TRUST AND SECURITY AT SNAPDOCS

A Commitment to Protecting Your Data & Assets

July 2025

snapdocs

Table of Contents

1. Our Commitment to Your Security

In the rapidly evolving digital mortgage landscape, the security and privacy of your sensitive information are paramount. At Snapdocs, we understand that trust is the cornerstone of our partnership with you. This white paper provides insight into our comprehensive security program, demonstrating our unwavering commitment to protecting your data and ensuring the reliability of our solution. Our security measures are not an afterthought; they are integral to our operations, engineered into our products from the ground up, and governed by a robust Information Security Management System (ISMS) aligned with international standards. We proactively manage risks and continuously enhance our defenses to provide a secure, reliable, and compliant environment for every digital mortgage transaction.

2. Company & Solution Overview

Snapdocs is the mortgage industry's leading digital closing provider, on a mission to automate the home mortgage experience by connecting the people, processes, and technologies that power the industry. Our platform automates every interaction between lenders, title companies, and other participants across the entire mortgage closing process, from pre-closing through the sale of the loan.

Our specific solutions—including eClosing, eVault, Notary Connect, Quality Control, and CD Balancing—leverage patented AI technology and extensive settlement networks to deliver fast, accurate, and secure transactions. This approach reduces closing times, minimizes errors, and enhances the borrower experience. The security of the data processed through these solutions is our top priority.

3. Snapdocs' Security Foundation: ISMS and Guiding Philosophies

Security is integral to Snapdocs' operations and culture, forming a core component of our ISMS, which is certified against the ISO 27001 standard. We adopt a "security by design" approach, embedding security considerations into every aspect of our product development and service delivery. This is guided by our detailed Risk Management Policy and a commitment to ethical practices, including the responsible use of technologies like Artificial Intelligence, as detailed in our Use of Artificial Intelligence Policy, and maintaining integrity in our operations as per our Corporate Fraud Policy.

Our security strategy encompasses:

a. **Defense in Depth**
   We implement multiple layers of security controls across our digital infrastructure and physical assets. This multi-layered approach protects our cloud platform, hosted in secure AWS data centers, and the company-provided equipment used by our remote workforce, as governed by our Physical Security Policy and Network Security Policy.

b. **Zero Trust Model**
   Based on the principle of "never trust, always verify," every access request to our systems is rigorously authenticated and authorized, regardless of its origin, minimizing the risk of unauthorized access.

c. **Continuous Monitoring**
We proactively monitor our systems 24×7 for suspicious activity and potential threats, utilizing advanced tools and processes designed to ensure rapid detection and response.

d. **Compliance Alignment**
Our practices are designed to meet or exceed stringent regulatory requirements relevant to financial data and the mortgage industry, including the FTC Safeguards Rule. This is supported by a comprehensive suite of internal policies, including our Internal Privacy Policy, intended to ensure adherence to data protection laws and industry standards.

e. **Ethical and Responsible Innovation**
As we innovate, including with technologies like Artificial Intelligence, we are committed to doing so responsibly, with a focus on data privacy, security, fairness, and compliance, guided by our Use of Artificial Intelligence Policy.

4. How We Protect Your Data and Ensure Service Reliability

Our security practices are built upon specific, documented policies that translate our philosophy into action, providing robust protection for your information and the continuous availability of our services.

a. **Securing the Infrastructure**
Snapdocs leverages the secure and resilient infrastructure of Amazon Web Services (AWS). Our partnership with AWS operates under a Shared Responsibility Model for security and compliance. This model clearly defines distinct responsibilities:

- AWS is responsible for the security OF the cloud. This includes protecting the global infrastructure that runs all AWS services, such as their hardware, software, networking, and facilities.
- Snapdocs is responsible for security IN the cloud. This means we manage and secure everything we deploy and operate within the AWS environment. Our responsibilities include securing our customer data, managing access to our applications and systems, configuring operating systems, network and firewall settings (like security groups), and implementing appropriate data encryption measures. Understanding and diligently managing our responsibilities within this model is a cornerstone of our infrastructure security strategy. Our *Network Security Policy* and *Physical Security Policy* govern additional key measures, including:
  - Multi-layered network defenses with advanced firewalls, network segmentation, and DDoS (Distributed Denial of Service) protection to safeguard your data from external attacks.
  - Secure configurations for all systems and proactive vulnerability management, including timely patching, to address potential weaknesses.
  - Robust physical security for AWS data centers, designed to ensure the underlying infrastructure is protected against unauthorized access and environmental hazards.

b. Building Secure Applications

We build security into our solution from the ground up. Our System Acquisition, Development, and Maintenance Policy mandates a Secure Software Development Lifecycle (SSDLC). This means rigorous security considerations at every stage:

- **Secure Design:** Incorporating threat modeling and security requirements early in the development process.
- **Secure Coding:** Adherence to secure coding best practices and regular training for our developers.
- **Rigorous Testing:** Employing static and dynamic application security testing (SAST/DAST), comprehensive code reviews, and engaging independent third-party firms for regular penetration testing to proactively identify and remediate vulnerabilities before they can impact you.

c. Comprehensive Data Protection

The confidentiality and integrity of your data are paramount. Our approach is guided by:

