Third-Party Security Requirements Documentation
ZENTRA Cloud – METER Group, Inc.

Document Version: 2.0

Last Updated: October 15, 2025

Contact: support.environment@metergroup.com

Platform Overview

Product Name: ZENTRA Cloud

Organization Display Name: METER Group, Inc.

Website: metergroup.com

Primary Contact for Security Inquiries: support.environment@metergroup.com

Platform Description: ZENTRA Cloud is a web subscription service software for ingesting scientific environmental data transmitted by METER Group dataloggers.

1. Data Classification

1.1: How is data being collected by, transmitted to, or stored by METER Group?	Data is collected and stored locally by METER Group's data logging devices. These devices are equipped to transmit environmental data to ZENTRA Cloud via cellular or Wi-Fi networks. Once received, the data is stored securely in cloud infrastructure and made accessible through a web-based interface. The types of data collected and managed include: • **Device Configuration**: Cellular and Wi-Fi network settings. • **Device Metrics**: Battery voltage, barometric pressure, and other operational parameters. • **Sensor Data**: Output from connected sensors, including environmental measurements. • **Location Information**: Measurement coordinates • **User-Defined Metadata**: Plot names, customer designations, and other contextual labels. • **Data Logs**: Time-series records of sensor readings and device status. This data enables real-time monitoring, historical analysis, and remote management of environmental sensing systems.

2. Network Security

2.1: Can you provide sanitized copies of system architecture diagrams and data flow diagrams, as pertaining to the service being provided?	Due to the sensitive nature of system architecture, we do not publicly share diagrams.
2.2: Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?	Yes. METER uses segmented networks.
2.3: Does METER Group require secure remote connectivity to My Network (or a Third-party network) to access data, or to perform support/administration tasks?	No. METER does not require access to your network.

2.4: What protocols will you use to protect application data in transit (e.g., TLS, SSL, SFTP, FTP/S)?	All client to server communication is SSL encrypted.

3. Application Security

3.1: Do you follow a formal software development process that includes application security requirements? Please explain.	Yes. METER follows a formal software development lifecycle, integrating application security and functional requirements. Developers follow secure coding practices. Code reviews include security checks. Manual and automated testing checks for vulnerabilities.
3.2: Do you use non-production systems to prohibit the storage and use of production data in non-production (e.g., test and development) applications?	No. Separate development environments, but with real data for optimal testing and validation.

4. Data Storage Security

4.1: Do you purge application data according to a defined data retention schedule? Please explain.	Data is retained indefinitely unless otherwise requested.
4.2: How do you secure data in your backups?	All servers and data tables are regularly backed up in an offsite encrypted form.
4.3: How do you ensure that subcontractors and other third parties handle my data securely?	Data access is limited to internal company use only. No third party or subcontractor is granted access to your data.

5. Security Policies and Procedures

5.1: Do you have current, documented policies that I can read?	Confidentiality and internal security policies prohibit publishing this information.

6. Access Management

6.1: Please describe your process to grant, modify, review, and terminate end-user access to the system.	• User access is managed by the admin. • Users create accounts via the ZENTRA Cloud web interface. Each account is uniquely tied to an email address. • Organization admins can invite users by email, specifying their role and scope of access.

	• Admins can update a user's role at any time through the organization or project settings. • Admins can modify or remove users from organizations, immediately revoking or modifying access. • Access to the organization is not terminated unless expressly requested.
6.2: Are you an InCommon Participant, and/or do you support SAML2?	No.

7. Change Control and Vulnerability Management

7.1: Do you rely on one or more cloud service providers? If so, please confirm which controls are maintained by you and which controls are maintained by your provider (e.g., patch management, log management).	The platform relies on service providers for maps and graphs. Controls for these services are maintained by METER and not by the providers.

8. Security Assessments

8.1: How often do you conduct regular security control reviews of IT systems (by Internal Audit, a trusted third party, etc.)?	Quarterly.
8.2: Do you have a process to address audit recommendations and to ensure compliance with security policies and standards?	Yes. Quarterly meeting with our Security Committee.

9. Disaster Recovery and Business Continuity

9.1: Have you activated and tested all or part of your BCP/DRP in the last twelve (12) months? If yes, please describe the scenario and the impact it had on your ability to meet customer service commitments.	Recovery tests are conducted monthly. Recent recovery scenarios have been successful without incidents.
9.2: Please explain how you would communicate with Customers during an emergency or an outage.	For planned and unplanned outages, customers are notified directly via email or in-app.
9.3: What is your expected recovery time for the services provided to Customers?	Recovery time varies depending on the nature and severity of the incident. Recoveries are expected to be completed within 24 hours.

9.4: How often do you assess your operational and environmental risks (e.g.,quarterly, semi-annually, and annually)?	Operational risks are assessed quarterly.

10. Public References

10.1: Are other Customers currently using this solution that would be available to contact.	Kevin Hyde: Montana Mesonet Coordinator kevin.hyde@mso.umt.edu