ancora Software Information Security Whitepaper

Introduction

ancora Software delivers a groundbreaking advanced data capture solution built in accordance with information security best practices and end-to-end security and end-to-end privacy. We leverage industry standard technologies and protocols, leading platform providers and an industry recognized risk management framework to deliver a compliant and trustworthy system. Ensuring the confidentiality, integrity and availability of customer data is central to Ancora Software, as is maintaining the trust and confidence of customers and clients.

Continuous improvement of the Ancora Software Information Security program is sought through certifications and third-party assessments. These independent sources of information assist customers in understanding the controls in place, and how those controls are validated. This paper outlines how ancora Software creates a secure solution and maintains compliance while, increasing product capability and improving document classification and data capture rates.

Overview

ancora Software has taken a risk-based approach to information security, considering likelihood, impact to the business and cost, with controls applied following a defense in depth strategy. Essential to this approach is the performance of accurate risk assessments and business impact analysis. The company manages risk through implementing controls represented in policies, procedures, standards and baselines.

ancora Software Corporate policies are designed to ensure the appropriate security customer and client data across the environment, in compliance with existing laws. Information Security and compliance with SOC 2 Type 2 and NIST are an integral part of our business operations, therefore ancora Software has established a program to address our own compliance requirements while also meeting the expectations of its customers. ancora Software has chosen the NIST security framework as the foundation for our Corporate Information Security program. The NIST framework provides a prescriptive process to meeting the regulatory requirements that apply to ancora Software in the markets we serve.

ancora Software commits to annual risk assessments and penetration tests by qualified third parties a requirement of SOC 2 to remain in good standing. Independent audits and review are cornerstones of our Information Security Program and a requirement for objective validation or critique of our approach and implementation.

Corporate Security Policies

ancora Software policies cover security related topics ranging from general policies such as access management, data security, physical security, and third-party risk management, as well as policies covering internal applications and systems. Policies are updated at least annually, and employees are required to review and acknowledge acceptance of Ancora Software policies upon hire and annually thereafter.

Employees undergo yearly information security awareness training, with periodic information security reminders throughout the year. To protect confidentiality, we also provide an anonymous compliance hotline for employees.

Organizational Security

The Ancora Software Privacy Officer and CISO share responsibility for ensuring security processes are in place, communicated to all stakeholders, and consider and address organizational requirements. Together, they ensure the effectiveness of the information protection program through program oversight. They establish and communicate the organization's priorities for organizational mission, objectives, and activities, review, and update of the organization's security plan, ensure compliance with the security plan, and evaluate and accept security risks on behalf of the organization.

Data and Asset Management

Ancora Software protects data and assets according to established policies, through multiple technical controls and procedures. Technical controls are administered by a combination of internal staff and managed service provider (MSP), with oversight by outside legal counsel.

Data Loss Prevention

Data loss is a threat to any data driven technology company and is a threat that demands modern solutions. Data loss prevention (DLP) is built into ancora Software products at the design phase and continually tested and retested. We implement backup and recovery solutions in the datacenter and at the endpoint using industry recognized products and technologies

Encryption at Ancora Software

Data at rest on ancora Software endpoints and servers is encrypted with AES-256 or higher. Encryption status is enforced, monitored, tracked, and reported so we can always say with confidence that data at rest is safe from foreseeable threats.

ancora Software policy is that information in transit must always be encrypted with strong, industry validated algorithms, disallowing any weak algorithms or hashes. Adherence to this policy is reflected in every product we use, develop or consider.

Additional Endpoint Protections

Ancora Software further ensures confidence in endpoint security through a suite of software that enforces, enhances, and supplement the native capabilities of the latest major operating systems. Through these technologies, we can enforce controls such as:

- End to end SSL data encryption
- host-based firewall
- host-based intrusion detection
- web filtering
- software blacklisting
- antivirus and antimalware
- external storage control and restriction
- patch status reporting
- ransomware protection
- detection and block of confidential information transmission
- remote locate
- remote lock
- remote wipe capability
- patch deployment
- and other native controls

Access Control and Infrastructure Security

Access control at Ancora Software includes industry best practices, such as role-based access control (RBAC), password enforcement, multifactor authentication (MFA), and centralized audit logging. Through these controls, Ancora Software maintains compliance and security, with audit trails non-modifiable from the systems producing the logs.

