METER

AROYA CONTROL SECURITY, PRIVACY, AND ARCHITECTURE

METER CORPORATE COMMITMENT TO TRUST

The trust of METER customers is critical to us, and we are committed to earning and maintaining that trust. To that end, METER considers it integral to provide a robust security and privacy program that carefully considers data protection matters, including protection of customer data.

SERVICES INCLUDED

This documentation describes the architecture of the security and privacy-related audits and the administrative, technical, and physical controls applicable to (1) AROYA Hardware (including Gateways and Routers) and (2) AROYA Control (collectively, referred to for the purposes of this document only as "Covered Services").

ARCHITECTURE AND DATA SEGREGATION

The Covered Services operate in a multitenant architecture, which is designed to segregate and restrict customer data access based on business needs. The design of the system allows for an effective and logical data separation for different customers via customer-specific Facility IDs and allows the use of role-based access privileges. Further additional data segregation is ensured by providing unique, purpose-driven environments for different functions, such as testing, development, and production.

AUDITS

The covered services undergo security assessments by internal personnel and third-party security experts on at least an annual basis. These audits include infrastructure vulnerability assessments and application security assessments.

AROYA uses infrastructure provided by Amazon Web Services, Inc. (AWS) to host Customer Data submitted to AROYA. Information about the AWS security and privacy audits and certifications, including ISO 27001 and SOC reports, is available at the AWS Compliance Website and the AWS Security Website.

SECURITY POLICIES AND PROCEDURES

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way, salted hash.
- User Access Log Entries are maintained, containing date, time, URL executed or entity ID operated on, operation performed (Create, Update, Delete), and source IP address.

  NOTE: Source IP address may not be available if the customer is using NAT or PAT.
- Customer log entry records are provided upon request to resolve suspicion of inappropriate access.
- System Infrastructure logs and Application logs are kept for a minimum of 14 days. Logs are kept in a secure area to prevent tampering.
- Passwords are not logged.
- Passwords are not defined by METER for any users. Passwords are set to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

SECURITY LOGS

All systems used in the operation of the Covered Services, including firewalls, routers, network switches, and operating systems, log information to their respective log facility or a centralized log server (hereto referred to as the SIEM) in order to enable security reviews and analysis.

METER Group, Inc. USA
2365 NE Hopkins Court, Pullman, WA 99163
T +1.509.332.2756 **F** +1.509.332.5158
E info@metergroup.com **W** metergroup.com

INCIDENT MANAGEMENT

METER maintains security incident management policies and procedures. METER will notify any impacted customer without undue delay of any unauthorized disclosure of their respective Customer Data by METER or its agents of that METER becomes aware to the extent permitted by law.

METER typically notifies customers of significant incidents by email and, for incidents lasting more than 4 hours, may invite customers to join a conference call about the incident and the METER response.

USER AUTHENTICATION

Using the Covered Services requires authentication. All data access requires successful authentication. Following successful authentication, the system will assign a random Access Token to the user to preserve and track session state.

PHYSICAL SECURITY

Production data is housed in a data center that utilizes access control systems to ensure only authorized personnel have access to secure areas. These facilities are designed to withstand adverse weather, provide redundant electrical and telecommunication systems, utilize environmental monitoring systems to monitor temperature, humidity, and other conditions, and contain strategically placed heat, smoke, and fire detection and suppression systems. Facilities are secured by around-the-clock guards, surveillance, and 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 backup generators.

RELIABILITY AND BACKUP

All networking components and servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services are stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Covered Services, up to and including the last committed transaction, are automatically replicated on a near real-time basis to the secondary site and backed up to localized data stores. The foregoing replication and backups may not be available in the case that a “Right to be Forgotten” request is submitted or the account is canceled or otherwise terminated because either may delete Customer Data submitted to Covered Services without the possibility of recovery.

VIRUS

The Covered Services will not scan for potential viruses included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and, therefore, will present no risk to damage or compromise of the Covered Services by containing a virus.

DATA ENCRYPTION

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer’s network and the Covered Services, including through Transport Layer Encryption (TLS) leveraged at a minimum of 2048-bit RSA certificates and 128-bit symmetric encryption keys. All data transferred between data centers utilizes AES-256 encryption.

PROTECTION OF CUSTOMER DATA

The Covered Services will maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of customer data. Safeguards will include, but not be limited to, measures designed to prevent unauthorized access to, or disclosure of Customer Data. Customer Data is only processed or utilized to fulfill the contractual obligations set forth in the Covered Services contract.

DELETION OF CUSTOMER DATA

Day 0	Contract termination—data is available for return to the customer.
Day 31	Data is inactive and no longer available for the customer.
Day 121	Data is deleted or overwritten from production.
Day 365	Data is deleted or overwritten from backups.