- **Data Classification:** Our Asset and Data Classification Policy ensures that all information, especially sensitive customer data, is identified, classified, and handled with the appropriate level of security controls throughout its lifecycle.
- **Encryption:** As detailed in our Encryption Policy, all sensitive customer data is encrypted both in transit (using protocols like TLS 1.2 and above) and at rest, utilizing strong, industry-standard algorithms and secure key management practices.
- **Privacy by Design:** Our Internal Privacy Policy and practices embed privacy considerations into our systems and processes, helping you meet your data protection obligations under regulations such as the Gramm-Leach-Bliley Act (GLBA) and the California Consumer Privacy Act (CCPA).

d. Controlled Access to Your Information

Access to your data is strictly limited and meticulously controlled. Our Access Management Policy dictates:

- **Least Privilege:** Users are granted only the minimum level of access necessary to perform their job responsibilities.
- **Strong Authentication:** Multi-Factor Authentication (MFA) is mandatory for all user access to Snapdocs systems, providing a critical additional layer of security against unauthorized logins.
- **Role-Based Access Control (RBAC)**: Access rights are assigned based on defined roles, to provide clear separation of duties and accountability.
- **Regular Access Reviews:** We conduct periodic reviews of user access privileges to ensure they remain appropriate.
- **Secure Remote Access:** Our Remote Work and Mobile Device Policy is designed to ensure that employees accessing systems remotely do so through secure, authenticated channels.

e. **Continuous Vigilance and Operational Resilience**
We are committed to providing a secure and highly available solution.

- **Proactive Monitoring:** As outlined in our Communications and Operations Policy and Incident Management Policy, our systems are monitored 24×7 using advanced tools to detect and alert on security events and potential operational issues. We leverage advanced threat intelligence feeds and tools (such as SIEM and Deepwatch) to stay ahead of emerging threats.
- **Incident Response:** We have a documented and regularly tested Incident Management Policy and plan to enable swift investigation, containment, eradication, and recovery in the event of a security incident.
- **Business Continuity and Disaster Recovery:** Snapdocs is committed to service continuity. Our Business Continuity Policy details robust strategies for disaster recovery, including comprehensive data backup procedures, utilization of geographically distinct AWS availability zones for resilience, and regular testing of our recovery plans to meet defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

5. Our People, Processes, and Partners: A Culture of Security

A truly secure environment relies on more than just technology; it requires a pervasive culture of security.

a. **Our People**
All Snapdocs employees undergo background checks where appropriate and receive comprehensive security awareness training upon hiring and regularly thereafter. This training, governed by our Human Resources Security Policy and reinforced by our Acceptable Use Policy, covers critical topics such as data handling, phishing awareness, and incident reporting, enabling our team to serve as your first line of defense.

b. **Our Processes**
Our Operations and Change Management Policy ensures that any modifications to our production systems are meticulously planned, tested, and approved through a formal change control process. This minimizes the risk of unintended disruptions or security vulnerabilities.

c. **Our Partners**
We understand that our vendors and partners can play a role in service delivery. Our Vendor Management Policy mandates a rigorous due diligence process for all third-party vendors, designed to confirm that they meet our stringent security and compliance requirements before they are integrated into our ecosystem.

6. Our Comprehensive Policy Framework

Our security practices are underpinned by a comprehensive suite of internal policies. While these are internal documents, they form the backbone of our commitment to you. Key areas covered by our detailed policies include:

- Information Security Management System (ISMS) Compliance Policy
- Summary Security Policy
- Risk Management Policy
- Human Resources Security Policy
- Asset and Data Classification Policy
- Access Management Policy
- Vendor Management Policy
- Incident Management Policy
- Internal Privacy Policy
- Encryption Policy
- Physical Security Policy
- Network Security Policy
- Communications and Operations Policy
- System Acquisition, Development, and Maintenance Policy
- Business Continuity Policy
- Operations and Change Management Policy
- Remote Work and Mobile Device Policy
- Acceptable Use Policy
- Corporate Fraud Policy
- Use of Artificial Intelligence Policy

These policies are living documents, regularly reviewed and updated to adapt to the evolving threat landscape and business requirements.

7. Validated Compliance: Our Certifications and Attestations

To provide you with independent assurance of our security commitments, Snapdocs undergoes rigorous third-party audits and maintains key industry certifications:

a. **SOC 2 Type II**
   Our annual System and Organization Controls (SOC) 2 Type II attestation, covering the Security, Availability, and Confidentiality Trust Services Criteria, is prepared by an independent CPA firm. This report provides a detailed examination of our controls, confirming they are appropriately designed and operate effectively over a period of time to safeguard your data.

b. **ISO 27001**
Snapdocs is ISO 27001 certified. This internationally recognized standard validates that we have implemented a comprehensive Information Security Management System (ISMS) for managing sensitive company and customer information, demonstrating a systematic and ongoing approach to security.

c. **FTC Safeguards Rule**
We maintain full alignment with the data protection standards stipulated by the Federal Trade Commission (FTC) Safeguards Rule, which is crucial for institutions handling financial information.

8. Partnering with Snapdocs

Snapdocs is dedicated to providing a digital closing infrastructure solution that you can trust implicitly. Our multi-layered security strategy, rooted in our comprehensive policy framework, advanced technologies, vigilant operations, and a culture of security, is designed to protect your sensitive information at every stage. Our independent certifications further attest to our commitment to meeting and exceeding industry best practices. We believe in transparency and are committed to being your trusted partner in navigating the security complexities of the digital mortgage landscape.

For more details on our security program, please visit the Snapdocs Trust Center at https://www.snapdocs.com/trust-center, review our Privacy Policy at https://privacy.snapdocs.com, or contact your Snapdocs representative. We welcome discussions about how we secure your data and transactions.

Index

Index

