Security, Privacy, and Architecture

Apolloware's Corporate Trust Commitment

Apolloware is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing robust security and privacy program that carefully considers data protection and security matters across our services. Apolloware is dedicated to protecting Customer Data from Utility, Commercial entities, or Residential users.

Services Covered

This documentation describes the architecture of the security-related and privacy-related platforms, and the administrative, technical, and physical controls applicable to Apolloware.

Architecture and Data Segregation

The Apolloware Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Utility IDs" or "Commercial IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for development, testing, and production. The specific infrastructure used to host Customer Data is described in the "Sub-processors and Infrastructure" documentation available here.

Apolloware is hosted in the Amazon Web Services (AWS) infrastructure and maintained securely by Apolloware development and oversight teams. This infrastructure is described in the "Sub-processors and Infrastructure" documentation. This means the underlying physical infrastructure on which your Customer Data is stored will be with AWS for what is commonly referred to as Infrastructure as a Service, and the Covered Services will run on top of the AWS Platform.

Control of Processing

Apolloware has implemented procedures designed to ensure that Customer Data is processed to allow reporting on customer Power and Energy as prescribed by the Apolloware EULA. The Customer Data is processed throughout the entire chain of processing activities by Apolloware and its sub-processors. In particular, Apolloware and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities. The "Sub-processors and Infrastructure" documentation describes the sub-processors and certain other entities material to Apolloware's provision of its Platform.

Third-Party Functionality

Certain features of the Covered Services use functionality provided by third parties.

When customers use messaging capabilities to transmit or receive mobile messages, such as SMS and email messages, the content of those messages and related information about those messages are received by (a) aggregators – entities that act as intermediaries in transmitting mobile messages or provisioning mobile numbers, and (b) carriers – entities that provide wireless messaging services to subscribers via wireless or wireline telecommunication networks. Such aggregators and carriers access, store, and transmit message content and related information to provide these functions.

Customers may decide to not use the SMS feature or the Email features.

Security Policies and Procedures

Apolloware is operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash
- Passwords are not logged
- Apolloware personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user through a managed authentication process
- User access log entries will be maintained, containing date, time, user ID, URL executed or ID operated on, the operation performed (created, updated, deleted), and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by the Customer or its ISP or if the Customer is accessing the site through a VPN (Virtual Private Network)
- If there is suspicion of inappropriate access, Apolloware can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs are not available except as requested to AWS

- System logs, and application logs will be kept for a minimum of 30 days. Logs are stored withing AWS in a secure area with minimal access

Security Logs

All systems used in the provision of the Apolloware are cloud-based in AWS, and include network access, network changes, network traffic from outside and inside of the virtual private networks. These logs are all stored securely to a cloud-based system and only are accessible by minimum Apolloware employees.

Incident Management

Apolloware maintains security incident management policies and procedures. Apolloware notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Apolloware or its agents of which Apolloware becomes aware, to the extent permitted by law.

User Authentication

Access to Apolloware requires authentication via one of the supported mechanisms including user email/password. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state. The session is only good for one hour before it has to be refreshed or the user will be logged out.

Physical Security

Cloud4Wi Products uses AWS, as described above; further information about security provided by AWS is available from the AWS Security website, including AWS’s overview of security processes.

The production data centers of Amazon, used to provide the Covered Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data stored in Apolloware is stored on a primary database server with multiple active clusters for higher availability. All Customer Data stored in Apolloware is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance.
All Customer Data stored in Apolloware, is backed up daily to ensure restore capability. Raw Customer Data is stored under encryption and is able to be re-used to re-create and data deficiencies or errors. The Raw data is redundant and has a reliability through AWS of 9.99999999%.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. Apolloware utilizes secondary AWS facilities that are geographically diverse but in the same general region from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Apolloware production facilities at the primary data centers were to be rendered unavailable.

The Apolloware disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Apolloware within 12 hours after Apolloware’s declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of both data centers at the same time, and exclude development and test bed environments.

Viruses

Apolloware does not scan for viruses that could be included in attachments or other Customer Data that could be introduced by a customer. Uploaded attachments, however, are not executed or executable in the Apolloware cloud environments and therefore should not damage or compromise the Apolloware by virtue of containing a virus.

Data Encryption

The Cloud4Wi Products use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and Apolloware. These include Secure HyperText Transport Protocol (HTTPS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys at a minimum. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption. All Customer Data is encrypted at rest in storage. It is encrypted using industry-accepted encryption keys which are stored, maintained, and rotated using AWS services.

Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data stored within Apolloware is retained in inactive status within Apolloware databases for 180 days, after which it is securely overwritten or deleted from production and from backups. This process is subject to applicable legal requirements.

Sensitive Data

Important: In the event that Apolloware accepts credit cards for any type of payment. A third party service using an iframe presented through a page hosted on Apolloware. The cardholder data is collected by the third party that is configured and managed by the third-party. Apolloware does not and will not store payment cardholder data and authentication data, credit or debit card numbers, or any security codes or passwords within its system.

Analytics

Apolloware may track and analyze the usage of the Apolloware users for purposes of security and helping Apolloware improve both Apolloware Products and Offerings and the user experience in using the Apolloware. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.