ABI SECURITY POSTURE

ABI DOCUMENT SUPPORT SERVICES: INNOVATING SECURE DIGITAL RECORD RETRIEVAL AND DOCUMENT MANAGEMENT

ABI Document Support Services has made significant capital investments in their IT infrastructure to further enhance retrieval and document management services while maintaining information confidentiality, integrity, availability and privacy at the highest levels for their clients.

Leveraging the elastic capability of cloud computing with its highly integrated security services, virtual appliances, and tools, ABI redesigned its infrastructure to deliver its products and services responsive to dynamic customer demand and the ever changing technology landscape. ABI uses cloud technology features such as availability sets and site recovery services to enable superior business continuity and disaster recovery capabilities.

ABI delivers a high performing, resilient, and secure platform and portal that customers demand. This commitment to securely facilitating record retrieval allows the ABI team to continue to focus on and develop solutions for what we believe to be the document retrieval industry's most secure computing platform. Records are collected, processed, and summarized, many of which contain sensitive information such as: personal identifiable information (PII) or protected health information (PHI), within a secure environment.

Additionally, ABI heavily promotes information security awareness in all segments of the organization to include infrastructure, application development, and IT operations. ABI has established a program that diligently follows recommended cyber security frameworks to protect the interests of the business and its clients. ABI has successfully completed a SOC 2® Type 2 audit that provides assurances to our clients that all systems are performing to the highest operational standards.

ABI® DOCUMENT SUPPORT SERVICES

LEVERAGING THE SECURITY BENEFITS OF A CLOUD COMPUTING PLATFORM

The information technology cloud based infrastructure was designed primarily to protect ABI's information assets and all customer data in its custody during the course of conducting business and delivering its products and services. ABI inherits the security and compliance controls from the cloud provider and uses these as building blocks for a custom security program tailored to the requirements of the business environment and its clients.

Key components:

- Data Protection. ABI's systems are protected from daily threats to data and sensitive information assets through the use of integrated security tools, appliances, and services.

- Agility and Flexibility. The cloud environment provides ABI with the flexibility to turn up capacity to accommodate unpredictable transaction volume and scale down when no longer required. This allows for seamless adjustment to customer demand while maintaining service performance and data integrity.

- High Availability and Support. The cloud technology has inherent redundancies in place to ensure applications and services are always on-line. The cloud services vendor provides constant support complement the ABIDSS technical team for 24/7 monitoring.

- Compliance. The cloud service providers are also keenly aware of their customers' need to be compliant with regulations on processing of PII and PHI are audited for security framework certifications such as PCI, ISO 27001, and SOC2.

The cloud based infrastructure platform implemented not only "future proofs" ABI's computing environment, but provides a tight coupling with the application development platforms and tools. This coupling establishes the development roadmap for the next generation of applications and services that are secure and high performing.

SECURE CUSTOM APPLICATION SOFTWARE DEVELOPMENT

All applications utilized in the delivery and processing of ABI products and services are developed and maintained internally with the most current development platform, Agile software project management (SCRUM) methodology, and software code release automation. All personnel involved in these three areas are trained to maintain awareness in secure application development using best practices as recommended by the Open Web Application Security Project or OWASP. Software developed goes through the rigors of application security assessment and scans both in a static and dynamic state. All applications have inherent identity and access management controls to ensure users have the appropriate access to resources their roles entitle them. Identity and access control techniques such as single sign-on (SSO) are supported including standard application programming interfaces (API). Data processed through these applications are encrypted both at rest and in transit using ciphers with the highest level of encryption (Ex. AES 256 bit).

CLOUD COMPUTING SERVICE MODEL: DYNAMIC, RESILIENT, SECURE, AND COST EFFECTIVE

In 2017 and again in 2018, **KMWorld Magazine** named ABI one of the "100 Companies That Matter in Knowledge Management."

ABI's software tools and services are delivered over the web, and this model is commonly called Software as a Service or SaaS. In this model, ABI manages and maintains its cloud infrastructure of virtual networks, servers, storage, databases, and other services to host the applications for document retrieval requests; records organization, and analysis applications such as eSummary by ABI™. The hosting environment is architected to be highly available, redundant, and resilient from unforeseen increased computing demands, and adverse events such as hardware failures. The agility of the infrastructure reduces costs and increases efficiency by having the flexibility to adjust the environment to its optimal performance at any given moment. This capacity elasticity allows users to experience a consistent level of experience and performance. ABI maintains both a primary and secondary virtual data center separated geographically in different continental US regions. These data centers leverage the site recovery services provided by the cloud for a best-in-class Business Continuity and Disaster Recovery solution. ABI conducts a Business Continuity and Disaster Recovery test annually to ensure the promise of continuous availability is maintained even in extraordinary circumstances.

SECURITY OPERATIONS

ABI has a comprehensive security policy that includes detailed Intrusion Detection and Incident Response Policies and Procedures that monitor all aspects of the network, software and applications. The Computer Security Incident Response Team (CSIRT) also conducts Intrusion Detection simulations to ensure system integrity. The network is protected from email-borne threats consisting of virus attacks, spam, false positives, distributed denial-of service (DDoS) attacks, spyware, phishing regulatory compliance violations and data loss, which are central to security protection. Network Penetration tests are also performed routinely. Preventive monitoring and reactive blocking security measures are active components of our security profile.

SECURITY OVERSIGHT

ABIDSS completes a SOC 2 security audit annually. SOC 2 is a security standard of the American Institute of Certified Public Accountants. The SOC 2® Type 2 audit is performed in accordance with the Trust Services Principles, testing and reporting on the design (Type I) and operating (Type II) effectiveness of a service organization's controls. The ABI SOC 2 report focuses on a business's non-financial reporting controls. Each of the principles has defined criteria controls that must be met to demonstrate adherence to the principles.

The company maintains an information security program that adheres to recommended cyber security frameworks supported by technical and administrative policies and controls that are designed to provide the highest level of security quality and oversight of our records retrieval services and operations. The ABI information security organization conducts periodic self-audits to ensure adherence and compliance to the policies. The company maintains a unique set of information technology policies that address network, cyber and physical security. The Security team provides comprehensive instructions around key areas such as: Business Continuity and Disaster Recovery, Change Management, Privileged Access Management, End-Point Security, Data Confidentiality and Security, Incident Response, Intrusion Detection, and Identity multi-factor authentication (MFA).