Monitoring

Infrastructure and application availability and performance is monitored 24x7, with thresholds triggering intervention, and logs from infrastructure and applications aggregated for analysis. The combination of logs from multiple sources allows correlation of events by automated systems that would otherwise go unrecognized by a human observer.

Network Security

Network firewalls and web application firewalls (WAF) protect the perimeter of the Ancora Software infrastructure, with intrusion detection systems, network segregation and network access control lists (ACL) protecting the inside.

Intrusion detection systems use signature and anomaly-based analysis mechanisms to analyze all traffic for known or suspicious intent from outside the organization as well as within. Application and network traffic signature pattern matching identify potential security weaknesses.

Vulnerability and Incident Management

Security Scanning and Patching

ancora Software performs automated and manual security testing of cloud assets, corporate endpoints, infrastructure, and applications. We engage third-party specialists on a regular basis to identify potential security vulnerabilities and bugs, including annual penetration testing by qualified third parties.

Results of these scans, as well as vulnerability announcements and patch publication by vendors serve as inputs to the Ancora Software vulnerability management process and ultimately to our change management process. Vulnerabilities and changes, including patching, configuration changes and mitigations, are evaluated according to severity of risk to confidentiality, integrity and availability of systems and data. Changes are implemented with a priority commensurate with the outcome of that evaluation, with security receiving the highest priority.

Incident management

An incident management process is initiated for security events that may affect the confidentiality, integrity, or availability of systems or data. This process guides the course of action and procedures for notification, escalation, mitigation, documentation, with root cause analysis following any incident.

Through outside counsel, ancora Software has access to forensics analysts to determine scope and severity of an incident should it arise. Incident response plan testing for systems that store sensitive customer information occurs at least annually. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities, and are performed as tabletop exercises led by a third-party.

Systems Development and Change Management

ancora Software Engineering follows formal software development lifecycle (SDLC) and change management to ensure that application changes have been authorized prior to implementation into the production environments, that changes are reviewed by senior engineers and initiated by business requirements documents or project tickets.

Proposed changes are reviewed and approved using a Risk Based decision model that considers all aspects of the Business, including Information Security. Changes are promoted through a pipeline, where automated Quality Assurance (QA) testing verifies that functional and security requirements are met. Included in the QA phase are source code quality checks, library vulnerability analysis and web application vulnerability scans. Builds passing all QA and UAT tests receive a final review by Engineering leads and the Business. Upon a successful review, Cloud Ops, in coordination with the Business, initiates the production release to complete the deployment. Changes released into production are logged and archived, and rollback procedures are documented.

Data centers

The ancora Software Platform is built upon state-of-the-art, and industry leading cloud provider Microsoft Azure. With certifications attained, such as SOC 2, HITRUST and ISO 27001:2013, 27017:2015, 27018:2014, and ISO/IEC 9001:2015, Azure is the trusted technology partner of some of the world’s largest companies, and government agencies handling the most sensitive of data. The Azure facilities provide the secure, scalable, and reliable foundation ancora Software requires to meet regulatory requirements and business objectives.

Business Continuity and Disaster Recovery

All functional and business areas, including administrative, legal, IT support functions, and Dev/ops are included in the business continuity planning process. Ancora Software continually refines plans, procedures, and guidelines for continued operations in the event of disaster, establishing procedures for recovering business operations, internal data, systems, and critical internal functions to maintain client services in the face of unexpected events.

Third Party Suppliers

Ancora Software performs a risk analysis of third-party suppliers, including Information Security Assessments (ISA) and an executed Business Associate Agreement (BAA) if warranted by the nature of the service provided. Suppliers that cannot provide assurance of necessary information security standards, policies and procedures, are not acceptable to the Ancora Software Information Security Management Program.