# Doxim Data Security Measures

**Reduce your operational burden, hardware costs, and ensure business continuity in the event of an emergency by selecting Doxim's scalable, flexible, SaaS-based solutions.**

## Secure Data Hosting

Doxim maintains an extensive network of data centers across the nation and around the globe, all fully equipped to meet critical security requirements. With a variety of deployments including on-prem, co-location, as well as private and public cloud, our data centers are strategically located and able to provide business continuity in the event of business disruption.

Doxim software and client data, as well as systems and protocols in our data centers, are regularly audited to ensure security, processing integrity, confidentiality, and privacy. Our security posture exceeds industry standards and is verified by third parties as top ranked across all criteria.

## No Cross-Border Data Transit

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

## Application-Level Security

Doxim adheres to OWASP development security practices to reduce the risk of vulnerabilities within our technology.

- User access control - A role-based user permission system controls access to the application and the hierarchical tree structure allows for tiered access levels.
- Separation of roles - The application splits privileges into several roles. Each element of the application's features has its own roles, such as 'view' or 'edit', which can be assigned to different levels of users that administer the system.
- Access logging and reporting - User actions are logged by the platform for audit purposes. While all services generate log files, the quantity and type of information that is recorded is configurable.

Prior to every software release, each SaaS application is subjected to vulnerability and penetration testing using a variety of attack scenarios.

## Ensuring Performance

All of Doxim's SaaS solutions are housed in Tier 3 data centers with secure, compliant environments with built-in N+1 redundancy and high availability. These environments are monitored 24/7 using both external and internal systems to assess availability and response time. Alerts are sent to support teams if issues are encountered, quickly triaged and addressed.

## Penetration & Vulnerability Monitoring

Doxim deploys multiple enhanced external vulnerability scanning tools that alert for new security or application vulnerabilities within our operations. These regular vulnerability and penetration assessments are conducted against applications and environments to ensure configurations are up to date and new vulnerabilities are patched.

Our security team also manages a program of automated security scanning tools that monitor the production network for suspicious activity. These scans ensure network and infrastructure assets remain free of vulnerabilities and malicious activity.

## Controls Within Our Environment

All changes 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 2 certifications and ensures changes are approved prior to implementation. All changes are scheduled and performed by Doxim staff within the defined change window.

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

## Security & Service Certifications

Doxim's documented security policies provide a comprehensive policy framework that address the full range of required compliance and regulatory controls with regards to data privacy, security, retention, protection and accountability. Many of our policies and procedures also map to NIST controls.

Doxim maintains an annual external audit schedule for environments and SaaS products to comply with standards such as SOC 2, ISO 9001, ISO 27001, PCI DSS and HIPAA, depending on location. For audit compliance, we perform security awareness and privacy training upon hire and annually for all employees, and phishing test are performed throughout the year.

## Business Continuity

Doxim maintains a robust business continuity plan for each of our data centers and across our network of production facilities. As part of this plan, each data center replicates between primary and disaster recovery sites, and these capabilities are audited annually as part of our SOC 2 certification. In addition, Doxim's production servers are entirely virtualized and have multiple real-time redundancies within the data centers. This ensures systems are highly available and protects against common hardware failures.

doxim®

Doxim is the customer communications management and engagement technology leader serving financial and regulated markets, providing omnichannel document solutions and transforming experiences to strengthen engagement throughout the entire lifecycle. The Doxim Platform helps clients communicate reliably and effectively, improve cross-sell and upsell opportunities, and drive increased loyalty and wallet share through personalized communications. The platform addresses key digitization, operational efficiency, and customer experience challenges through our suite of plug-and-play, integrated, SaaS software and technology solutions. Learn more at www.doxim.com.