PREPARED BY: INTERNAL DATA SECURITY TEAM, ANTERA SOFTWARE USA, INC.

DATE LAST REVISED: MARCH 24, 2020

Introduction

Antera Software USA provides Software as a Service (SaaS) to promotional product companies across the globe. Security is a key concern and of utmost importance to us. As such, it is reflected in our handling of our people, partnerships, products and processes. This page covers data security, operational security, and physical security, and outlines how we provide security to our customers.

Overview

Our security strategy makes the following considerations:

- Organizational security
- Physical security
- Infrastructure security
- Data security
- Identity and access control
- Operational security
- Incident management
- Vendor management
- Customer controls and security

Organizational Security

We have an Information Security Management System (ISMS) in place which considers our security objectives and the risks and mitigations concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

Security Awareness

Each employee, prior to beginning work, signs a non-disclosure agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance.

We educate our employees on information security, privacy, and compliance on an ongoing basis to keep them updated regarding the security practices of the organization.

Continual monitoring of security & privacy

Our development/IT team implements and manages our security and privacy programs. They oversee and maintain our defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity.

Endpoint security

All workstations issued to Antera employees run up-to-date OS version and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by Antera's endpoint management solutions. These workstations are secure by default. They are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. We have a strict policy concerning who and who may not use mobile devices in the company or for company business.

Physical security

At workplace

Access to our resources (buildings, infrastructure and facilities), where accessing includes consumption, entry, and utilization, is gained via access cards. Only select employees have access to our offices out of hours.

At Data Centers

Our Advance™ application runs 100% in the Amazon Web Services (AWS). AWS has world class security at their Data Centers. https://aws.amazon.com/compliance/data-center/controls/

Monitoring

Our office management company has monitoring on all entry and exit movements throughout our premises via CCTV cameras deployed according to local regulations. Back-up footage is available up to a certain period, depending on the requirements for that location.

Infrastructure security

Network security

Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We use firewalls to prevent our network from unauthorized access and undesirable traffic. Our systems are segmented into separate networks to protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting Antera's production infrastructure.

Network redundancy

All the components of our platform are redundant. If there's a server failure, users can carry on as usual because their data and Antera's services will still be available to them.

Additionally, we use multiple switches, routers, and security gateways to ensure device-level redundancy. This prevents single-point failures in the internal network.

Server hardening

All servers provisioned for development and testing activities are hardened (by disabling unused ports and accounts, removing default passwords, etc.).

Data security

Data isolation

Each customer's service data is logically separated from other customers' data using a set of secure protocols in the framework. This ensures that no customer's service data becomes accessible to another customer.

The service data is stored on our servers when you use our services. Your data is owned by you, and not by Antera. We do not share this data with any third-party without your consent.

Encryption

In transit: All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We mandate all connections to our servers use Transport Layer Security (TLS 1.2/1.3) encryption with API access. This ensures a secure connection by allowing the authentication of both parties involved in the connection, and by encrypting data to be transferred.

We have enabled HTTP Strict Transport Security header (HSTS) to all our web connections. This tells all modern browsers to only connect to us over an encrypted connection, even if you type a URL to an insecure page at our site.

Data retention and disposal

We hold the data in your account as long as you choose to use Antera's services. Once you terminate your Antera user account, your data will get deleted from the active database during the next clean-up that occurs once every 6 months. The data deleted from the active database will be deleted from backups after 3 months. In case of your unpaid account being inactive for a continuous period of 120 days, we will terminate it after giving you prior notice and option to back-up your data.

Administrative access

We employ technical access controls and internal policies to prohibit employees from arbitrarily accessing user data. We adhere to the principles of least privilege and role-based permissions to minimize the risk of data exposure.

Access to production environments is maintained by a central directory and authenticated using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Furthermore, we facilitate such access through a separate network with stricter rules and hardened devices. Additionally, we log all the operations and audit them periodically.

Operational security

Logging and Monitoring

We monitor and analyze information gathered from services, internal traffic in our network, and usage of devices and terminals. We record this information in the form of event logs, audit logs, fault logs, administrator logs, and operator logs. We store these logs in a secure server isolated from full system access, to manage access control centrally and ensure availability.

Backup

We run full backups once a week and incremental backups every day. Backup data in a DC is stored in the same location and encrypted at rest, as the original data.

If a customer requests for data recovery within the retention period, we will restore their data from the backup and make it available to them.

Disaster recovery and business continuity

Application data is stored on resilient storage that is replicated across data centers. Data in the primary zone is replicated in the secondary in near real-time. In case of failure of the primary zone, secondary zone takes over and the operations are carried on smoothly with minimal or no loss of time.

Incident Management

Reporting

We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will provide you with necessary evidences regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations.

Breach notification

As data controllers, we notify the concerned Data Protection Authority of a breach within 72 hours after we become aware of it, according to the General Data Protection Regulation (GDPR). Depending on specific requirements, we notify the customers too, when necessary. As data processors, we inform the concerned data controllers without undue delay.

Vendor & Third-party supplier management

We evaluate and qualify our vendors based on our vendor management policy. We onboard new vendors after understanding their processes for delivering us service and performing risk assessments. We take appropriate steps to ensure our security stance is maintained by establishing agreements that require the vendors to adhere to confidentiality, availability, and integrity commitments we have made to our customers. We monitor the effective operation of the organization's process and security measures by conducting periodic reviews of their controls.

Customer controls for security

Here are the things that you as a customer can do to ensure security from your end:

- Choose a unique, strong password and protect it.
- Use multi-factor authentication
- Use the latest browser versions, mobile OS and updated mobile applications to ensure they are patched against vulnerabilities and to use latest security features
- Exercise reasonable precautions while sharing data from our cloud environment.
- Classify your information into personal or sensitive and label them accordingly.
- Monitor devices linked to your account, active web sessions, and third-party access to spot anomalies in activities on your account and manage roles and privileges to your account.
- Be aware of phishing and malware threats by looking out for unfamiliar emails, websites, and links that may exploit your sensitive information by impersonating Antera or other services you trust.

PCI Compliance

Antera is committed to protecting consumer credit card data in compliance with the Payment Card Industry Security Data Security Standard. Our alignment with this standard is reflected in the people, technologies and processes we employ. As such, we conduct regular reviews and vulnerability scans in accordance with the PCI DSS requirements for our business model.

Questions or comments? Please contact our support team: 214.556.8040 support@anterasoftware.com.