External Testing

Doxim maintains a regular external audit schedule for all environments and SaaS products. Doxim deploys multiple enhanced external vulnerability scanning tools that alert for new security or application vulnerabilities. Prior to every release, each SaaS application is subjected to a vulnerability and penetration test that use a variety of attack scenarios.

No Cross-Border Data Transit

Your client data is stored in secure Doxim data centres within the country of origin. Data traffic is routed exclusively through your country as well, so your data does not cross borders.

Disaster Recovery & Redundancy

Doxim maintains a robust disaster recovery program at all data centers. Each of Doxim's data centers maintain replication capabilities to the designated disaster recovery (DR) sites. These DR sites have a four hour recovery time objective, and a recovery point objective of less than an hour.

Doxim's production servers are entirely virtualized and have multiple redundancies inside the data centers that are "real-time". This ensures that systems are highly available and protects against common hardware failures.

Automated Internal Scans

Doxim's internal security team has implemented several automated security scanning tools that perform regular security scans on the production network. The ensure network and infrastructure assets remain free of vulnerabilities.

Third-Party Auditing

Part of each major software release is a third party security audit for vulnerabilities within our applications. If any are found, we treat them as top priority and will fix them before we release to market.

Security & Service Certifications

Doxim has regular certification audits to comply with stadnards such as SOC 1, SOC 2, ISO9001, and HIPAA. Doxim products also support KYC standards around Anti-Money Laundering and Anti-Terrorism.

Business Continuity

Doxim's Business Continuity plan encompasses our disaster recovery policies and procedures. These are audited annually as part of our SSAE-16 certification. The failover process includes benchmarks for the resumption of business processes, including a RTO (Recovery Time Objective) of approximately 4 hours, depending on the severity of the disaster.

Continuous Monitoring

All of Doxim's SaaS applications and environments are monitored 24/7 using both internal and external systems to monitor availability and red response time. Alerts are sent to support teams if issues are encountered

Change Management

Any change to the production environment in Doxim's Data Centers and SaaS applications are performed within Doxim's change management process. This process is audited as part of our SOC 1 and SOC 2 certifications and ensure changes are approved prior to implementation. All changes are scheduled within the change window.

Patch Management

Doxim has standardized patch management operations across all of Doxim's office and data center locations. This done utilizing industry standard tools and is completed as part of Doxim's change management process during alloted time frames.

doxim®

www.doxim.com Info@doxim.com 866 475 9876